
OISSG
OPEN INFORMATION SYSTEMS SECURITY GROUP
Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1A
Date : May 01, 2006

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Opportunities for business today are everywhere. Technologies such as the internet today enable even any business to enter markets globally. Market forces such as globalization impact even local businesses in the remotest markets. Research, Marketing, Manufacturing, Distribution, and Accounting are all functions that are constantly evolving to meet the exigencies demanded by the cumulative effect of these on-going changes. Uncertainties therefore have become a constant that organizations have to deal with on a day to day basis. Every organization is, to some extent, in the business of risk management, no matter what its products or services. It is not possible to "create a business that doesn't take risks," according to Richard Boulton and colleagues, co-authors of “Cracking the value code”. "If you try, you will create a business that doesn't make money." As a business continually changes, so do the risks. Stakeholders increasingly want companies to identify and manage their business risks. More specifically, stakeholders want management to meet their earnings goals. Risk management can help them do so. According to Susan Stalnecker, vice president and treasurer of DuPont, "Risk management is a strategic tool that can increase profitability and smooth earnings volatility." Senior management must manage the ever-changing risks if they are to create, protect, and enhance shareholder value.

Risk management despite its key role in formulating business priorities is not usually a central activity within an organization. Today no organization that we know has a Chief Risk Officer. It is expected that the CEO, or the CFO or the CIO will handle risk as part of their portfolio of results. Loss avoidance is usually the priority when risk is handled in this manner. Addressing opportunities however requires a bit more than just loss avoidance, it has to address the uncertainties an organization has to deal with. And today no uncertainty is more certain than the fact that information technology can create risks that can put an organization’s reputation on the line and end up destroying critical assets that the business requires to manage day to day operations. To address this Information Security has evolved today into a body of knowledge that has many different contributors providing vital insights into the benefits of information controls and technology standards. Unfortunately all of this activity has not still culminated in a unifying principle that would integrate the plenitude of options available today, including multiple standards, many control frameworks and divergent methodologies. Practitioners of information security as a profession are therefore still seeking a disciplined approach that could contextually place the available offerings to help them identify and apply the right answers to their most pressing concerns.

To understand this situation better, it is important to realize the nature of information itself and it's role in enabling those seeking to manage business priorities. A business comes into existence to transform resources into results with the objective of exchanging these results for revenue. Information itself is derived from this transactional nature of business. Hence what is important to a business is not the data collected during transactions but in how this data can be used to understand and manage business priorities, whether is managing cash flow, or fulfilling customer orders. Business transactions by their very nature are dependent on organizational infrastructure. Information is captured, processed and delivered using technology infrastructure in the form of systems and people. Internal processes combine these systems and people into the shared services that constitute front office and back office units that have to work in concert to deliver the desired business results. As such Information and Technology have a vital role to play in enabling cost efficient, and increasingly time efficient business transaction processing. Any downtime caused by disruption in the underlying technology or the processes or the subversion of the information delivered by these technologies or processes result in a cumulative impact that can lead to losses that are either critical or material to an organization. Critical when the nature of these disruptions lead to a loss of trust in customers or other vital stakeholders in the dependability of the business infrastructure as it then threatens the survival of the organization. Material when it leads to substantive losses caused by the dissolution of assets represented by accumulated transactional information, as it would require substantial financial resources to replace or repair these losses.

Before a company can manage it's risks, it has to know what risks it has to manage. And to understand these risks, it is important to consider strategic business scenarios. For example a key scenario for a CEO could be a question such as What happens if we add a new business capability such as an e-Business portal? How will it impact our existing ability to deliver results is as important a consideration as asking the other side of the question, which is what happens if we don't add the business capability? Will our customers shift to a competitor because they prefer the added value the new capabilities will bring to bear on their transactions? It is in considering these scenarios that the relationship between risk and opportunity becomes clear to both the CEO who has to drive the required organizational changes and the IT division that will be tasked with delivering the changes to systems to enable the organizational changes. Therefore both the leaders of an organization who will create the driving vision as well as the managers who will implement the desired changes need to meet on common ground. At OISSG we have chosen to focus on Enterprise Risk Management to facilitate IT as a business enabler in delivering new business capabilities. We have chosen to deliver this using a disciplined approach that step by step identifies and

eliminates business inhibitors related to the risks that accrue from implementing information related technologies.

This summarizes the vision that led to the development of ISSAF. We consider assessment as the unifying idea to integrate three separate but related set of risk management activities viz interviewing, observation and testing. We have chosen assessment as a process instead of auditing because auditing will require an established body to promulgate the underlying standards. As an open organization that have not sought such affiliations to date, we have not been restricted in choosing an approach that integrates exhaustive penetration testing with accepted business continuity practices, and seeks to validate the alignment of business policies to internal IT realities. All of this is delivered through a step by step engagement management approach to facilitate the assessment process within an organization seeking to secure their information assets.

I think the point to risk management is not to try and operate your business in a risk-free environment. It's to tip the scale to your advantage. So it becomes strategic rather than just defensive as said by Peter G. M. Cox, CFO, United Grain Growers Ltd.

2 ABOUT ISSAF

2.1 PREFACE

The Information System Security Assessment Framework (ISSAF) is a peer reviewed structured framework that categorizes information system security assessment into various domains & details specific evaluation or testing criteria for each of these domains. It aims to provide field inputs on security assessment that reflect real life scenarios. ISSAF should primarily be used to fulfill an organization's security assessment requirements and may additionally be used as a reference for meeting other information security needs. ISSAF includes the crucial facet of security processes and, their assessment and hardening to get a complete picture of the vulnerabilities that might exists.

The information in ISSAF is organized into well defined evaluation criteria, each of which has been reviewed by subject matter experts in that domain. These evaluation criteria include:

- A description of the evaluation criteria.
- Its aims & objectives
- The pre-requisites for conducting the evaluations
- The process for the evaluation
- Displays the expected results
- Recommended countermeasures
- References to external documents

Overall framework is large, we chose to provide as much information as possible on the assumption that it would be easier for users to delete material rather than develop it. The Information System Security Assessment Framework (ISSAF) is an leaving document that will be expanded, amended and updated in future.

2.1.1 What are the Objectives of ISSAF?

- To act as an end-to-end reference document for security assessment
- To standardize the Information System Security Assessment process
- To set the minimal level of acceptable process
- To provide a baseline on which an assessment can (or should) be performed
- To asses safeguards deployed against unauthorized access

- To act as a reference for information security implementation
- To strengthen existing security processes and technology

2.1.2 What are the Goals of ISSAF?

The goal of the ISSAF is to provide a single point of reference for security assessment. It is a reference that is closely aligned with real world security assessment issues and that is a value proposition for businesses. To this aim the ISSAF has the following high-level agenda:

- Evaluate the organizations information security policies & processes and ensure that they meet industry requirements and do not violate any applicable laws & regulations.
- Identify critical information systems infrastructure required for the organizations' business processes and evaluate their security
- Conduct vulnerability assessments & penetration tests to highlight system vulnerabilities and thereby identifying weaknesses in systems, networks and applications.
- Evaluate controls applied to various security domains by:
    - Finding mis-configurations and rectifying them
    - Identifying risks related to technologies and addressing them
    - Identifying risks within people or business processes and addressing them
    - Strengthening existing processes and technologies
- Prioritize assessment activities as per system criticality, testing expenses, and potential benefits.
- Educate people on performing security assessments
- Educate people on securing systems, networks and applications
- Provide information on
    - The review of logging, monitoring & auditing processes
    - The building and review of Disaster Recovery Plan
    - The review of outsourcing security concerns
- Compliance to Legal & Regulatory Standards
- Create Security Awareness
- Effective Management of Security Assessment Projects
- Guarding against social engineering exploitation
- Physical security control review

This approach is based on using the shortest path required to achieve one's goal by finding flaws that can be exploited efficiently, with the minimal effort. The goal of this framework is to give completeness and accuracy, efficiency to security assessments.

2.1.3 Why we had come up with ISSAF?

After working on many information assurance projects, the lack of a comprehensive framework that provides information security assurance through performing standardized vulnerability assessment, penetration testing, security assessment and security audit, was felt.

While there are a few information security assessment standards, methodologies and frameworks that talk about what areas of security must be considered, they do not contain specifics on HOW and WHY existing security measures should be assessed, nor do they recommend controls to safeguard them.

ISSAF is a comprehensive and in-depth framework that helps avoid the risk inherent in narrow or ineffective security assessment methodologies. In ISSAF we have tried to define an information system security assessment methodology that is more comprehensive than other assessment frameworks, it seeks to mitigate the inherent risk in the security assessment process itself. It helps us understand the business risks that we face in performing our daily operations. The threats, vulnerabilities, and potential exposures that affect our organizations are too huge to be ignored.

At this particular time it is not the answer to every question or situation, but we are committed to continuous improvement by improving current topics and adding new topics.

ISSAF has laid the foundation; now it's your turn to benefit from it, whether you use it as is or tailor the materials to suit your organization needs. Welcome to ISSAF, we hope you will find it useful.

2.2 TARGET AUDIENCE

This framework is aimed at a wide spectrum of audiences that include:

- Internal and External Vulnerability Assessors, Penetration Testers, Security Auditors and Security Assessors
- Professionals responsible for perimeter security
- Security engineers and consultants
- Security assessment project managers
- System, Network and Web Security Administrators
- Technical and Functional Managers
- Information systems staff responsible for information security

2.3 TEAM

Authors

Balwant Rathore	Mark Brunner	Miguel Dilaj
Omar Herrera	Piero Brunati	Rama K Subramaniam
Subash Raman	Umesh Chavan	

Key Contributors

Arturo "Buanzo" Busleiman	Christian Martorella	Dieter Sarrazyn
Hernán Marcelo Racciatti	Karmil Asgarally	

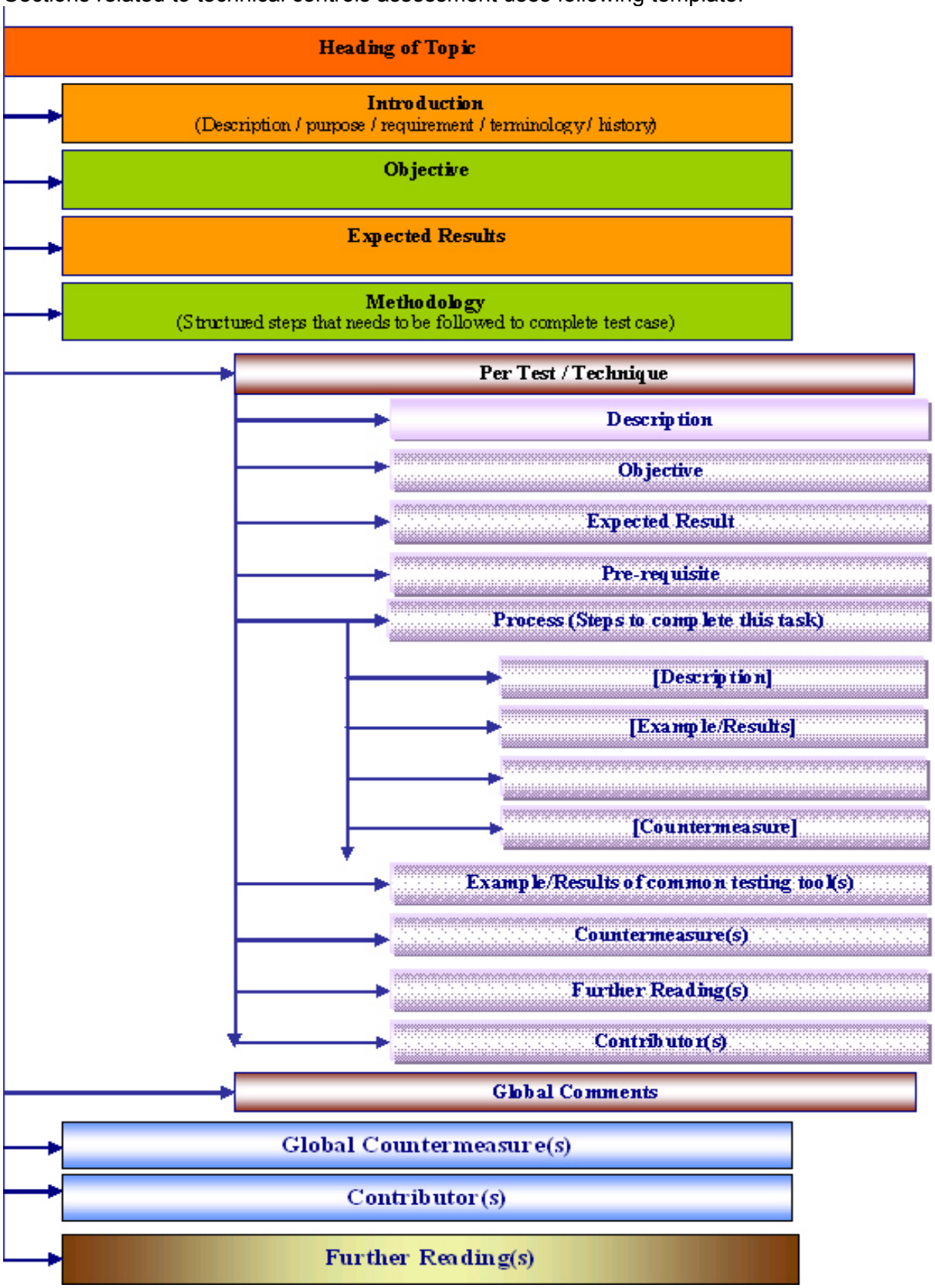
Contributors

Andres Riancho	Anish Mohammed	Arshad Husain
Bernardo Reino	Bob Johnston	Clement Dupuis
David Stern	Dhanya Thakkar	Dharmesh Mehta
Diego San Esteban	Dragos Ruiu	Frank Sadowski
Gabriel O. Zabal	Galde Edgar	Gareth Davies
Hamid kashfi	Hari Prasad	Hiten Desai
Jayesh Thakur	Jeremy Martin	Joel Weise
Kalpesh Doshi	Kartikeya Puri	Krishnakant Duggirala
Laurent Porracchia	Major Gajendra Singh	Niels Poulsen
Niloufer Tamboly	Oliver Karow	Oscar Marín
Param Singh	Pieter Danhieux	Rahul Kashyap
Rajendra Armal	Richard Gayle	Richard Zaluski
Rocky Heckman	Ross Patel	S. Saravanan
Salman Ashraf	Saman Ghannadzadeh	Samir Pawaskar
Sandhya Kameshra	Soorendrana	Travis Schack
Vicente Aguilera	Vicente Diaz	Vinay Tiwari
Viraf Hathiram		

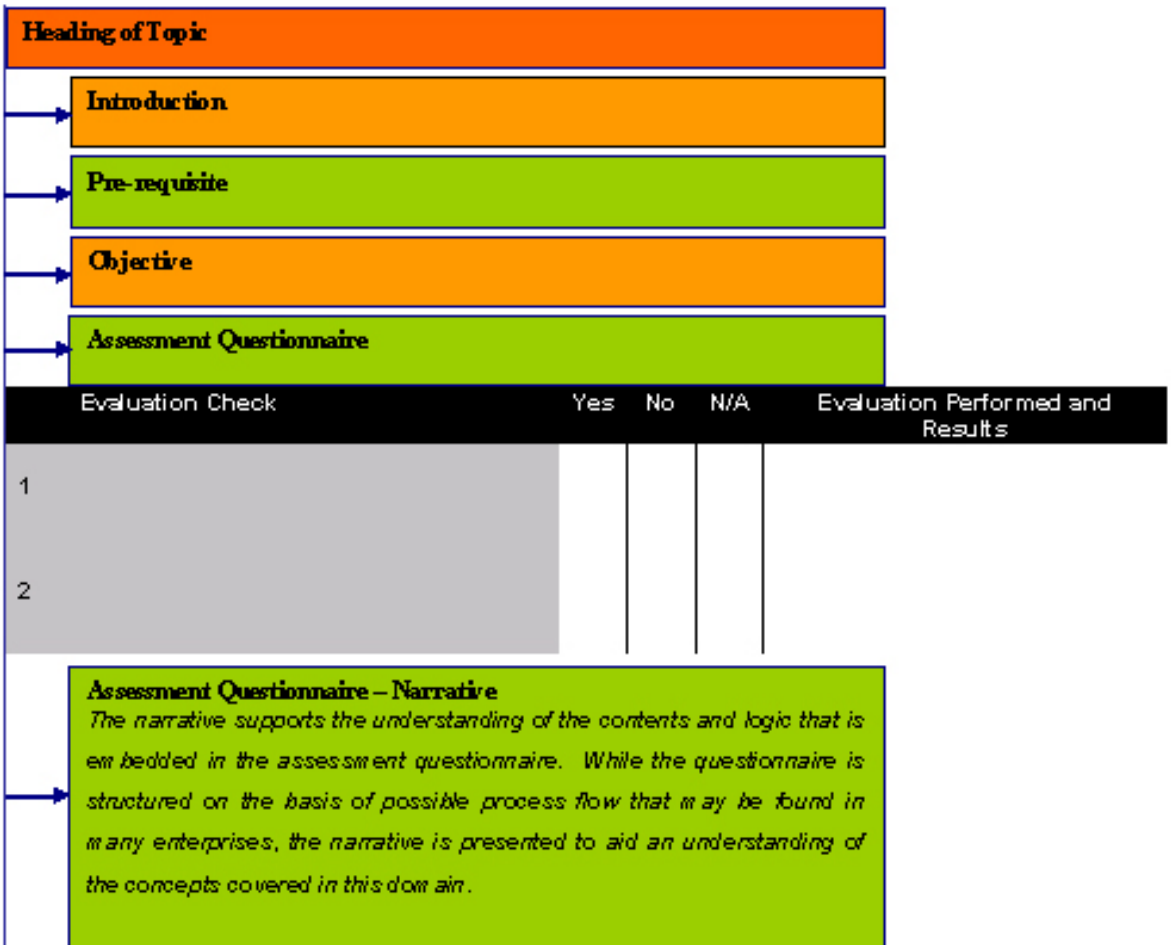
A-Z, Ascending Order

2.4 DOCUMENT STRUCTURE

Sections related to technical controls assessment uses following template:



Sections related to policies & processes evaluation uses following template:



2.5 DISCLAIMER

While all possible precautions have been taken to ensure accuracy during the development of the Information System Security Assessment Framework (ISSAF), also referred to as ISSAF, the Open Information System Security Group (OISSG) assumes no responsibility for any damages, errors or downtime resulting or caused by the use of the information contained herein.

OISSG does not warrant or assume any legal liability or responsibility for the completeness, usefulness, accuracy of the information presented in this document.

OISSG will not be responsible for any damage, malfunction, downtime, or other errors that might result from the usage of this document.

2.6 LICENSING

- Any individual/organization is granted unlimited distribution of ISSAF in whole or any part of it, provided the copyright is included in the document
- We impose no restrictions to any individual or organization for practicing ISSAF
- We impose no restrictions to any individual or organization to develop products based on it
- We impose no restrictions to any individual or organization that uses ISSAF for commercial purposes, provided the appropriate copyright is included in the document
- Tools developed for ISSAF assessment are released under GNU GPL, unless mentioned (http://www.opensource.org/licenses/gpl-license.html)

Should you have any question on our licensing, please do reach us at licensing@oissg.org

3 THE FRAMEWORK

"Begin at the beginning said the king gravely, and go on till you reach the end, then stop"

-Lewis Carroll

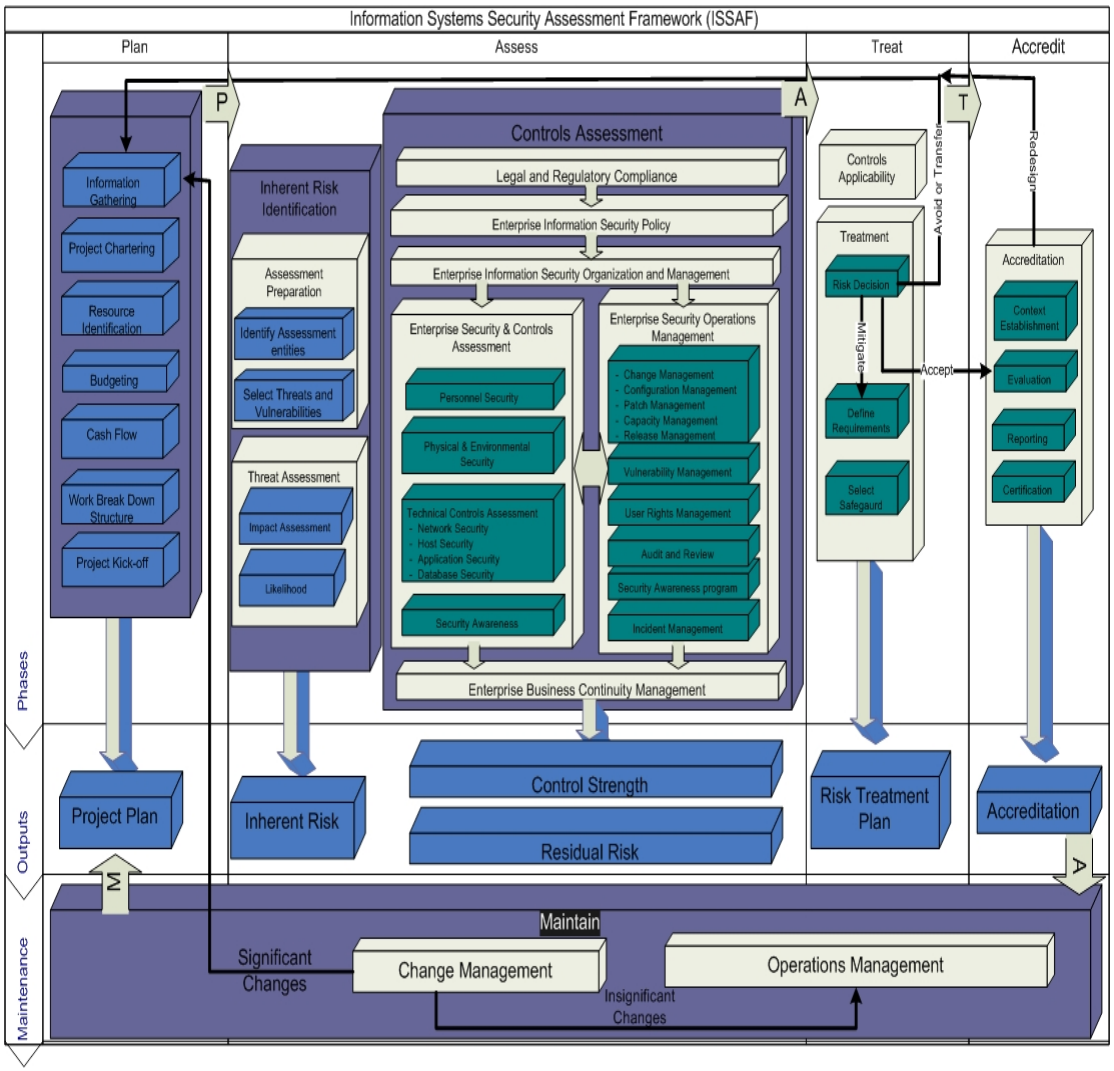
Who is responsible for ensuring security? Who authorizes the decisions that have to be made in this regard? Who has to be consulted to ensure all the bases are covered? Who has to be kept informed to ensure that the organization copes with the resulting changes?

Security can be an immediate priority if the corporate website has been vandalized or a logic bomb destroys crucial corporate records, or the corporate email system was responsible for promulgating a known virus or a fraud based on subversion of automated processes was uncovered after the fact. In these instances the above questions become the basis for initiating a program that seeks to address the issues that have surfaced. However in instances that do not present a compelling need for change, there can also be issues that can seriously impact the organization's long term chances of survival. Information that is leaked to competitors such as blueprints or estimates for a tender may not be as clear and a present danger as the above instances, but they can seriously erode the company's chances of gaining a crucial advantage in the marketplace. Similarly, lack of controls in Accounts payable systems or payroll may not result in immediate fraud, but they can set the stage for an interested party to manipulate the data or the underlying vouching mechanisms to subvert the system to meet their own ends. It could be as simple as falsifying attendance records and it could be as financially deleterious as removing evidence of stock returns from inventory records. What all of these instances cite however is the need to understand how the integrity or the lack thereof in information records can potentially affect the viability of the organization. These records cost money to capture, to transmit, to store, to process and to report, and these investments. Once material to the balance sheet, they should become drivers for further investments to ensure the safety and security of the underlying infrastructure and related operations.

What is therefore needed is a systematic approach to helping a concerned party take up security as an initiative, make a compelling business case if required for investing in this initiative, go about identifying the order in which activities need to be carried

out step by step, and then manage these activities one by one until a reasonable level of assurance can be provided to management regarding the security of their information assets. ISSAF provides a four phase model that structures the management of security initiatives and ensures the viability of the engagement by providing the requisite know-how in the form of bite-sized work packages (referred to as activities) that can be assigned to individuals within the project team.

The four phases respectively are Planning, Assessment, Treatment, and Accreditation. Each of these phases has specific work packages that are generic to all organizations regardless of their size, their specific key result areas, and their geographical siting. Through the sequencing of their respective work packages, these phases focus on delivering specific results, be it a deliverable or a desired state of affairs. The outputs of these phases are then followed by operational activities designed to integrate the deliverable or to maintain the achieved state, feasibly and effectively.



3.1 PHASE I – PLANNING

3.1.1 Information Gathering

Security initiatives normally do not have the same set of triggering events within organizations. In some instances a change in management could result in a focus on security as a critical requirement. In other instances it could be triggered by the realization of losses caused by systems outage. In other instances it could be the result of a proactive approach by managers concerned about the outcome of their investment. Whatever be the triggering event, the fact remains that information has to be gathered to substantiate the underlying concern. If an auditor is concerned about the retention period of system activity logs, he cannot make a business case unless he is able to substantiate the need for backing up activity logs with the specific non repudiation based legal or compliance requirements that he is basing his requirements upon. If there is a business dependency on a particular information service such as email, it is incumbent upon the process owner of the concerned business function to identify the potential losses that could accrue from an hour, a day, or a week of systems outage caused by a virus or other such likely threats. Otherwise it would be impossible for those responsible for authorizing the requisite investments to make an informed decision in this regard.

Information gathering therefore seeks to assemble a complete picture of the information technology infrastructure to serve as the basis for the next phase, namely risk assessment.

ISSAF has assembled a set of questions that can serve as the basis for this information gathering in a document titled ISSAF – Information Gathering Questionnaire. It is recommended that the security practitioner collates this information and analyze their findings prior to moving to the next stage namely, preparing the business case to align management of security as a priority.

3.1.2 Project Chartering

Unless an executive sponsor is available to support the funding of the project, the initiative is likely to die stillborn. This is the fundamental reality of corporate life, and this condition has to be respected by security practitioners. Hence the quest for project funding should begin by first identifying who is likely to be interested in sponsoring the project and then identifying the key result areas that are likely to motivate their self interest in promoting this initiative. We recommend identifying the

critical success factors (desired outcomes) and then mapping them to all key internal business processes including revenue and expense cycles, as a starting step. This will facilitate the identification of which business processes are most critical to the business, and this in turn will help prioritize which systems are critical to these processes. An example critical success factor to process mapping has been included to clarify this concept further. Based on this analysis, it is recommended to fill out the sample Project Charter template to initiate discussions with the proposed project sponsor(s) and to document their expectations in this regard. Once the project charter is completed, use this document to obtain an internal signoff to ensure that project planning proceeds on the documented assumptions.

3.1.3 Resource Identification

Using the project charter, it is possible to identify at a high level the resources that are likely to be required to deliver the required results. Resources can range from people, products, processes, tools, knowledge and political support. The objective of this activity is to research the type and potential costs of the resources that will be required to execute this project. Normally security initiatives are based on specific project charters, such as hiring an external vendor to implement a secure firewall, or hiring an auditor to identify control weaknesses in the enterprise systems. The process of meeting and discussing the proposed initiatives with vendors can help clarify the key cost areas likely to result from an implementation of the proposed initiatives. The key objective for this phase is to understand whether this project is feasible from a financial and human resourcing standpoint. At this point it is likely that the project charter may require further revision to narrow or broaden the scope based on the correction or validation of the many assumptions that would have driven the definition of the earlier charter. This is quite normal and should be treated as a value added outcome of this particular activity. The first output of the resource identification phase is the preparation of an RFP that is issued to vendors that will supply the required resources. Guidelines for preparing this RFP as well as a sample structure is provided in the appendices for further reference.

3.1.4 Budgeting

Next a budget is prepared that identifies investments and subsequent operating costs to establish whether the required funding is likely to be feasible from an overall business perspective. The budget should consist of the following supporting schedules in addition to the actual project budget to help the organization's financial

team assess and/or integrate the project funding into the annual capital/operations budgets.

3.1.5 Cash flow – pro forma preparation

Its important to prepare the following:

- Income statement (Profit & Loss)
- Balance sheet

Unless these pro forma statements are prepared the financial team will be unable to do basic financial analysis such as the preparation of depreciation/amortization schedules, identify the increase in operating costs caused by new hires, training needs, etc.

3.1.6 Work breakdown structure

A work breakdown structure (WBS) essentially creates a framework that groups and integrates the individual work packages that will work in concert to deliver the project results. Work packages are a collection of related tasks usually carried out by an integral unit, such as a team or an individual or through automation. This structure is composed using a hierarchical outline that progressively breaks down activities into smaller and smaller chunks until the final chunk results in an assignable work package.

3.1.7 Project kick-off

The primary purpose of the Project Kick-off is to formally appoint the project manager. This ensures that the project manager has the necessary visibility and functional authority to make the decisions required to deliver the defined project results.

The WBS is used to kick off the project, and subsequent discussions are used to generate a sense of ownership within the team members that have been pulled together for this project. The key result of the project kick-off is the Responsibility, Accreditation, Consultation, Information (RACI) matrix or chart, which designates who is Responsible, who will Accredit the deliverables, who has to be Consulted, and who has to be kept Informed throughout the project. The RACI chart then becomes the key document that will be used to manage all further project communications.

Output – Project Plan

Based on the above results, the final project plan is prepared, integrating schedules and resources to the work breakdown structures. This initial project plan will then serve as the baseline to monitor and control the actual execution of the projected results and outcomes.

Please keep in mind that the above planning phase was designed to be generic and can be used both to deal with a unit task such as the purchase and implementation of a new firewall as well as for re-engineering the entire corporate IT architecture if required.

Note

The following section, Risk Assessment, is designed to act as a pre-project audit and provides a complete structure for assessing the state of information security controls. It is designed to report the state of internal controls to management, who can then use the findings and recommendations to assess and remediate their overall risk exposure. Part of this remediation effort may result in the original scope of the project being modified to incorporate the risk treatments required to mitigate, reduce or transfer the identified risks.

3.2 PHASE II – ASSESSMENT

The Assessment Phase provides a holistic approach to assessing Information Security Risks to an enterprise. This phase advocates approaching Information Security Risk assessments from the perspective of the enterprise business objectives and associated risks. This would ensure the alignment of the enterprise business risks with the risks in relation to the nature and extent of usage of Information Technology for the achievement of the business objectives of an enterprise.

The framework commences with an Enterprise Risk Assessment of the business which helps identify the inherent risk to the business as a whole. This provides focus to the nature of risks being considered for the assessment of Information Security. The inherent risks identified during the assessment are further used to identify specific risks that stem from the nature and extent of usage of Information Technology in the enterprise. The identified Information Technology risks are then used to formulate the security and control requirements of the enterprise.

Given the costs of implementing and maintaining security and controls in the Information Technology environment, an enterprise would consider the cost benefit of any security implementation by measuring the cost of control against the impact of not having such a control. In instances where the cost of control exceeds the impact of the risk both in terms of effort and value, the enterprise may choose not to implement such security or control mechanisms. Alternatively, the insignificance of the impact of risks may also prompt an enterprise not to implement any specific controls to mitigate these risks. Such risks are considered as 'Residual Risks'

The assessment phase provides an overview of the ISSAF risk assessment process and addresses the different components involved. The assessment phase is divided into two categories:

1. Inherent Risk Identification
2. Controls Assessment.

In the course of inherent risk identification all the relevant risks to business are identified based on impact and likelihood of threat occurring irrespective of controls. After obtaining the inherent risk of an assessment entity, evaluation of controls is performed to identify the residual risk for the assessment entity.

The following tasks are carried out during the assessment process:

3.2.1 Inherent Risk Assessment

3.2.1.1 Assessment Preparation

The following activities are performed:

- Identification of Assessment entities – These could be processes, assets, facilities etc. The assessment entities constitute the basis for identifying applicable assessment parameters, threats, etc to the entities.
- Identify threats and Vulnerabilities – The various vulnerabilities of the selected or identified entities for assessment are documented. Next, the threats that could exploit a single or multiple vulnerabilities are identified and listed. These threats constitute the risks for the entities. These risks can be repeatable to an entity.

For more information we suggest you read the ISSAF Risk Management Tool documentation.

3.2.1.2 THREAT ASSESSMENT

The following activities are performed:

- Impact Assessment – The impact to the business of an organization of a threat being realized against an asset is measured or estimated. This is done individually for each asset entity, and does not consider risk mitigating factors. It is a measure of raw risk.. The assessor can choose to average or sum the assessment parameter values for mathematical or logical reasons.
- Likelihood Assessment – Here the probability of occurrence of the threat for the chosen assessment entity is measured or estimated.

The resulting totals from the above two tasks is the inherent risk for the entity being assessed.

3.2.2 Controls Assessment

Compensating controls may be in place to reduce or mitigate risks. These factors need to be accounted for in an accurate risk assessment. After obtaining the inherent risk of an assessment entity, evaluation of controls is performed to identify the amount of risk reduction they offer, and the residual risk that remains for the assessment entity.

During this stage the assessor may select the controls from the ISSAF or other controls. The idea here is to identify that the control selection is adequate and the control's existence and contribution is acceptable for the risk decision.

The most important aspect of control evaluation is to evaluate the control against the assessment parameter to verify that it is contributing to reduce the impact of a given assessment parameter to an acceptable level.

The result of this task is the residual risk for the assessment entity. The various control areas for assessment entities available to the assessor for selection from ISSAF are given below.

Evaluation of Legal and Regulatory Compliance

A review of the legal and regulatory requirements impacting the enterprise is essential to ensure that the enterprise is compliant with any laws and regulations that are applicable to the Information Technology infrastructure of the enterprise.

Evaluation of Enterprise Information Security Policy

Upon commencing an Enterprise Security Assessment one of the first tasks would be to understand and evaluate the Information Security Policy of the enterprise. The Information Security Policy is a reflection of the management's intent and approach to Information Security and epitomizes the extent and the nature of Information Security implemented within the Enterprise. A review of the enterprise's Information Security Policy is necessary to gain a comprehensive understanding of the approach to implementing and maintaining the Information Security posture of the organization.

Evaluation of Enterprise Information Security Organization and Management

Subsequent to the Enterprise Risk Assessment and the review of the Information Security Policy, a review of the Information Security Organization and Management is performed. This comprises of a review of the organization of the security functions, relevant roles and responsibilities and management responsibilities amongst other areas.

Having obtained an understanding of the risks applicable to the technology infrastructure of the enterprise, the enterprise's approach to managing security as stated in its Information Security policy and the allocation of security roles and responsibilities, it would be logical to assess the specific security infrastructure and operational controls implemented within the enterprise to mitigate the identified Information Technology risks.

This stage of the Security Risk Assessment Framework comprises of the following:

- Enterprise Security and Controls Assessment
- Operations Management Assessment

Assessment of Enterprise Information Systems Security and Controls

This stage comprises of a review of the following:

- Physical and Environmental Security
- Technical Controls
  - Network Security
  - Host Security
  - Application Security
  - Database security
- Evaluation of Security Awareness by:

- Interviews
- Observation
- Structured walk through
- Social Engineering

Evaluation of Enterprise Security Operations Management

This review is performed in conjunction with the Enterprise Security and Controls Assessment, to gain an understanding of the risks and controls of the security operations processes. This would be comprised of the assessment of the following operational areas:

- Capacity Management
- Vulnerability Management
- Release Management
  - Patch Management
  - Configuration Management
  - Change Management
- Enterprise Incident Management
  - Logging
  - Monitoring
  - Security Incident Management
  - Operation Event Management
- User Management
- Certification and Accreditation

Evaluation of Enterprise Business Continuity Management

An evaluation of Enterprise Business Continuity Management capabilities is essential to assess adequacy of the readiness of the enterprise in ensuring availability of the Information Technology infrastructure. This review is complemented with a review of Business Continuity processes of the enterprise to ensure that in the event of a disaster the enterprise is adequately prepared to continue core business operations until such time that normal operations are completely restored.

Manage Residual Risks

As stated earlier, the risks not covered by the enterprise's security and controls implementations are categorized as Residual Risks. Given the volatile nature of business in general and the ever changing risks applicable to general industry and information technology in particular, it is important to regularly review the residual risks not addressed by an enterprise's Information Security Management Framework. This is required to ensure that risks that were previously categorized as residual are appropriately escalated and managed as their relevance and importance to the enterprise changes.

A review of the process for management of Residual Risks is performed to ensure that residual risks are regularly reviewed and reassessed to ensure that their status of criticality has not changed, and that the need for compensating controls in these areas has not increased.
We suggest you read the ISSAF document for details of these controls.

3.3 PHASE III - TREATMENT

Risk treatment provides a platform for taking a decision for the residual risks, through the selection of safeguards, development of implementation plans, and providing accurate documentation for the implementation of, and decision making process. Risk decision is an important stage where executive management and other stakeholders review your documentation and make a decision to accept, mitigate, transfer or avoid the risk. Once this decision is made, plans for implementing the outcome are made, and approvals are sought for budgetary requirements, for project planning, for implementation and for change management.

Another important task in the risk treatment process is that when a decision to mitigate a risk is taken, the selection of controls to mitigate the risk is selected and a project plan to implement the controls is developed.

We suggest you use the Risk Treatment Plan template in the ISSAF for this process.

3.4 PHASE IV - ACCREDITATION

The process of accreditation involves assessing the controls that have been selected for implementation under the scope for certification. The assessment results determine the accreditation of the ISSAF certification to an organization.

The assessment process will include a detailed plan that will be agreed upon with the entity being assessed. The assessment will be conducted by the OISSG nominated ISSAF auditors and the results will be evaluated by the OISSG certifying authority.

OISSG provides a formal certification on ISSAF compliance. This certification is available through certifying agencies authorized by OISSG.

3.4.1 Context Establishment

- Contact OISSG / Authorized Certification Bodies

  OISSG can be contacted on acreditation@oissg.org for details regarding the authorized accredited agencies that are able to certify you for your chosen locations. OISSG would require the following details for the same:

  - Name of the Organization
  - Number of Employees of Organizations
  - Type of Organization (Banking / Technology / Manufacturing /Energy / Telecom / Others)
  - Number of Locations
  - Further information may be requested by the OISSG coordinator

- Auditor Assignment

Based on the inputs provided, OISSG would facilitate the choice of authorized accreditation agencies. The selection of accreditation agency is done on the basis of their experience in the accreditation process in various industry verticals & size of assignments that the auditors have handled. The auditors are carefully selected based on the skill levels required for the complexity of your environment, business knowledge, functional knowledge and project management expertise. Once the accreditation agency and auditors are selected, they will visit your organization for evaluation purposes. OISSG recommends that a project manager be appointed from within the business who will also serve as a single point of contact. This project manager should have sufficient operating knowledge of the organizational processes and should have enough authority to approach departments and co-ordinate meetings with the visiting auditors. The project manager should serve as the only interface between the accrediting agency and the organization.

3.4.2 Evaluation

After the initiation is done, OISSG auditors would approach the organization for further discussions regarding the scope and coverage of the accreditation process. The scoping should highlight what specific areas under ISSAF need to be covered

under the assessment. After the scoping exercise the OISSG auditors would start assessment of the organization based on ISSAF.

The auditors would assess the organizations' information security processes based on the detailed controls / methodology defined in ISSAF

3.4.3 Reporting

Auditors would then prepare a draft report based on their findings and present it to the senior management of the organization. This report highlights the level of compliance that the organization has achieved vis-à-vis ISSAF. It also consists a detailed breakdown of areas where non-compliances were found along with the severity of such non-compliance. Management feedback on the non-compliances found is considered before deciding on further course of action.

3.4.4 Certification

Based on the degree of compliance, a certification of ISSAF compliance is issued. Any outstanding issue in the form of recommendations for further action will be checked in subsequent ISSAF reviews & subject to closure of all outstanding items from previous ISSAF reviews, a recertification will be granted every two years.

However if the issues are fairly significant the certification is denied stating adequate results as to what are the significant issues. All the significant issues need to be closed out prior to attempting a fresh certification.

3.5 PHASE V – MAINTENANCE

ISSAF certified organizations will be required to demonstrate compliance to the ISSAF accreditation on a continuing basis. To ensure this, OISSG will conduct regularly scheduled compliance assessments/reviews. The frequency for this review will be based on the size of the organization and the accreditation scope.

4 ENGAGEMENT MANAGEMENT

An engagement is grouping of activities that, when put together, achieve an objective and a goal. An engagement always has a recognizable start and an end. This document provides an overview on engagement management for security assessment engagements.

The security-assessment engagement entails numerous tasks and involves several parties. Such engagement requires engagement planning from start and management activity throughout the development of the engagement. This section describes the engagement management aspects of a security assessment engagement.

The following guidelines can be directly used for providing engagement management plan to the client.

4.1 ENGAGEMENT EXECUTIVE OVERVIEW

(Optional) The executive summary provides a summary of the engagement definition document. In many cases, this is a PowerPoint presentation. If it is, then a reference to the external document can be included. This section contains high-level explanation of the engagement objectives, scope, assumptions, risks, costs, timeline, approach, and organisation. (Remove this comment section from final document.)

Describe the background and context for the engagement and why it is being undertaken. Speak to the business value of the work being performed. Place adequate information here to ensure appropriate coverage of the rest of the sections in the engagement definition. (Remove this comment section from final document.)

4.2 OBJECTIVE

Objectives are statements to describe what a engagement will achieve and deliver. Objectives should be "SMART": Specific, Measurable, Achievable, Realistic, and Time-Based. To be specific and concrete, objectives should be based on deliverables (outcomes). The completion of an objective should be evident through the creation of one or more deliverables. If the statement is at a high level and does not imply the creation of a deliverable, it may be a goal instead. If the statement is

too low-level and describes features and functions, then it may be a requirement statement instead. (Remove this comment section from final document.)

The XXX engagement will meet the following objectives:

- Objective #1
- Objective #2
- Objective #3

Expected Result[s]

Provide a brief description of the deliverable. *A sample deliverable report can also be attached.*

The XXX engagement will produce the following deliverables:

- Deliverable #1
- Deliverable #1
- Deliverable #1

4.3 APPROACH

Illustrate an over view of the methodology used for security assessment engagement. Generally the phases involved in typical security assessment engagement are:

- Planning and Preparation (Scoping & Logistics)
- Assessment (Fieldwork)
- Reporting (Conclusion / Results)

4.4 ENGAGEMENT SCOPE

In this section, you should clearly define the logical boundaries of your engagement. Scope statements are used to define what is within the boundaries of the engagement and what is outside those boundaries. Examples of areas that could be examined are data, processes, applications, or business areas. The following information can be helpful:

- The types of deliverables that are in and out of scope (Business Requirements, Current State Assessment)
- The major life-cycle processes that are in and out of scope (analysis, design, testing)
- The nature and sensitivity of data that is in and out of scope (financial, sales, employee)

- The data sources (or databases) that are in and out of scope (Billing, General Ledger, Payroll)
- The organisations / departments that are in and out of scope (Human Resources, Manufacturing, vendors)
- The major functionality that is in and out of scope (decision support, data entry, management reporting)

(Remove this comment section from final document.)

The scope of this engagement includes and excludes the following items.

In scope:

- ……
- ……
- ……
- ……

Out of scope:

- ……
- ……
- ……
- ……

4.5 ENGAGEMENT KICKOFF MEETING (INTERNAL)

As you win an engagement, Engagement Manager shall call a Engagement Kickoff Meeting. Following are some points shall be discussed in this meet:

- Quick look at lesson learned in previous engagement
  - Highlight challenges/problems and design strategy to resolve them
- Declare Single Point of Contact for Engagement
- Form Engagement Team and divide their tasks
- Set deadlines on divided tasks to members responsible for Engagement Execution
- Process Administrative Tasks
  - Visa Processing (If required)
  - Travel Management
  - Check Passport status and Important papers with candidates
  - Check Emigration Check Not Required (ECNR) on passport of candidates
- Availability of Tools (Commercial/Freeware)

- Efficient delivery capabilities of promised tasks in proposal
- Any help needed for delivery
  - Infrastructure for testing
  - Training
  - Backup infrastructure
- Inform Technical Infrastructure Management department about IP Addresses
- Engagement manager or assigned team member shall give minutes of meetings to everybody

4.6 COMMUNICATIONS PLAN

Name / Engagement Role	*Numbers*	*Email*
INSERT CONTACT LIST		

Standard/Scheduled Communications

The Assessment Team Program/Engagement Manager will initiate the following engagement meetings through the engagement life cycle:

On-site at –CUSTOMER NAME-:

- Mid-Planning and End-of-Planning Meetings
- Engagement Kick-Off Meeting
- Progress Meetings (frequency and method to be determined by the CUSTOMER NAME). A meeting agenda will be distributed to attendees prior to the meeting and meeting minutes will be distributed after the meeting.
- Engagement End (Debrief) Meeting

On a weekly basis, Assessment Engagement Management will provide status to all engagement stakeholders via the CUSTOMER NAME engagement web site (to be developed). All engagement related, the Engagement Manager would post

documents developed during the week each Friday. The engagement web site is a valuable tool that historically archives all documents, making them easily, and readily available for baseline reviews.

It is imperative for all managers to be aware of issues that their teams are managing / experiencing; therefore, all engagement communications will follow a "chain of command" structure. Please refer to the Engagement Org Chart for communication checkpoints.

- Explain your understanding of client's requirement
- Discuss dates of assessment offshore/onsite
- Request client to issue an Invitation letter to embassy by the name of test team members (If required)
- Update client for source IP addresses used for assessment

4.7 ENGAGEMENT KICKOFF DISCUSSION WITH CLIENT

Points to discuss

- Identify access points and number of devices needs to be tested
- Deliverables
    - Executive Summary
    - Vulnerability Summary
    - Detailed Test results with countermeasure to safeguard against vulnerabilities
- Single Point of Contact from both end
- Team Introduction
- Engagement start and end date
- Working days/hrs
- Internet Access during onsite assessment
- Site location and contact numbers
- Update client about source IP addresses used for testing
- Make sure access to service is open in firewall from given source IP address to perform assessment.
- Make sure access to service is given from your company /ISP Router and Firewall

4.8 SAMPLE STATUS REPORT

From:

Subj: Status Report for

Period:

If appropriate, provide background information for this report. You may wish to include the following information in your comments:
Origins of the engagement; business reason for its initiation; anticipated value to the customer; and engagemented increase to revenue or decrease to cost.
Engagement scope and objective

Summary:

Total Hours Used:

Identify overall engagement status and provide a few key bullet points highlighting planned vs. actual aspects of each relevant topic:

Engagement Status:

☐ GREEN ☐ YELLOW☐ RED

NOTE: Status Reports will be completed weekly. Do not be hesitant to provide a yellow or red status; this is a tool to alert management to potential issues.

- Green – Engagement is proceeding on plan with no major showstoppers.
- Yellow – Engagement has tasks that "may" impact engagement completion.
- Red – Major issues exist with required tasks that are needed to complete the engagement. Management assistance is needed immediately.

Engagement Schedule

Indicate the current planned completion date for all major tasks & milestones through completion of the engagement.

TASK/EVENT ***PLANNED DATE***

Major Accomplishments: (Any significant completed tasks)

Highlight major accomplishments achieved during the reported status period. Identify focus of current engagement work and any additional information on completed tasks.

Outstanding Issues or delinquent items

Identify appropriate critical issues that threaten the success of this engagement. Provide further information regarding background and action plans for addressing the issue.

ISSUE	***ACTION PLAN***

Next Steps/Upcoming Events - (planned tasks for the next reporting period)

4.9 Issue Escalation Plan

Escalation chart in case of issue can be provided in this section. Escalation will happen both client and assessment organization. A flow chart will be of great help.

4.10 Develop a Engagement Plan and Send it to Customer for update

It should include followings:

- Send test cases which you are going to execute
- Put time for every test case
- Mention start and end date of engagement
- Time of assessment
- Contacts of each team

4.11 Set Milestones and Timelines

Define milestones of engagements as per tasks, stick to them and achieve in defined time. Try to complete testing in office hours. It will help to minimize any down time if it occurs in any circumstances.

Event	Week 1-5	Week 6-10	Week 11-15	Week 16-20	Week 17-25
Planning and Prepration					
Assessment					
Assessment – Pertinent Risk Identification					
Assessment – Controls Assessment					
Treatment					
Accreditation					

4.12 ENGAGEMENT SCHEDULE

The CUSTOMER NAME Engagement will be driven with a Engagement schedule chart.. The Master Schedule details all major phases and it's associated sub-tasks. The Master Schedule is detailed below.

<INSERT ENGAGEMENT SCHEDULE HERE>

4.13 DELIVERABLES PRODUCED

All engagements have deliverables. In this section, describe the deliverables of the engagement. Provide enough explanation and detail so that the reader will be able to understand what is being produced. (Remove this comment section from final document.)

- Deliverable 1: description
- Deliverable 2: description
- Deliverable 3: description

4.14 ENGAGEMENT ESTIMATED EFFORT/COST/DURATION (COST OPTIONAL)

The estimated effort hours and engagement costs may be depicted in many ways, including cost by team member, cost by deliverable, cost by milestone, or cost by category (internal labor, external labor, travel, training, supplies, etc.). Also include a chart showing the engagement start date, major milestones, and end date. The deliverables included in this milestone chart should all have been described in the scope section. (Remove this comment section from final document.)

Milestone	***Date completed***	***Deliverable(s) completed***
Engagement planning	*Mm/dd/yy*	• *Engagement definition* • *Workplan*
Milestone 1	*Mm/dd/yy*	• *Deliverable 1* • *Deliverable 2*
Milestone 2	*Mm/dd/yy*	• *Deliverable 3*
Milestone 3	*Mm/dd/yy*	• *Deliverable 4*
Milestone 4	*Mm/dd/yy*	• *Deliverable 5*
Engagement conclusion	*Mm/dd/yy*	

4.15 ENGAGEMENT ASSUMPTIONS

Engagement assumptions are circumstances and events that need to occur for the engagement to be successful but are outside the total control of the engagement team. They are listed as assumptions if there is a HIGH probability that they will in fact happen. The assumptions provide a historical perspective when evaluating engagement performance and determining justification for engagement-related decisions and direction. (Remove this comment section from final document.)

In order to identify and estimate the required tasks and timing for the engagement, certain assumptions and premises need to be made. Based on the current knowledge today, the engagement assumptions are listed below. If an assumption is invalidated at a later date, then the activities and estimates in the engagement plan should be adjusted accordingly.

- Assumption #1
- Assumption #2
- Assumption #3, etc

4.16 ENGAGEMENT RISKS

Engagement risks are circumstances or events that exist outside of the control of the engagement team that will have an adverse impact on the engagement if they occur. (In other words, whereas an issue is a current problem that must be dealt with, a risk is a potential future problem that has not yet occurred.) All engagements contain some risks. It may not be possible to eliminate risks entirely, but they can be anticipated and managed, thereby reducing the probability that they will occur.

Risks that have a high probability of occurring and have a high negative impact should be listed below. Also consider those risks that have a medium probability of occurring. For each risk listed, identify activities to perform to eliminate or mitigate the risk.

	IDENTIFICATION	QUANTIFICATION				MITIGATION	
		PROBABILITY (%)					
WBS #	DESCRIPTION OF RISK EVENT	Low 0-.35	Medium .35-.65	High .65-1.0	CONSEQUENCES	SOLUTIONS	COMMENTS

4.17 ENGAGEMENT APPROACH

This section is used to describe how the engagement will be structured and the important techniques that will be utilized. The engagement approach is intended to encourage the engagement manager to think about the engagement from the top down instead of the traditional bottom-up method. Including the approach in the engagement definition compels the engagement manager to both consider the dependencies of the engagement and to incorporate the engagement management necessary to plan and manage the engagement. (Remove this comment section from final document.)

4.18 ENGAGEMENT ORGANIZATION (ASSESSMENT TEAM & CLIENT)

It is important to understand who the major players are on the engagement. An organization chart works well. Otherwise, list the major engagement roles and the actual people involved. (Remove this comment section from final document.)

Add a engagement organization chart, if available. (Remove this comment section from final document.)

4.19 RESPONSIBILITY MATRIX

A – Approves the Deliverable

R – Responsible for Creating the Deliverable

N- Notified when deliverable is complete

M – Manages the Deliverable

F – Facilitates timely Resource Allocation

S – Responsible for Acceptance and Signoff

P – Participate in Archiving the Deliverable

S.NO	Deliverables & Tasks	Assessment Team				Clients	
		Program Manager	Engagement Manager	Consultants	Team Members	Engagement Manager	Stake Holders & Functional Heads
1	Engagement Scope	A	R	R		R	

4.20 SIGN-OFF SHEET

Client Name: XXXXX

Engagement Manager: XXXX,

Engagement Name:	IT Security Assessment		*Purchase Order Number:*		
Begin Date:	04/06/03	*Target End Date:*	10/09/03	*Final End Date:*	

S.NO	Deliverables	Date Completed	Assessment Team Name	Xxxxxxxxxxx
1	Statement of Work	13/06/2003		

Final Sign off

Assessment team has successfully performed according to the conditions set-forth in the SOW, Dated _____for the Security Assessment Engagement.

Sign Off on Work Performed:

_____

_____

XXXXXXX XXXXX

Assessment Lead Client Lead

Remarks
Typically the RIR WHOIS databases will not locate any domain-related information or any information relating to military networks.

4.21 ANNEXURE - ASSESSMENT ADMINISTRATION ROADMAP

(Cycles indicators)	ASSESSOR	CLIENT
	Suggests scope and objectives (optional)	Defines requirements (scope, objectives, and acceptance criteria)
		Publishes RFP (optional)
Repeats until RFP	Evaluates RFP (feasibility, risk, technical considerations)	

requirements are clear to assessor		
	Clarification meeting (optional)	
	Signature of Mutual Confidentiality Agreement	
	Requests additional information (if allowed by RFP)	
		Prepares and sends additional information (if allowed by RFP)
	Estimates project needs (staff/resources/time) and cost	
Repeats until Client is satisfied with proposal(s)	Creates and delivers proposal	
		Evaluates proposal(s)
		Requests adjustments to proposal(s) (optional)
	Compliance/expectative check meeting(s)	
		Evaluate vendors capabilities (optional)
		Select best proposal (if more than one proposal was received/requested)
	Engagement refinement meeting (starting ending/dates, holiday considerations, business activities considerations, technical considerations, contact lists exchange, etcetera)	
	Kickoff meeting	
Repeats until all phases are completed	Performs technical evaluation phase; reports critical findings immediately.	Requests information on progress and provides feedback (optional) and decides whether to suspend or not evaluations, depending on some findings.
	Reports phase status	
Repeats until client and assessor are satisfied with findings and comments included in the report	Prepares and delivers technical report draft	
		Reviews technical report
		Prepares and delivers comments to be included in the report (business impact/considerations and technical considerations)

	Technical report review meeting (correlation with client data, accuracy validation and business impact review)	
	Provides training on techniques tools used for evaluation (optional, usually defined in RFP and/or proposal)	
	Prepares and delivers final report	
	Prepares presentation for management	
	Findings review meeting with management	
Repeats until problems outlined in the report are solved	Provides support for problem solving. (optional)	Defines project plan for solving problems (including prevention of future occurrences)
		Reports problem solution status to management
		Lessons learned internal meeting.

5 GOOD PRACTICES– PRE ASSESSMENT, ASSESSMENT AND POST ASSESSMENT

Over the last few years, the security assessment process has evolved from an assorted set of attacks carried out by amateurs to a mature and reviewable assessment process with strong legal boundaries and well-defined deliverables.

Irrespective of Vulnerability Assessment, Penetration Testing and/or Security Assessment, there are certain things which the assessor needs to take care of while assessing the strength of an enterprise's security.

A well defined, proven and structured assessment can assist greatly in fortifying your defenses; it also throws up newer, complex issues that you will have to deal with. E.g. Legal Aspects, Check Knowledge base section for more detail on this.

This section provides all the good practices / guidelines required to perform the security assessment. Management, key people involved in assessment and all other members of the assessment team must read and follow it. Owner and Assessment Company (irrespective of internal or external) should sign it before starting an assessment.

Good practices / Guidelines	Compliance (Yes/No)	Comments
Legal Aspects		
Ensure that you have signed a Non-Disclosure agreement with the company that is performing the assessment. **Recommended Reading:** Non Disclosure Agreement in Appendix.	✓	
Ensure that you have signed the Security Assessment Agreement. **Recommended Reading:** Security Assessment Agreement in the Appendix.	✓	
Ensure that you do not scan outside IP Address and are limited to the IP addresses and domains specifically assigned to you.	✓	

Clearly define the boundaries of the assessment to avoid any conflict and/or confidentiality issues. E.g. an assessor breaks into the system and he may read confidential information on it. Make it clear whether you want the assessor to access confidential information and show it to you or just leave a message on the system in a text file.	✓	
Clearly define the limits of liability for the assessment team, in case of an incident caused by negligence or malpractice. E.g. most assessment teams limit the liability up to the cost of the security service being performed.	✓	
People		
Assessment team participating in the assessment, the following information must be documented and evaluated by the Assessed Company: a) Experience with the platforms, applications, network protocols and hardware devices being tested. Experience of candidates should match that of the targeted infrastructure. b) Certifications and courses related to penetration testing. This information should confirm that assessment team members are capable of performing the activities described in the scope of the service. c) Years of experience in penetration testing engagements. This information should confirm that assessment team members are capable of performing the activities described in the scope of the service. d) Attack scripting/programming languages mastered by each member. This information should demonstrate abilities for designing and performing manual testing procedures. e) Public information showing participation in the community of each member, such as articles, forum posts, papers, participation in events, etc. People	✓	

that show up in public places demonstrate their credentials and is more easily trusted. Assessors that have engaged in a public discussions on information security testing demonstrate their knowledge and experience. f) List and description of tools/scripts created/modified by each member, related to security assessment. This information should demonstrate abilities for designing and performing manual testing procedures. g) Roles and Responsibilities of each member in the team. This information should indicate the grade of involvement of each assessor and the importance of their participation in the team.		
Have you gone through the resumes (including references) of the assessment team members and are you satisfied with their skills?	✓	
Have you checked recruiting policies of company and are you comfortable with them?	✓	
Have the employees of the Company performing the assessment signed strong Non-disclosure agreements with their firm?	✓	
Processes		
Have you clearly mentioned that you want to assess a denial of service attack on your live or test system? Or do you prefer that they simply audit the system and describe the specific flaws in your network that leave you susceptible to a particular Denial of Service attack?	✓	
Generally a security assessment / penetration test is recommended only when you have baseline security in place.	✓	
Are you assessing security of secondary systems (may be redundant) instead of primary systems? Both approaches have their advantages and disadvantages but it is generally recommended that	✓	

you assess the security of secondary servers rather than primary servers when strict confidentiality has to be maintained and any kind of down time is not acceptable. The path used to attack the secondary servers can reveal flaws in your security architecture that apply equally to your primary servers.		
Is the test infrastructure secure and is logging performed? Please give details.	✓	
Is the assessment team or a team member going to perform any test from home? Especially using a PC other than an official Laptop or assessment machine.	✓	
Ensure that the assessment team provides precise information on the assessment equipment physical and logical locations (E.g. physical addresses from where tests will be conducted and IP addresses used at the time of the test).	✓	
Is the process established to get clearance before starting a test?	✓	
Are the test cases provided to you?	✓	
Ensure that the organization/company has licenses for the commercial tools used by the assessment team. Make sure that both parties are clear on who is going to provide what tools.	✓	
Is the date, time and day for the assessment fixed? A time when traffic is minimal is preferred, late nights and weekends are good times since any unexpected negative impact on the network will cause least harm to the users during off-peak hours.	✓	
Does the Assessment Company have well-defined processes for managing the output of the test cases?	✓	
Ensure that both the Assessment Company and the Assessed Company exchange contact information of people involved in the tests anytime during the engagement. (E.g. email addresses, phone	✓	

numbers, fax numbers and pagers).		
Deliverables		
The assessment team should show a clear approach and path of attack to be carried out and a demo as and when required. A list of vulnerabilities on the compromised network is not sufficient since it may not give the actual path that can be exploited.	✓	
Has the Assessment Company submitted a sample copy of previous Assessment reports? Does it cover everything you want as a client? Ensure that you do not reveal any kind of client information, very clearly mask client name and information that makes resources identifiable such as IP addresses.	✓	
The report shall contain all tests performed and their outputs as per the ISSAF test case template	✓	
List of vulnerabilities identified and countermeasure to safeguard against them.	✓	
Very high critical threats must be reported immediately.	✓	
Ensure that you do not use new/unfamiliar tool on a production environment.	✓	
Guard against performing a man-in-the-middle attack and forgetting to forward traffic further.	✓	
Guard against performing a man-in-the-middle attack and not considering the speed of a device which is performing the man-in-the-middle attack. Generally middle man devices are slow and they can't give high throughput. For example a laptop.	✓	
Readiness of Infrastructure	✓	
• The assessor should make sure the connection for testing is up and that a backup line or internet access is readily available before starting the tests.		
• Ensure that due to some reason certain		

protocols/services are not blocked at the assessment center end (Your company/ISP). It may seriously affect you assessment results. • E.g. ICMP is blocked as per corporate policy • E.g. UDP traffic is blocked at ISP end due to any worm. Strange but it happens some time.		
• Ensure that your company's technical infrastructure department does not change IP addresses of the Assessment Center without your permission; these could negatively impact your tests because the target firm will expecting connections from a certain IP range.		
• Ensure readiness of a assessment team kit: • Assessment Tools / Products • Operating System CDs		
• Ensure that the people involved in the assessment process properly understand the client's requirement as specified in the RFP.	✓	
• Ensure that you are using a dedicated equipment for testing. Emails and any other administrative or personal activities should be preformed on other machine(s) or if it's on same machine it's recommended to do on different boot partition. This guarantees the integrity of the testing machine.	✓	
• Ensure that a process is available for collecting test results and they are presented in a proper format. Otherwise analysis will take a lot of time and important information may be missed.	✓	
• Ensure that the testing process is closely monitored and documented, in order to facilitate the identification of telecommunications problems and false positives (usually the test is recorded at network level using a protocol analyzer and a different machine, in order to	✓	

avoid an impact in performance to the testing equipment).		
• Avoid a breach in confidentiality by releasing client data.	✓	
• Ensure that your storage server for test results is secure.	✓	
• Ensure all correspondence in appropriate way. If you exchange asset information verbally or on a plain paper or on phone (generally this happens while performing onsite assessment). Later on you don't have any record to prove that this is what was given for assessment by the client, just in-case if any undesirable politics happens. This guideline can be adopted at various stages in the assessment process. Use of digital signatures and encryption for formal electronic communication is necessary to guarantee confidentiality, authenticity and non-repudiation.	✓	

5.1 PHASE – I: PRE-ASSESSMENT

5.1.1 Request for Proposal (RFP)

The organization shall clearly define followings:

- Name and details of person to whom proposal needs to be submitted
- Maximum time to submit the proposal (E.g. 1st Jan 2005)
- Maximum time to complete the assessment (e.g. March 2005)
- High level design of network architecture to selected companies after signing Non-Disclosure Agreement(NDA)

The organization shall clearly ask Assessment Company to state followings in the proposal:

- Maximum time to complete the assessment (e.g. March 2005)
- Expected time to complete each task
- Serial and parallel tasks in proposal
- Dependencies between tasks
- Time period in which the assessment has to be completed
- Understanding of Assessment Company's requirement

- Your understanding of our requirement
    - Asset segments which needs to be assessed
    - Number of Access Points and devices from where assessment has to be performed
    - Expected deliverables
    - Clearly defied scope of assessment. Expected depth of tests in each task (how far should the assessors go: network, O.S., application level, etc.)
    - List of objectives by which each task will be evaluated (should be effort oriented, not success/failure oriented)

5.1.2 Evaluation of Third Party Contracts

5.1.2.1 Purpose of Third Party Contracts Evaluation

In today's highly connected world, organizations typically share business information with a number of third parties, either out of a business imperative or to comply with regulatory requirements. The sharing could be as simple as an exchange of emails or as 'invasive' as providing remote access to each other's internal systems.

An organization would typically have no control over the security management at a third party and therefore have no control over the security of their own information. The best an organization can do in most cases is to cover themselves legally with the appropriate clauses in contracts with third parties.

5.1.2.2 Aim / Objective of Third Party Contracts Evaluation

As part of an evaluation of information systems security, contracts with third parties must be evaluated to see if the organization is adequately covered legally.

This is also a recommendation within ISO 17799.

5.1.2.3 Third Party Contract Evaluation Guidelines

The roles of third-parties can be varied:
Application support and maintenance for an organization's internal systems; Business partner (e.g. distributor) with access to internal systems; Facilities managed service, i.e. they host and manage the organization's "internal" system; Business partner providing services to the organization's clients on behalf of the organization.

Contracts with third-parties should have clauses similar to those mentioned in this section. Not all clauses will be suitable in all cases. And additional clauses will be required for the specific services provided.

Existing contracts typically provide good coverage of some of the items listed in ISO 17799, such as service level agreements and intellectual property rights. This section highlights those items that existing contracts do not typically cover.

[start of contract clauses]

Security of <Company's> and <Company's> Clients' Information Assets

By 'information assets' is meant, without limitation, paper documents, electronic data, servers, desktop computers, laptops, PDAs, software, network elements and mobile telephones.

The Supplier may be given access to <Company's> and <Company's> clients' information assets to allow them to fulfill their obligations under this contract.

1) The Supplier shall take all reasonable steps to protect the confidentiality, availability and integrity of <Company's> and <Company's> clients' information assets, including but not limited to:

a) Implementing appropriate security policies and practices, consistent with the most current version of AS/ISO 17799.
b) Complying with the <Company> Acceptable Use Policy, the current version of which is attached in Appendix XXX. The most up-to-date version of this policy is available on the <Company> web site.
c) Complying with all applicable privacy and cybercrime legislation.
d) <*Optional*> Complying with all applicable financial/health/other industry standards.
e) <*Optional*> Compliance with the security policies and standards attached in Appendix XXX.

2) Upon written request, the Supplier shall provide to <Company> a copy of their information security policy, standards, operating procedures and related documentation. <*Optional*> The Supplier authorises <Company> to forward this documentation to any <Company> client who is supported by the Supplier.

3) Where <Company> has responsibility for maintenance of user accounts: The Supplier shall notify <Company> within 1 working day, if an employee, contractor or agent of the Supplier, who has access to <Company's> or <Company's> clients' information assets:

a) Leaves the employment or hire of the Supplier. If the termination happens under unfriendly circumstances, the Supplier shall notify <Company> within 1 hour.

b) No longer requires access to <Company's> or <Company's> clients' information assets.

4) Where the Supplier has responsibility for maintenance of user accounts: The Supplier shall change all relevant passwords within 1 working day, if an employee, contractor or agent of the Supplier, who has access to <Company's> or <Company's> clients' information assets:

a) Leaves the employment or hire of the Supplier. If the termination happens under unfriendly circumstances, the Supplier shall change passwords within 1 hour.

b) No longer requires access to <Company's> or <Company's> clients' information assets.

5) Security Incidents.

A breach of security includes, but is not limited to, a loss or theft of information assets.

a) The Supplier shall notify <Company> immediately upon a confirmed, or suspected, breach of security of <Company's> or <Company's> clients' information assets. The notification shall be to ALL of the following:

i) by telephone – <Insert the <Company> contact the Supplier uses for issue escalation>

ii) by email - infosec@<company>.com.au

b) The Supplier shall provide all required assistance to <Company> in investigating a breach of security.

OR

5) The Supplier shall adhere to the Information Security Incident Response Plan agreed with <Company> and attached in Appendix XXX.

6) The Supplier shall ensure that all the Supplier's information assets with access to <Company's> or <Company's> clients' information assets:

a) are free of viruses and other malicious software;

b) have an anti-virus tool installed, enabled and configured to use the latest signature files provided by the anti-virus vendor.

7) The Supplier shall ensure that all employees, contractors or agents who require access to <Company's> or <Company's> clients' information assets sign a Non Disclosure Agreement prior to being given access.

8) The Supplier shall ensure that all employees with access to <Company's> or <Company's> clients' information assets are provided training on the relevant security policies and procedures prior to being given access and are provided refresher training every year subsequently.

9) Upon written request, the Supplier shall allow <Company> to audit the Supplier's facilities, networks, computer systems and procedures for compliance with the Supplier's and other agreed Information Security policies and standards. <Company> may utilise a third party to conduct the audit. Audits may include, but not be limited to, the use of automated tools and penetration tests. <Company> shall request audits as and when necessary, but no more than four times in any 12 month period. A minimum of 48 hours notice shall be given prior to an audit.

10) <*Optional*> If the above clauses are breached:
a) <Company> reserves the right to terminate this contract, etc.
b) The Supplier shall be liable to pay penalties to <Company>, etc.

[end of contract clauses]

The following must be attached to the contract as required:

- <Company's> Acceptable Use Policy;
- Security policy and standards documents;
- An Incident Response Plan

5.1.3 Sales and Marketing

Some of the guidelines during the sales life cycle are as follows:

- Consider the size, politics, type of industry
- Take into account the skills and knowledge of the organization's personnel
- Consider the organization mission, goals and objectives for this project.

- Consider the risks and complexity of the service required.
- The Sales Person should understand the need for right pricing, based on the two considerations above.
- Sales person should understand the complete assessment cycle.

5.1.4 Obtain Authorization and Make sure Right People has given it

Security assessment involves performing actions very similar, if not identical, to those carried out by an attacker. Likewise, the security test may result in the compromise of information systems due to which classified information may be accessed during the test. Even in the case that an agreement exists between the security assessor and the client, the latter may not accept, for instance, that classified information may become revealed to the security assessor.

For these reasons it is always necessary to obtain clear authorization from the client to perform the security assessment. Typically, approval from the client should be sought in such a manner that the client assumes responsibility for the results and side-effects (if any) of the security assessment.

It is also very important that right person has given permission to you. Obtain it from the appropriate management / authority. It is recommended that in every company IT department should have process to for approval.

Such approvals should be printed on company paper (letterhead) and signed by the responsible person(s).

Reference: Security assessment agreement in appendix

5.1.5 Define the scope of work

As part of the contract or agreement between the security assessor and the client, the scope of the work to be done must be clearly specified. Whenever possible, loose or ambiguous definitions should be avoided. The security assessment work will be performed with better accuracy and its results will be more reliable when the extent of the work is bounded.

Scope of Work

- Define Evaluation Criteria: Evaluation criteria uses metrics based on effort. E.g. N different automated tests + M different manual tests be performed, independently of whether those tests result in compromising the target/ vulnerability findings or not. All the results of tests will be submitted to client.
- Define Objectives
- Define Scope areas
- Define "Out of Scope" areas

Both parties should define and agree on the scope of work. The scope of work should clearly define, what should be done and what not, define timelines and dependencies of the work for both parties. Areas which the scope of work should cover include:

- Complete Organization
- Specific Location(s)
- Specific Branch(es)
- Specific division(s)/Sub-division(s)
- Nature of testing (intrusive / non intrusive)
- Testing from External, Internal and or Both
- In context with Web Presence(s)
    - Domain Names (DNS)
    - Server Names (Internal)
    - IP Addressing
- In context with Infrastructure
    - Remote Access like Dial-up, VPN, Frame Relay etc…
    - ATM

5.1.6 Define the "Out of Scope" Areas

After going through scope of work definitions; there must be clearly defined limitations and conditions for assessors, which he should not violate.

Some client prefers to have testing in off hrs (nighttime) and on weekends. It helps them to give less impact of any downtime. Off hrs testing is only good when it is being done in the presence of client staff; to ensure that if any downtime happens then the staff can control it and take necessary actions.

5.1.7 Sign Agreement

On the basis of above mentioned points sign a formal agreement. This written permission, often called the rules of engagement, should include two agreements: 1. Security Assessment Agreement and 2. Non Disclosure Agreement

5.1.7.1 Assessment Agreement

An assessment agreement should include:

- Scope of work
- Out of Scope work
- IP Addresses or ranges that needs to be assessed
- Any specific IP addresses / subnet, host, domain that should be restricted
- Liability for any downtime
- Time of Completion of project and indication of any delay
- The contract price, any additional charges, applicable penalties
- Payment (advance and after the project)
- Date and Time-wise schedule of assessment based on time and material or Fix bid contract.
- Some mechanism if testing takes more than estimated time
- Source IP address of machines from where security assessment and test will be conducted
- A mechanism for dealing with false positive in order to avoid unnecessary law enforcement
- Contact Person(s) at the client and at your company (both phone & mobile phone numbers as well as email addresses)
- General Provisions
    - For delay/non payment
    - For additional labor

Reference: Security assessment agreement in appendix

5.1.7.2 Non Disclosure Agreement

A Non Disclosure Agreement should include followings:

- Purpose
- Definition
- Non-Disclosure of Confidential Information
- Mandatory Disclosure

- Return of Materials
- No License Granted
- Term
- Miscellaneous
- Governing Law and Jurisdiction
- Remedies

Reference: Non Disclosure agreement in appendix

5.1.8 Team Composition

Consider efficiency and accountability and compose a team of domain experts, as per the scope of work. Security assessment can be achieve much better with specialized team members' then having one person doing everything. Different team members bring different set of skills together. Some team member may have skills to break into systems but may not know firewall/IDS security assessment. Quite often it is seen, people who are good into breaking into system are not quite good at putting test result in an appropriate format for report and also do not like taking notes of their work.

5.1.9 Commercials

Based on the type of engagement, scope, skill set requirements and complexity of the system, the commercials can be worked out. The type of calculation may vary for time and material/Fixed bid model.

5.1.10 Maintain confidentiality of client data - before start of Project

In preparation for the security assessment job, the assessor may require information from the client in order to carry out the tests, such as network infrastructure diagrams, IP addresses, location of client premises, contact information for people in the organization, existence and location of network access points, vendor of network and IT systems, among other types of information.

This information may be confidential, and it is the security assessor's duty to ensure that any such information handled throughout the project will be treated according to its classification within the client organization.

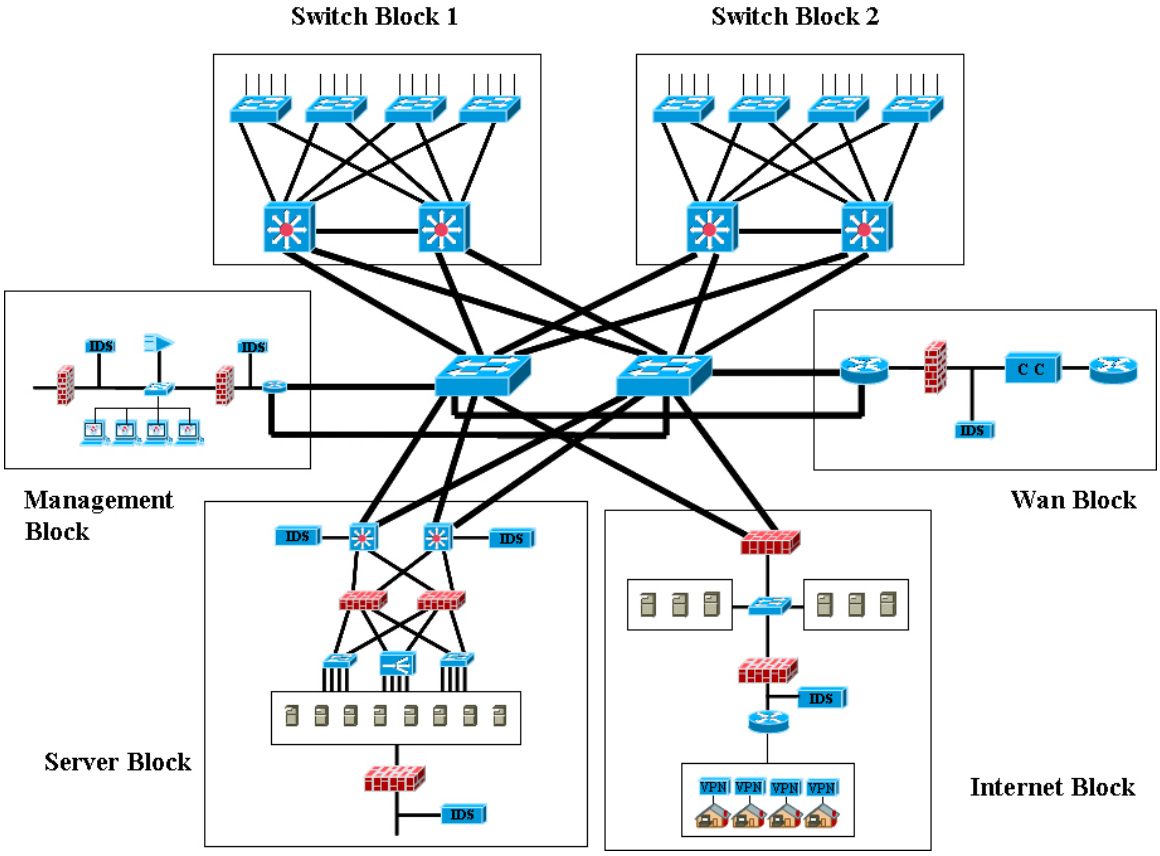
5.1.11 Access Point Identification

It is of paramount importance that the access points chosen for conducting a security assessment represent all the possible threats, threat agents and possible business risk. The choice of access points along with a good cross section sample of devices is imperative for correct determination of threat to the facility and Information Systems. Based on given low level network architecture design and with the help of client technical representatives choose the access points to represent various threat agents such as “internet”, “operators/clients”, internal etc. Along with the threat agents, test the network layer by layer as per the methodology. The generalized division of the network in layers is as follows:

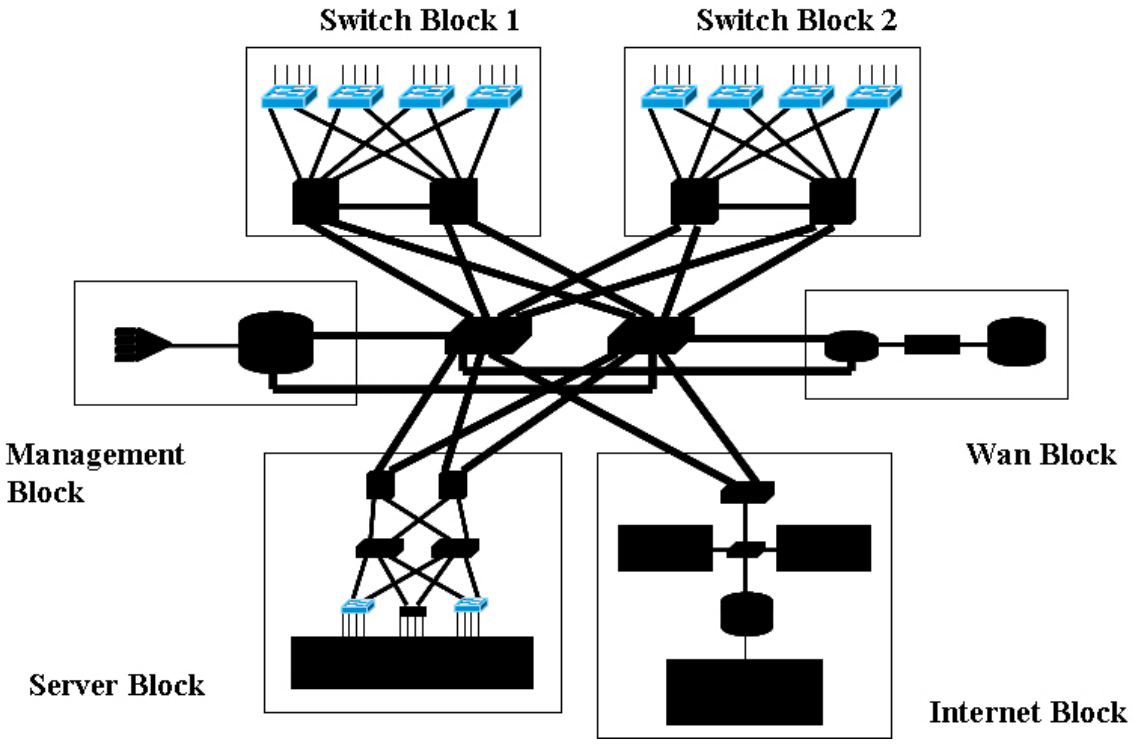
The above segments/components were tested from viewpoint of threat agents as “the internet”, “administrator” and as “client” etc…

Here we are taking a very common network architecture design and based on that we will identify access points for testing.

5.1.11.1 Layered Network Architecture Design

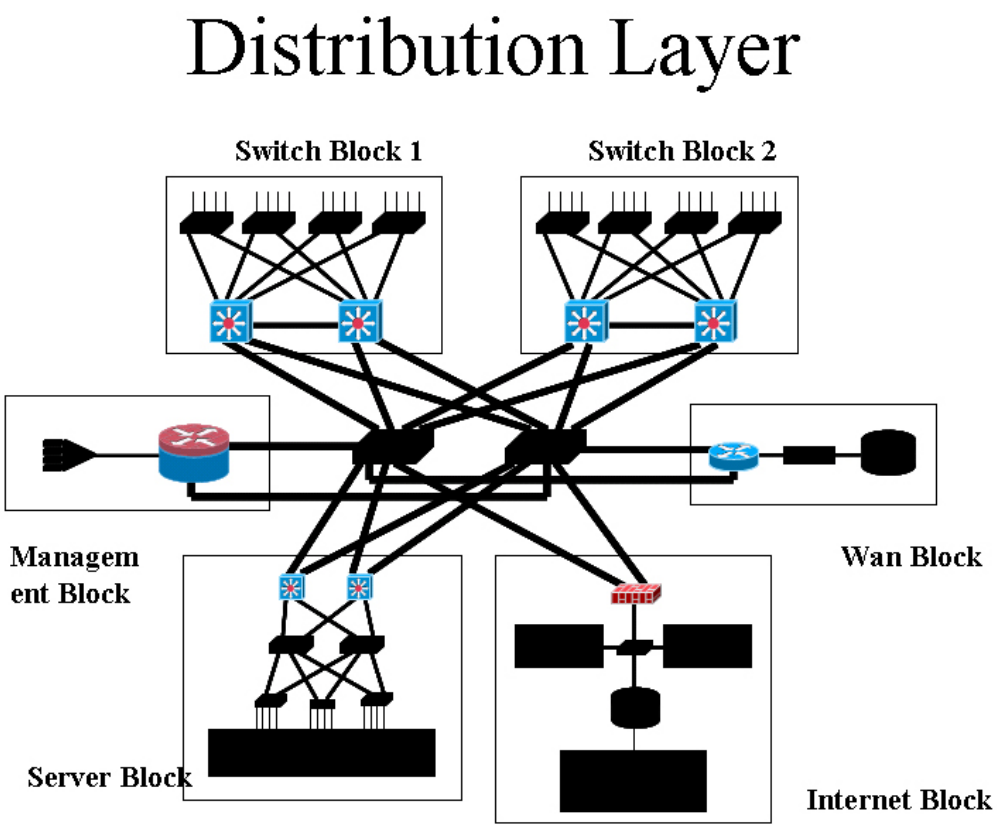


5.1.11.1.1 ACCESS LAYER



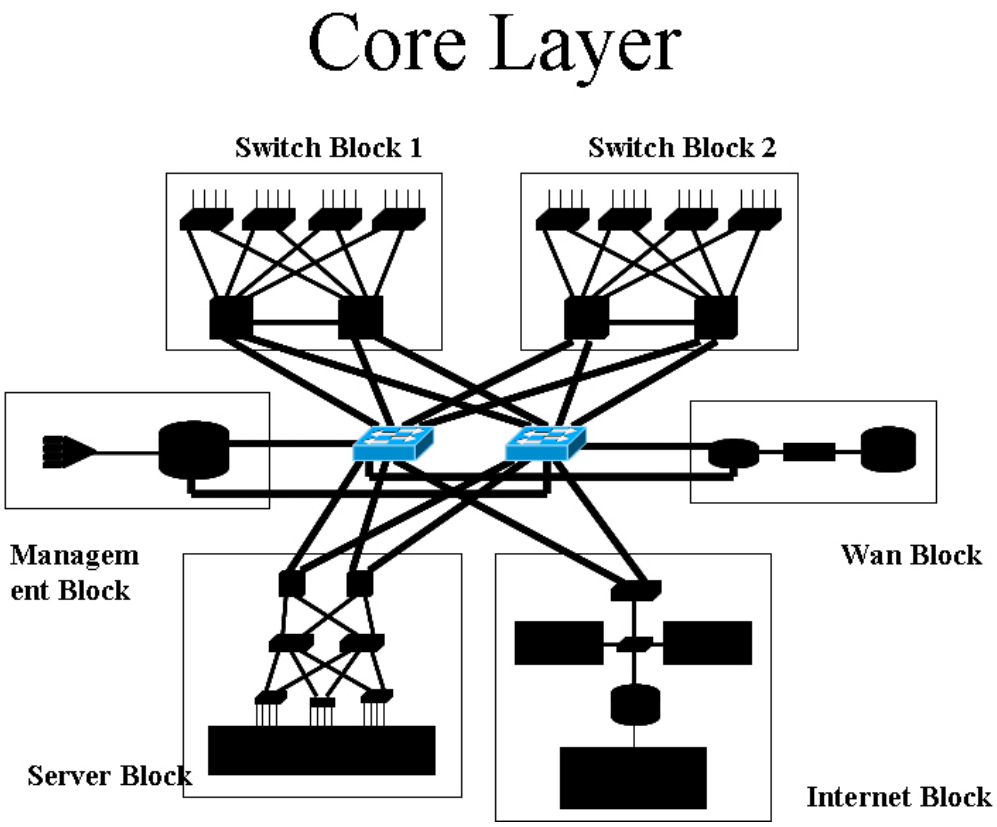
Key Elements to Assess	Access Points
Layer-2 Switch [Switch Block1]	
Layer-2 Switch [Switch Block2]	

5.1.11.1.2 DISTRIBUTION LAYER



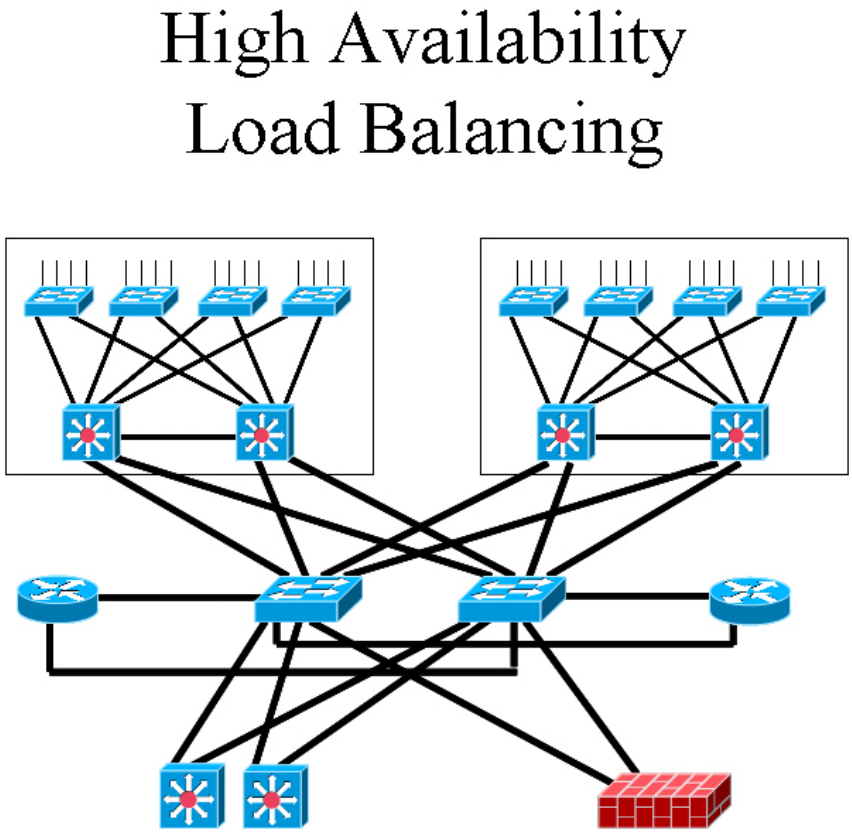
Key Elements to Assess	Access Points
Layer-2 Switch [Block1]	
Layer-2 Switch [Block2]	

5.1.11.1.3 CORE LAYER



Key Elements to Assess	Access Points
Layer-2 Switch [Core]	
Layer-2 Switch [Core]	

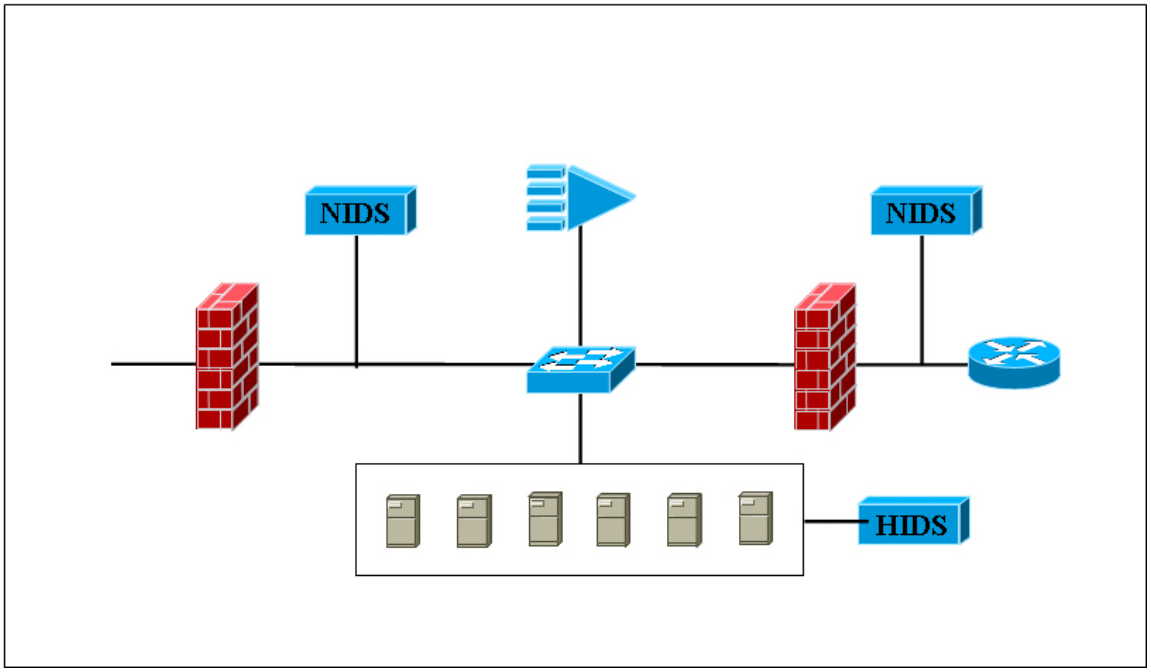
5.1.11.1.4 HIGH AVAILABILITY AND LOAD BALANCING



Key Elements to Assess	Access Points
Layer-2 Switch [Block1]	
Layer-2 Switch [Block2]	

5.1.11.1.5 MANAGEMENT BLOCK

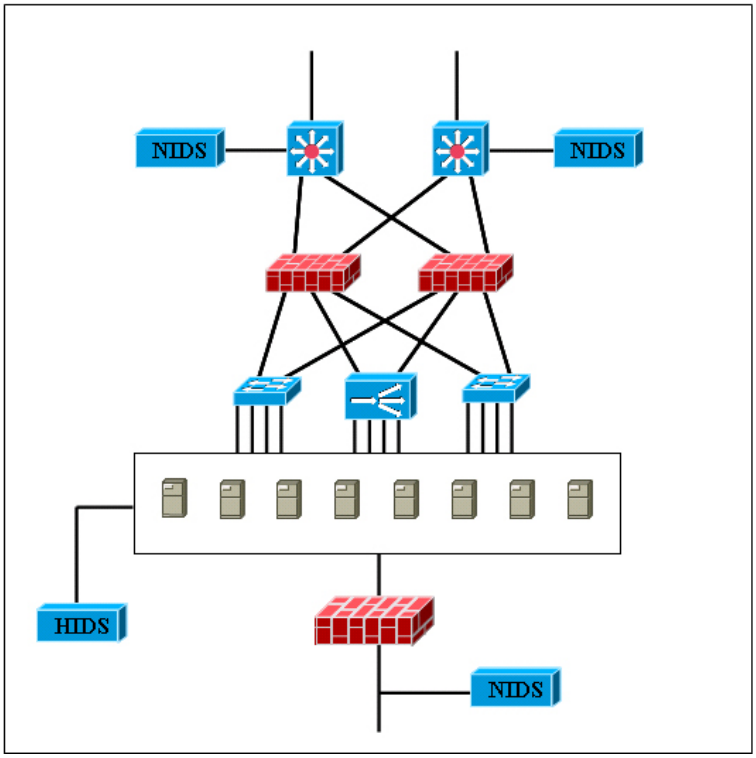
Management Block



Key Elements to Assess	Access Points
Firewalls	
Network based Intrusion Detection Systems	
Host based intrusion Detection Systems	
SYS log server	
SNMP Management System	
System Admin Hosts	

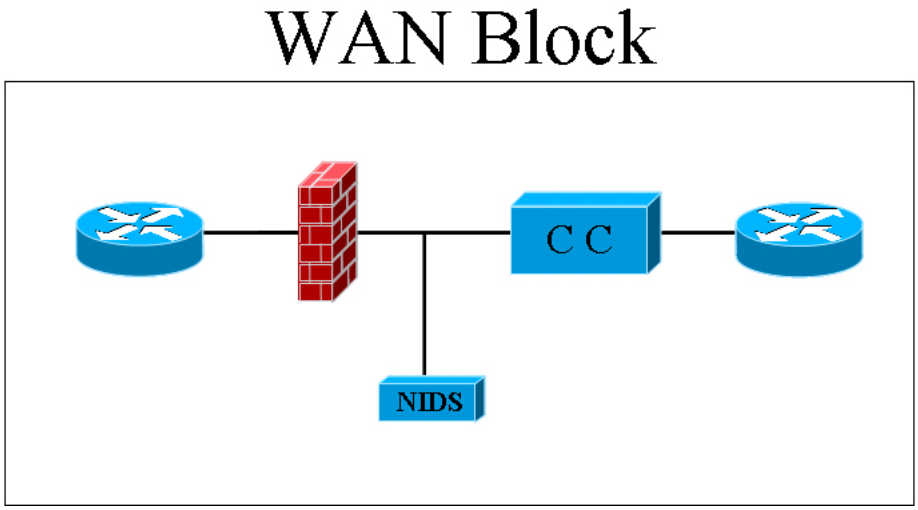
5.1.11.1.6 SERVER BLOCK

Server Block



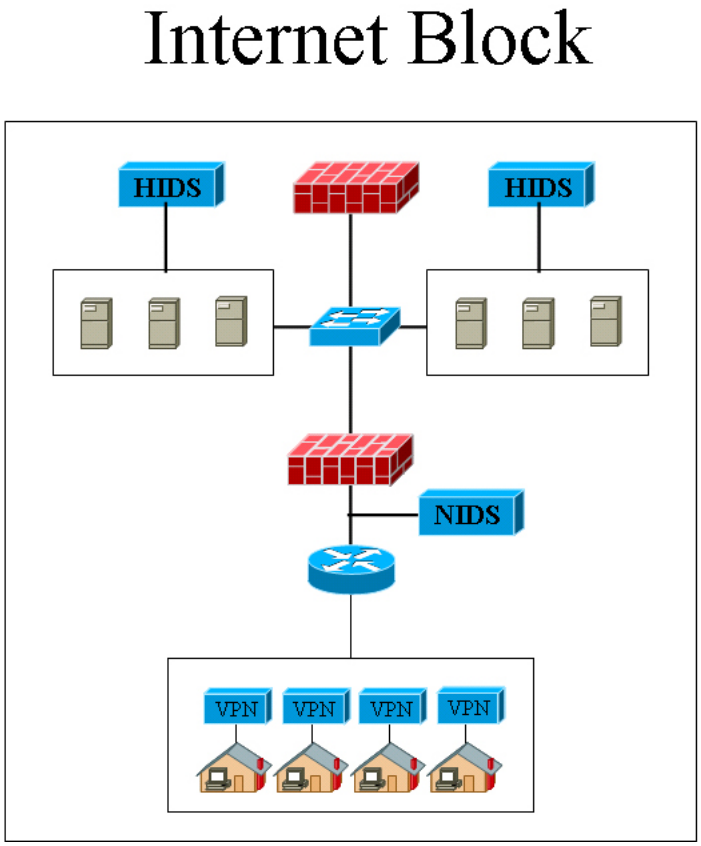
Key Elements to Assess	Access Points
Firewalls	
Network Intrusion Detection System	
Host Intrusion Detection System	
NTP Server	
TACACS+ Server	
Secure-ID Server	
Certificate server	
Corporate Servers	
Call Manager	
DNS Servers	
E-Mail Servers	

5.1.11.1.7 WAN BLOCK



Key Elements to Assess	Access Points
Firewalls	
NIDS	
Crypto Clusters	
Routers	

5.1.11.1.8 INTERNET BLOCK



Key Elements to Assess	Access Points
Firewalls	
Host Based Intrusion Detection System	
Network Based Intrusion Detection System	
VPN Concentrator	
HTTP Server	
DNS Servers	

5.2 PHASE – II: ASSESSMENT

5.2.1 Rules of Engagement

Establish clear rule of engagement based on the assessment scope. Covert the same in the scope of work agreement mutually agreed and signed by client and assessment team.

During the course of the project the client may provide the assessor with further information, as required by the progress of the security assessment job (network diagrams, system parameters, applications used, access credentials, etc...). The assessor must be aware of the confidentiality of the information used to do the job, and treat it as such.

Security tests may also yield information about the client's information systems that, while not provided directly to the assessor, may also be confidential. This includes any vulnerability that may be found as a result of the security assessment.

Likewise, any documents, company information, personal e-mail or any other types of computer files that the assessor may have access to as a result of a successful penetration test, shall also be treated with confidentiality.

- Observe and obey security policies
- Never operate beyond agreement
- Never operate beyond scope of work unless officially requested by the client (this should be done through a signed request & approval)
- Members of the analysis team may be present during the assessment
- Ensure all the required approval[s] from all concern department[s] (Just in case if it is required even after management approval) have been taken
- Ensure all the effected department/personnel have been informed. Inform them time of assessment and also if there are any chances of down time.
- Vulnerability Scan
    - Ensure latest signatures are updated
    - Ensure latest signatures are tested in lab environment before using them in production environment
    - Ensure automated vulnerability scanner (the current version which you are trying to use) is not creating any kind of problem during scan

(especially any kind denial of service against target). To achieve this you can subscribe to product and industry mailing lists and/or you can ask a question about this, and/or you can test the product at least once before using in production environment.

- Use at least two automated vulnerability scanners (to prioritize manual verification of common vulnerabilities before fiddling with false positives)

- Vulnerability assessment tool – A vulnerability assessment tool may be software (automated scanner which works based on a *vulnerability database*), a script, customized script and/or a check-list.
  - It should check for known/unknown weaknesses and mis-configurations.
    - For know vulnerabilities Common vulnerabilities and exposure (CVE) is publicly available commonly used vulnerability database. This database is maintained by MITRE Corporation and it's accessible at http://www.cve.mitre.org this vulnerability database is also not fully sufficient. One need to maintain custom vulnerability database
    - http://www.securityfocus.com/bid is also a good place to search for vulnerabilities (and for exploits and possible solutions)
- Perform manual verification of all vulnerabilities identified with the automated tools & vulnerability assessment tools
- Inform Analysis team immediately about any identified **high-risk** vulnerabilities and countermeasures to safeguard them.
- Ensure assessor's machine security
  - Implement latest patches for Operating System and Applications installed on it.
  - Administer assessor machine with security in mind.
  - Implement a Host based firewall, Intrusion Detection and Prevention System on it.
- Provide Proof of assessor machine security - Many time penetration tester / assessor don't apply the security patches on their machines in order to test some exploits before firing on target organization and/or for demonstration purposes. There are chances that these machines may be compromised by an attacker/worm and can be used as staging host to perform further attack on target organization.
  - Before start of test, perform vulnerability scan by automated vulnerability scanner on assessor machine and send it to the Project Manager and/or client everyday.

- Run audit script and send output to client.
- If needed, sign a “secure system” document of the client (can be a requirement to get access to the network)
- Make sure Anti Virus is not deleting/quarantining/clearing exploits/tools. Some time they just remove some part of code and as a result of this tool doesn’t work. Have your tools/exploits repository in a separate drive and set the antivirus not to scan the specific drive can be a good solution.

- Record everything during the course of testing. A simple manual logging sheet can be used for this purpose.

Record every testing activity. It will safeguard you against any consequences. Consider the fact; what if a production server comes down during the course of testing? Your recording and log of activities will make the incident very clear from your perspective; otherwise any problem may be directed to you. One simplest way to do this is log all outbound connections in your host based firewall and wipe them everyday.

- Send weekly status report to client and/or organize one follow-up meeting.
- Maintain sufficient record
  - It will support your findings and recommendations.
  - It will protect against un-necessary politics in which you may be accused of unprofessional, unethical or un-authorized practices
  - It will act as log repository to ensure recommendations are been addressed.
- Gather test information in structured order
  - Make folders as per domain name or task name
  - Give appropriate file names to test result files
    Ex:..IP-Address_Tool-Name_Option_Date-Time_other,
    111.222.111.222_Nmap_SYN-SCAN_020903-1530

5.2.2 Time of Assessment and Availability of Staff

- To reduce the down time, perform active assessment during off business hrs. Remember in this case you will not get a realistic picture of assessment. This is recommended while performing automated probing on critical devices.
- Make sure target organization staff is present during active assessment. It will reduce the down time just in-case if it occurs.
- ISSAF does not recommend any form of denial of service attacks (regular DoS or distributed DoS).

5.2.3 A mechanism for dealing with false positive to avoid calling law enforcement unnecessarily

- Alarms should be configured in such a manner so that only appropriate person(s) receive the warnings.
- Before calling law enforcement, senior management permission should be taken
- Senior management permission will even help in unnecessarily calling law enforcement.

5.2.4 Obtain IP Addresses or ranges that needs to be assessed

- Obtain IP Addresses or ranges (Network / Sub-network) that needs to be assessed
- Verify all the IP addresses (gathered through whois/dns and the received ones) with the tested company (prevent scanning somebody else …)
- Obtain information about any specific IP addresses / subnet, host, domain that should be restricted

5.2.5 Assessment Centre IP Addresses

- Inform client about Source IP address of assessment centre / machines from where a penetration test needs to be conducted. It will help client differentiating legitimate security assessment attack and from illegal hacker attempt.
- Make sure access to services from these access points is open from client firewall.

Add IP addresses where the tests are coming from to “white lists” if these are used (and if black lists with automatic blocking is used) to prevent a false sense of security when the results are presented.

5.3 PHASE – III: POST ASSESSMENT

After the assessment phase, the analysis and report submission activity starts. Various guidelines and good practices are suggested for various activities of this phase.

5.3.1 Reporting

5.3.1.1 PLANNING AND PREPARATION

Before starting the report writing process you should plan the activities for preparing and submitting the report. A great deal of effort is required to make a good report. It

really doesn't matter how good assessment you did if you don't convey it to client in appropriate format. It's generally seen people who perform assessment doesn't like making report of assessment and it's good to assign document writing part someone who has skills and interest in it.

- Organize the documentation based on the deliverable established.
- Ensure reporting documentation carries data classification.
- Ensure document control procedures are followed.
- Show preview of the reporting structure to the client before the final document submission.
    1. team meeting
    2. Responsibilities of team members
        a. Team Leader
        b. Assessors
        c. Technical writers
    3. Give appropriate data to appropriate team member

5.3.1.2 ANALYSIS

Analysis of test results shall be conducted on individual basis and with entire team (peer review). All the results should be shared with team members. Discuss should focus on vulnerabilities identified and verification of vulnerabilities based assessment conducted.

a. Who should perform analysis?
    i. Analysis by specific team member
    ii. Peer Review by another team member
    iii. Final Review by Subject matter expert.
b. Objective of analysis
    i. Determining current security posture of client. It helps while recommending safeguards.
    ii. Reviewing identified vulnerabilities and countermeasures for that
    iii. Removing any vulnerability if not appropriate
    iv. Reviewing recommended countermeasures if any
    v. Identifying more vulnerabilities

5.3.1.3 REPORT CREATION, MERGER AND FORMATTING

ISSAF recommends followings Structure for Report:

- Executive Summary
    - Scope of work
    - Nature of Assessment (Internal / External)
    - Summarized Out of scope work
    - Objectives
    - Time period of work Performed
    - Summary of findings with graphical chart
        - Assessment performed on number of systems/hosts
        - Total vulnerable hosts
        - Very-High risk vulnerabilities
        - High Risk vulnerabilities
        - Medium Risk vulnerabilities
        - Low Risk vulnerabilities
    - Findings at a glance as per domain
- Vulnerability Summary Review
    - Vulnerability summary report should include:
        - Name of vulnerability
        - Description of vulnerability
        - Severity of vulnerability
        - Effected system
        - Countermeasure to Safeguard the vulnerability
    - As per domain/assessed component severity of vulnerability should contain following information:
        - Very-High risk vulnerabilities
        - High risk vulnerabilities
        - Low Risk vulnerabilities
        - Informative vulnerabilities
        - None
- Action plan (all recommendations summarized into one table) with priorities assigned.
- Detailed Test Results with Countermeasures
    - Tools used
    - Date of test
    - IP address / Domain Name / Host / Device Name (as applicable)
    - Description of test
    - Tools plain output (logs)

- Analysis/Conclusion/Observation
- Countermeasure

5.3.1.4 FINAL REVIEW BY THE LEAD

Before sending report to client a final review shall be done by project lead and quality assurance for the project.

5.3.1.5 CLOSING THE DOCUMENT AND SENDING IT TO CLIENT

- Ensure Document control and data classification are implemented in the document.
- An Executive summary and a letter to client lead can be added.

5.3.2 Presentation

5.3.2.1 PRESENTATION WITH (TECHNICAL TEAM AND FUNCTION MANAGER)

- Produce an initial summary of vulnerabilities to analysis team before presentation.
  - Send report some days in advance of presentation. It should be mutually agreed with client as per availability of staff and convenience
  - Generally presenter should be the core person who has executed tests with good communication skills. He should understand that analysis team has technical and business, both kinds of people. It is his / her responsibility to make both people aware about this
  - Review and discuss all the finding and recommendations made to safeguard. Assessment team shall lead technical discussion
  - Have tools result with you for support while discussion

5.3.2.2 PRESENTATION WITH MANAGEMENT

Management presentation should carry the main summary of the assessment with supporting reasons of why, what, when, which, where and how. It should also include the key actions points. Presentation should include quantitative charts and tables of summarized information. This information matches the executive summary section of the report.

5.3.3 After Presentation

5.3.3.1.1 ACCEPTANCE CRITERIA IS MET

Ensure that the acceptance criteria are met. Refer Appendix for sample template. This template will contain all the test cases required to perform as per ISSAF.

5.3.3.1.2 ENSURE RECOMMENDATIONS ARE BEEN ADDRESSED

Ensure recommendations are been addressed. Follow-up for reasonable assurance that recommendations to plug the vulnerabilities is been addressed.

5.3.3.2 HELP CLIENT

Ensure client is not facing any problem to safeguard against vulnerabilities. Make sure you have answered all the questions regarding countermeasure to safeguard client organization. Ask client if he needs any other help before marking the assessment as closed since assessor may need to deploy his resources on some other projects.

5.3.3.3 MAINTAIN CONFIDENTIALITY OF CLIENT DATA

All information used before and during the project will normally be used in the reports generated to present the results of the security assessment. In order to maintain the confidentiality of this information, all reports and additional files (such as access log files, network traces and the like) must be kept and transmitted in a form that guarantees the confidentiality of the information, even in the event that storage media is misplaced or stolen.

Once stored, the information should be accessible on a need to know basis. The reports may include information regarding the need to patch software, harden systems, or establish firewalls, IDS or IPS systems. This kind of information should be made available only to the parties who should make infrastructure improvements following the recommendations produced after the security test.

Good practices / Guidelines	Compliance (Yes/No)	Comments
Do not disclose any client data to any person outside the project team. If shared it must be on the need to know basis and must not violate Non Disclosure Agreement (NDA).	✓	

Protect client data by encryption of stored files and folders.	✓	
Implement Host based firewall, Intrusion detection, Integrity check, updated Anti-Virus, latest patches and security on the server where client's data gathered during the course of assessment is stored.	✓	
Always use encryption during electronic transmission of client data.	✓	
Maintain a clear screen and clear desk policy with power on password and screen saver password on lab systems and/or system used for assessment.	✓	
Do not encourage or allow visitors, people other than team members to the assessment area. Meet visitors or other employees in conference room.	✓	
Refer client and project name by a code, don't call them by name.	✓	
Repair and prepare assessment machine on your own or in your presence.	✓	
Ensure assessor machine/desktop media is wiped and cleaned before handover to other team under any circumstances.	✓	
Ensure all clients related data (including CD's, floppies, and report copies, print out containing client data) is destroyed.	✓	
Take backup of client data in encrypted form and store this on optical disks in fireproof safes at Remote locations. Destroy this backup as client receives required data and it is not needed anymore.	✓	
No discussion of client assignments should be done in public areas or under the influence of alcohol	✓	
Take client related print outs on a secure printer and shred the unwanted hard copies.	✓	
All client related document including drafts must be marked confidential and have a cover page and distribution list on it	✓	

Have a policy, which defines action on violation of client data confidentiality.	✓	
Client Information should be stored on secure system in an encrypted manner, access controls are applied and access to information is given on need to know basis.	✓	
Client data like reports, proposals shouldn't be shared for business development and/or with expected clients.	✓	
Never ever share your previous client information with current employer.	✓	
Never ever share any client information in Articles, Papers and/or in News.	✓	
Desktop/laptops should have operating system which supports access control.	✓	

6 RISK ASSESSMENT

6.1 BACKGROUND

In today's extremely competitive business environment, organizations are being increasingly forced to reduce costs and increase profitability, the Senior Management of organizations worldwide are laying a greater emphasis on the Return on Investments (ROI) and Cost v/s Business Benefit of every dollar spent. Information Technology being an integral part of today's business environment is also required to demonstrate cost benefit justifications and an acceptable level of ROI for all IT spending. Information Systems Security is one IT investment that is constantly under the magnifying glass of the Senior Management, given the fact that millions of dollars are being spent on security assessments and implementations. To compound this further, the Senior Management also has to cope with a group of junkies who speak a strange language that is almost ethereal to them leading to greater scepticism amongst the Senior Management.

Given this scenario it has become extremely important for Information Systems Security professionals the world over to align their assessments and implementations with the business and its strategic business objectives. Demonstration of how and where Information Systems Security contributes to the business is of paramount importance today. To achieve this preceding a technology risk assessment with a business risk assessment is the order of the day in order to facilitate the integration of the business objectives with Information Systems Security objectives.

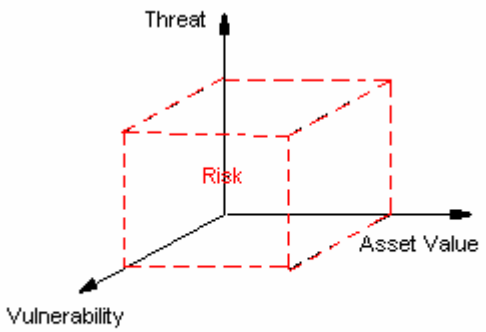
"Risk" can be defined as the potential loss suffered by the business as a result of an undesirable event that translates either into a business loss or causes disruption of the business operations. Performing a structured and methodical Risk Assessment facilitates the prioritization of the Information Systems Security initiatives from both technical and financial perspectives. Further it ensures the identification of risks in order of criticality to a business. It is important to note that risk assessments are a 'point in time' exercise, Information and Information Systems exist in a dynamic environment where the risks, threats and technology vulnerabilities of Information Systems Assets change rapidly. It would therefore be prudent of an organization to periodically assess its business risks from a technology perspective much similar to business's periodic reassessment of its business and operational risks.

Risk assessments are often an activity influenced by an organization's business, the nature of its operations and the role of Information Technology in business operations. A typical risk assessment process would involve the following:

- Understanding the strategic business objectives of the organisation
- Identifying key business processes that help the organization achieve its strategic business objectives
- Understanding the role of Information Technology within the business i.e. an enabler or a business support function
- Identifying key business risks that could result in any of the following:
    - loss or disruption of business operations,
    - financial losses
    - loss of reputation,
    - loss of operational effectiveness
- The value to the business of the assets that might be affected by threats
- Identifying the threats that the business may face irrespective of their probability of occurrence
- The vulnerabilities the business face with regards to these threats
- Prioritization of these risks
- An action plan to mitigate the risks by specifying milestones, entities responsible for implementing mitigating solutions and key performance indicators of these solutions.

Therefore, risk is a function of asset value, threats and vulnerabilities and can be calculated as follows:

RISK = ASSET VALUE X THREATS X VULNERABILITIES



Risk = Asset Value x Threat x Vulnerabilities

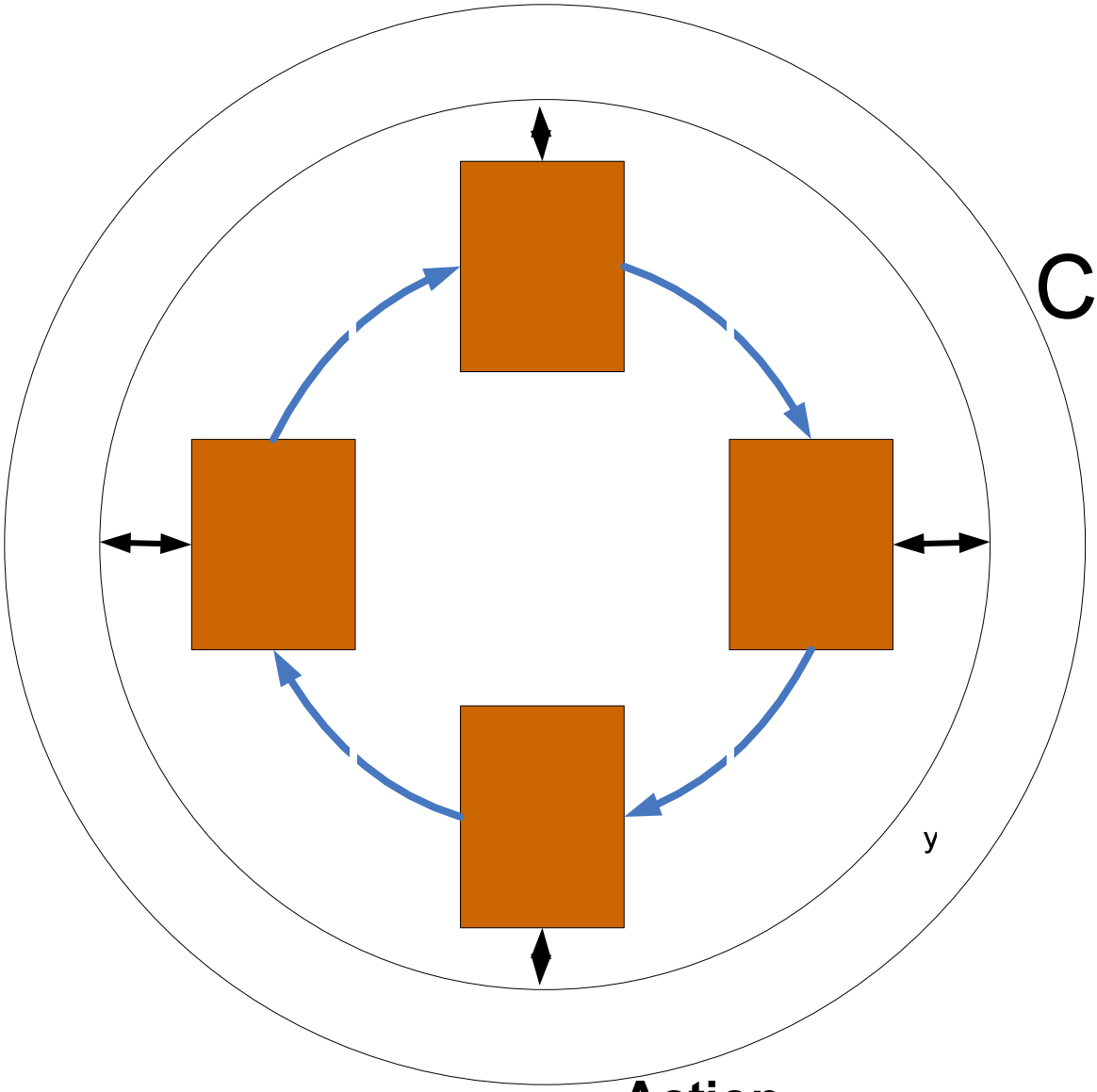
In brief, risk assessment is all about identifying valuable assets to the business, the threats that these assets face, the vulnerabilities that these threats can use to impact on the business and actions (controls and mitigating factors) to bring down these vulnerabilities thus reducing the risks to an acceptable level.

6.2 METHODOLOGY

The subject of risk assessment and actually how to carry out a risk assessment exercise can at first be confusing and mind-boggling. However, if some basic rules and the proper methodology are followed, a risk assessment exercise tend to be very fruitful and an interesting one for the business. This area of the framework provides you with practical procedures and tools to actually allow you to effectively run your own risk assessment exercise.

The exercise can be carried out through workshops where stakeholders of Information Systems brainstorm on the risks faced by the company and agree on the priorities. A “facilitator” is ideal for this kind of exercise to facilitate the workshop and keep discussions focused and within boundaries.

The overall process in a nutshell will be as follows:



Comm

Esta
the C

Objective

Stakehol

Assets

y

Action

Counter measures
implemen-
tation

y

Anal
Evalu

Agreeme
rating

Establish the Context

Objectives

The main objective of the risk assessment exercise is to identify risks and actions to be implemented to mitigate those risks and bring them down to an acceptable level. The output can be detailed in a document commonly termed a **"Risk Register"**. A risk register is a list of items comprising of the following:

- Assets classified by importance to the business
- Their related threats classified by their probability of occurrence
- Vulnerabilities classified by their criticality

Ideally, for the risk register to be effective, it needs also to include information regarding:

- Steps to be taken to mitigate those risks
- Responsibilities assigned
- Timeline for implementation for the controls

The above three areas allows for future monitoring and review.

Stakeholders

Stakeholders who should participate in the risk management exercise include, but are not limited to:

- CISO or ISO
- Senior management or owners' representative
- Functional management
- Subject Matter Experts
- End user community representative

The participants should ideally be experienced company employees well versed in the business strategy, objectives and values.

Assets

Asset Value can be known through an asset valuation exercise. Firstly the key business processes & the information assets that supplement these processes must be identified. These assets in most cases will have the highest scoring which in turn indicates their importance/criticality to the organization. Assets may also be evaluated for the tangibles like financial loss & regulatory impacts along with intangible factors like loss of customer confidence. E.g. an Internet Banking System

where consumers of Retail Bank logon & carry out financial transactions may have very high asset valuations as a break-in could cause significant financial losses as well as loss of customer confidence. The asset value would depend on:

- Cost of producing the information
- Value of the information on the open market
- Cost of reproducing the information if it is destroyed
- Benefit the information brings to the enterprise in meetings its business objectives or mission
- Repercussion to the enterprise if the information was not readily available
- Advantage it would give to a competitor if they could use, change, or destroy the Information
- Cost to the enterprise if the information was released, altered or destroyed
- Loss of client or customer confidence if the information was not held and processed securely
- Loss of public credibility and embarrassment if the information was not secure

There are generally two ways in which the company's assets can be valued – quantitative valuation and qualitative valuation. Quantitative valuation of assets involves the assignment of a monetary value to these assets based on the cost of the assets itself (if applicable) and the opportunity cost of that assets, that is what the business would lose in monetary terms should the assets become unavailable. Therefore,

Quantitative value of asset = Cost of asset + opportunity cost

More complex and in-depth mathematical methodologies do exist for asset valuation but are not covered in this version of the ISSAF.

However, the most widely used methodology remains the qualitative method of valuation due to its simplicity and ease of use and understandability. The qualitative method involves attributing a subjective qualitative rating to assets based on knowledge, experience and an understanding of the business. Therefore, it is crucial that there is common understanding and agreement between the stakeholders as to the importance and value of the assets to the business. This version of ISSAF focuses more on the qualitative nature of assets.

Although qualitative attributes are assigned to the assets, a value can still be assigned to these assets as depicted in the table below:

Asset Value	Assigned Value
Extremely Critical	1
High	0.8
Average	0.6
Low	0.4
Extremely Low	0.2

It is likely that, during a risk assessment workshop, there would be divergence of opinion between the stakeholders as to what constitute the value of an asset. For e.g., a DNS server is of utmost importance for an IS Manager to properly provide IS services. However, the same importance may not be perceived in the same way by Production Managers or End User representatives as they might not understand the criticality of this asset.

Therefore, it is important that the participants to the risk assessment workshops have a common ground of understanding for Asset Values prior to the workshop actually taking place. Ironically, the asset values are best understood by having and understanding the consequences following non-availability or disclosure of that asset (i.e. the business impact). The following table is useful to align all participants to the risk assessment exercise to the same level of understanding. The table is provided only as a brief example and guidance and risk assessors need to tailor it to the type of business and company in which they operate.

Rating	1. Facility	2. People	3. Reputation
Critical	Catastrophic facility damage with direct cost over $10 million	A large number of senior managers or experienced staff leave the company	International public attention, extensive adverse attention in international media National/international policies with potentially severe impact on access to new areas, grants of licenses or tax legislation Major loss of shareholder or community support
High	Major facility damage with direct cost of $0.5 – 10 million	Some senior managers or experienced staff leave High turnover of experienced staff Company not perceived as an employer of choice	National public concern, extensive adverse attention in national media Regional/national policies with potentially restrictive measures or impact on grant of licenses Mobilisation of action group Senior management displaced Significant decrease in shareholder or community support
Average	Significant facility damage with direct cost of $100k to 500k	Poor reputation as an employer Widespread staff attitude problems High staff turnover	Regional public concern, extensive adverse attention in local media Slight national media or local/regional political attention Adverse stance of local government or action groups Shareholders called to explain Decrease in shareholder or community support
Low	Moderate facility damage with direct cost of $10k to 100k	General staff morale and attitude problems Increase in staff turnover	Some local public concern Some local media or political attention with potential adverse aspects for company operations Shareholders directly involved Concerns on performance raised by shareholders or the community
Very Low	Moderate facility damage with direct cost less than $10k	Negligible or isolated staff dissatisfaction	Public awareness may exist, but there is no public concern

Identify

Threats – What can Happen?

Threats are events that could lead to potential damage & cause undesirable effects. An organization should perform a threat modeling exercise for its critical assets and develop and document its risks. E.g. Any information pertaining to the organization which may be for public viewing like press releases or systems hosting that information may have the least threats; hackers would not gain significant amounts of knowledge or information by breaking into these systems as information is already available. However in the case of an Internet Banking System there would be plenty of motivation for hackers to break-in to systems which could give them some financial gain. So a hacking threat to an Internet banking systems would typically receive a higher score as compared to a web server publishing press releases.

In the risk register, each threat should be clearly defined as an event that **could** happen, irrespective of the probability or likelihood of it occurring. Additionally, probability values can also be assigned to these threats as depicted in the following table:

Probability Rating	**LIKELIHOOD** The potential for threats to occur and lead to the assessed consequences		
1	Almost certain	Very high, may occur at least several times per year	A similar outcome has arisen several times per year in the same location, operation or activity
0.8	Likely	High, may arise about once per year	A similar outcome has arisen several times per year in the company
0.6	Possible	Possible, may arise at least once in a one to ten year period	A similar outcome has arisen at some time previously in the company
0.4	Unlikely	Not impossible, likely to occur during the next ten to forty years	A similar outcome has arisen at some time previously in an another company in the same industry
0.2	Rare	Very low, very unlikely during the next forty years	A similar outcome has arisen in the world-wide industry

The threat probability table is indicative only and risk assessor will need to customize this table to fit their perception of threat occurrences which the organization faced based on the industry and type of business.

Organisation generally cannot eliminate threats. However, what organizations can do is to mitigate and reduce their vulnerabilities which they face in front of these threats which in turn will lead to a reduction in the consequences as a result of those threats occurring.

For example, a company is known to be geographically situated in an area where the probability of earthquake is high. The earthquake is a threat. While performing their risk assessment workshop, the company realizes that they have a vulnerability because they do not have a disaster recovery site from where to resume operations if such an event is to occur. Therefore, the solution is to implement a disaster recovery site to reduce their vulnerability to the threats.

Vulnerabilities – How can threats affect us?

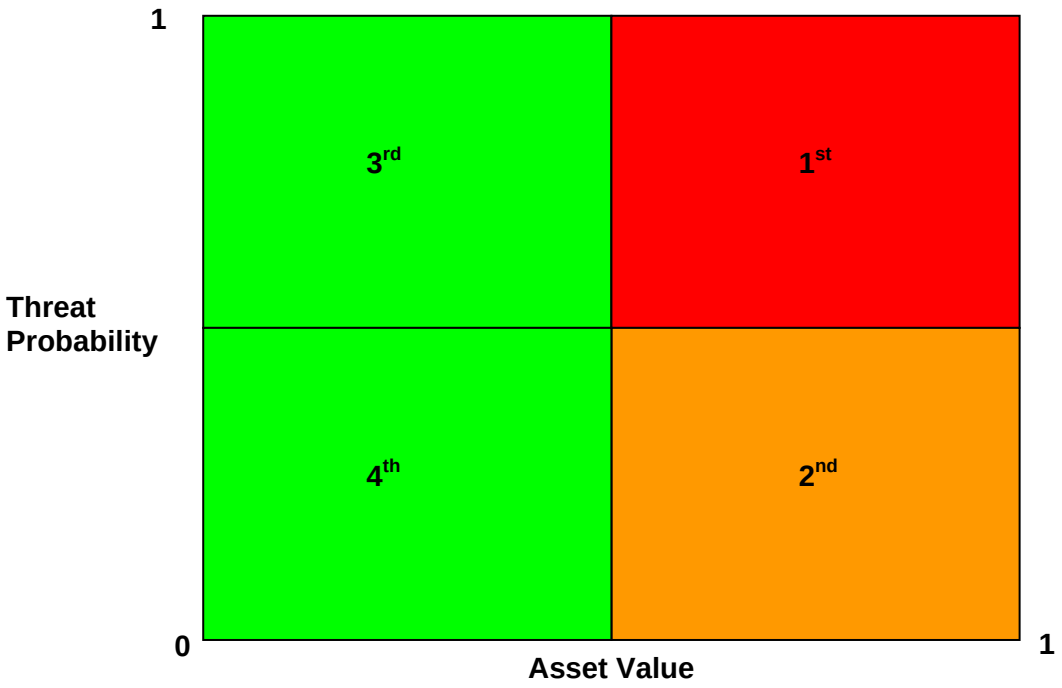
Vulnerabilities are weaknesses in systems that can be exploited for the threats to materialize. Vulnerabilities can be present within the operations, which could mean flaws in the process, or they could be weaknesses in the technology systems. Both types of vulnerabilities must be scored and a product of the two should signify a vulnerability score. Examples of process flaws could be a person having approved access could enter or modify information by the person who has input details regarding a financial transaction. Technology flaws could be weakness in the operating systems or applications the server is running. E.g. a vulnerability on the web server running the financial application. These flaws can be detected with a vulnerability assessment tool.

A rating method can also be assigned to the vulnerability levels as follows:

Vulnerability Level	Assigned Value
Extremely Vulnerable	1
Highly Vulnerable	0.8
Average	0.6
Low	0.4
Extremely Low	0.2

It is generally difficult to pin point technical vulnerabilities to the threats at first glance for Information Systems. Given that the threats which are most important are those which relate to high value assets, it is logical to start identifying vulnerabilities for

these threats first. The following quadrant depicts asset value against threats scenarios.



To clearly identify vulnerabilities to threats, consider using the **Controls Assessment** methodology described later in this framework. Although all vulnerabilities need to be identified for all threats at some point in time, vulnerabilities should generally be identified first for those high probability threats which might have an impact on high value assets (i.e., those threats which appear in the top right hand red quadrant).

Analyse and Evaluate

The "analyse and evaluate" activity of the risk assessment methodology consists mainly of communicating, discussing and agreeing upon the ratings with the concerned stakeholders regarding the value that needs to be assigned to:

- Asset Value
- Threats
- Vulnerabilities

Generally, this will ideally be performed and agreed upon in a risk assessment workshop.

Action

No proper risk assessment exercise will be complete unless:

- Clear comprehensive steps have been identified to mitigate the threats and bring them down to an acceptable level of risks
- Clearly defined responsibilities have been assigned – who should do what?
- A timeline for implementation for the controls or mitigating factors have been agreed upon.

The actions or mitigating factors which are identified in this part of the methodology is greatly depended on the participants' knowledge and expertise. Subject matter experts can also be required to assist in this process.

Additionally, the action plan serves as a road map for further monitoring and review of risks whilst performing periodic risk assessment exercise.

6.3 RISK ASSESSMENT TOOL

As a supplement to ISSAF, a basic spreadsheet-based tool has been developed to assist risk assessors in identifying and rating their asset values, threats and vulnerabilities.

The main worksheet is entitled "Risk". The following fields need to be input as follows:

- Column C (Optional) – ISSAF Domain Category – This field is for informational purposes only and allows the assessor to identify which area of the ISSAF domain is being considered while identifying and mitigating risks.
- Column D (Optional) – ISO 17799 Domain Category – This field is for informational purposes only and allows the assessor to identify which area of the ISO domain is being considered while identifying and mitigating risks.
- Column E (Optional) – Basel 2 Domain Category – This field is for informational purposes only and allows the assessor to identify which area of the Basel 2 domain is being considered while identifying and mitigating risks.
- Column F (Already populated) – Threat Category – The tool has been populated with threat categories. Assessors should customize the categories to fit their organization's environment.

- Column G (Already populated) – Threats – The tool has been populated with a list of threats. Assessors should customize the categories to fit their organization's environment.
- Columns H to M (Requires Input) – Assets value affected by threats. Identify the value of the assets being affected by threats.
- Column T (Computed) – Average Asset Value – The average of all values determined in Columns H to M
- Column U (Requires Input if necessary) – Override Asset Value. Given that the Average asset value might sometimes give a misleading indication of the true impact of enterprise overall assets, the assessor can input a subjective value to override the computed one.
- Columns W to AA (Optional) – Security Criteria – allows assessor to identify which security criteria the threat impacts on.
- Column AB (Requires Input) – Threat probability of occurrence. Identify the likelihood of occurrence of the threat.
- Column AF (Requires Description) – Provide a brief description of the current level of vulnerability of the enterprise
- Column AG (Requires Description) – Provide a brief description of the attack vectors that can be used to exploit the vulnerabilities
- Column AH (Requires Input) – Identify the current vulnerability level of the enterprise
- Column AM (Computed) – Risk Ranking
- Columns AN to AQ (Requires Description) – Provide descriptions of actions plans by specifying proposed countermeasures, responsibility assigned, implementation schedule and post implementation review and followup.

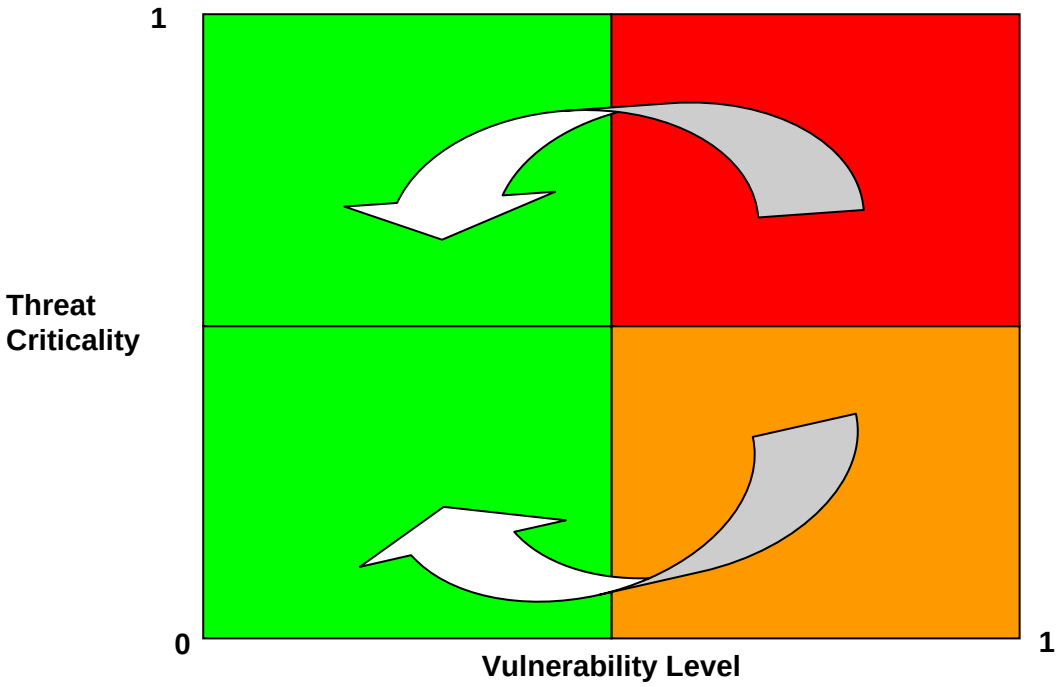
Some sample extracts of the tool with examples is iluustrated below:

1	B	C	F	G	T	U	V	AB	AC	AD	AE
2	**Threat No.**	**ISSAF Domains**	**Threat Category**	**Threats**	**Average Asset Value**	**Override Asset Value**	**Asset Value**	**Threat Probability of Occurrence**	**Threat Probability Value**	**Threat Criticality**	**Threat Ranking**
3	10	ESCA-Technical Control Assessment	Network Based	Session hijacking	0.40		0.40	Likely	0.80	0.32	4
4	13	ESCA-Technical Control Assessment	Network Based	Denial of service	0.70		0.70	Almost Certain	1.00	0.70	1
5	17	Business Continuity and Disaster Recovery Planning	Network Based	Failure of communication links	0.63		0.63	Unlikely	0.40	0.25	5
6	19	Operations Management	Host Based	Viruses	0.67		0.67	Likely	0.80	0.53	2
7	132	Business Continuity and Disaster Recovery Planning	Natural Threat	Fire	0.87		0.87	Possible	0.60	0.52	3
8	181	ESCA-Technical Control Assessment	Others	Unauthorized removal of property or media	0.70		0.70	Rare	0.20	0.14	6

1	B	AF	AG	AH	AI	AJ	AK	AL	AM
2	**Threat No.**	**Vulnerabilities**	**Attack Vectors**	**Vulnerability Level**	**Vulnerability Rating**	**Threat/ Vulnerability Rating**	**Threat/ Vulnerability Ranking**	**Risk Rating**	**Risk Ranking**
3	10	Weak physical security	An attacker can use several tools to combine spoofing, routing changes, and packet manipulation	Average	0.60	0.48	2	0.19	5
4	13	The inherent insecurity of the TCP/IP protocol suite	Brute force packet floods, such as cascading broadcast attacks	Average	0.60	0.60	1	0.42	1
5	17	Inappropriate redundancy/failover links	An attacker can bring down the network by flodding or attacking specific network device components	Highly Vulnerable	0.80	0.32	4	0.20	4
6	19	Inappropriate anti-virus deployment and monitoring systems	Viruses and worm propagation from external or internal sources	Low	0.40	0.32	4	0.21	3
7	132	Physical locations currently have manual fire extinguishers with no fire/smoke detectors	Natural threats	Average	0.60	0.36	3	0.31	2
8	181	Inappropriate security awareness of physical security personnel.	Use of Mass storage devices for data theft	Extremely Vulnerable	1.00	0.20	6	0.14	6

1	B	AN	AO	AP	AQ
2	**Threat No.**	**Proposed Countermeasures**	**Responsibility Assigned**	**Implementation Schedule**	**Post Implementation Follow Up**
3	10	Session encryption - using SSH for example	John Smith	3 months	
4	13	Filtering broadcast requests	George Brown	6 months	
5	17	Instate redundancy links	Carla Adams	3 months	
6	19	Appropriate anti-virus solution is already in place and operational. Monitoring procedures are adequately performed.	Carla Adams	6 months	
7	132	Implement appropriate smoke/fire detectors and automatic fire extinguishing capabilities	Jim West	9 months	
8	181	Implement software based solution to restrict the use of data to within the company asstes only.	John Smith	9 months	

The outcome of the tool is mainly a magic quadrant comparing vulnerabilities to their related threats probability of occurrence. The output is best described by the following diagram.



Since risk assessment is all about prioritizing threats and vulnerabilities which need to be addressed and mitigated first, all vulnerabilities in the upper left right red quadrant (i.e., the company is highly vulnerable to high probability threats) need to be addressed in priority. All resources and man power will be assigned to performing the agreed actions first. Subsequently, all vulnerabilities in the lower right hand

orange quadrant (i.e., the company is highly vulnerable but the probability of the threats to realize is low) will need to be addressed afterwards.

The rationale behind risk mitigation is to try to bring down the level of vulnerability to an acceptable level so that the company becomes immune to threats or have back up procedures and plan should the threat ever realize. Because it is very difficult to modify the probability of occurrence of threats, the company is better advised to use its resources to reduce the level of vulnerability.

The vulnerabilities identified in the remaining two quadrants are at the discretion of the company – whether they further want to reduce the risk. The key objective here of a risk assessment exercise is to take all reasonable steps to bring down the risk to an acceptable level.

From the tool, 2 scatter graphs can be generated as follows:

- Asset value to threat probability – Column V (x-axis) and Column AC (y-axis)
- Vulnerability to threat criticality – Column AI (x-axis) and Column AD (y-axis)

The tool also acts as and allows for the maintenance of a "Risk Register". A risk register is a complete listing of all risks which the business faces. In our model, the risks relate mostly to Information Systems. However, the tool can also be modified and extended to include other non-IS risks which the risk assessor deems fit to add.

6.4 Risk Assessment Methodology Evaluation

More than often, IS Security experts would be called upon to evaluate the security implementations in a company where risk assessment exercises were already carried out either using internal resources or by hiring external resources. Alternatively, he/she might be called upon to follow up on the action plan following the risk assessment exercise. This section depicts some of the things to look at while evaluating whether the client company has properly undergone a risk assessment exercise.

1. Does the risk assessment exercise at minimum include the following :
   1.1. How was the risk assessment performed? Did it include stakeholders? If so, were the stakeholders briefed and got a common understanding of asset value to and threats and vulnerabilities of the business?

1.2. Identification of all business critical information assets. (E.g., Data, paper documents, software, hardware etc.) ?
1.3. Threat identification to these assets?
1.4. Vulnerabilities assessment to the identified threats?
1.5. Identifying the risk scenarios for compromise of the assets via the vulnerabilities identified?
1.6. Assessing a probability of the risk scenario?
1.7. Assessing the impact on the business if the risk scenario were to come to pass?
1.8. Calculating the risk rating by multiplying the probability by the impact?
1.9. Prioritizing the risks based on the risk ratings?

2. Does the Organization conduct a comprehensive organization wide risk assessment exercise to reassess the threats, vulnerabilities and business impact for information security & is the Chief Information Security Officer (CISO) duly assisted by the respective Information Security Officers (ISOs) during this periodical risk assessment exercise?
3. Is there a Risk Assessment Template which is used as a general framework for the conduct of the risk assessment?
4. Is there a risk management plan developed to minimize the exposure of the company to the high risks that are identified?
5. Are the controls implementation instructions issued on the basis of the risk management plan, which will clearly identify responsibilities and timelines for implementation?
6. Does the CISO with assistance from the ISOs verify and validate the desired implementation actions within the stipulated time?
7. Are the details of the risk assessment, risk management plan and implementation will be preserved for a stipulated period? (3- 5 years)
8. Apart from the yearly risk assessment is a risk assessment carried out whenever there is a major change to the P&O network and systems such as addition of a new business application, relocation or redeployment of an existing application system, major changes to network architecture?

7 ENTERPRISE INFORMATION SECURITY POLICY

7.1 INTRODUCTION

Enterprise Information security policy demonstrates executive management commitment and direction for implementation and management of information security within the enterprise. Security policy also demonsrates adherence to the concept of due diligence and due care.

7.2 PRE-REQUISITE

1. Documented and formalized enterprise security policy and a formal policy on updates through scheduled reviews and a process for meeting any unscheduled changes.
2. Any audit/review reports of enterprise security policy conudcted either internally or externally. If a copy of policy can't be obtained, request for areas covered in policy/table of contents of policy.

7.3 OBJECTIVE

To establish whether the enterprise has formalized, implemented and communicated security policies with enterprise-wide applicability and supported by appropriate standards, procedures and guidelines within the enterprise.

7.4 ASSESSMENT QUESTIONNAIRE

This section contains a set of suggested evaluation check list that are expected to broadly fit the ISSAF based assessment process. Recognizing that each organization has its own unique processes, technologies and information processing architecture, it is possible that the ISSAF evaluation may need further steps to be performed. It is also possible that some of the suggested checks may need amplification. The assessor who is carrying out the ISSAF based evaluation should therefore use these check lists as guides and evolve a process that best fits the organization being reviewed.

	Evaluation Check	Yes	No	N/A	Evaluation Performed and Results
1	Does the organization have a formally approved and documented enterprise security policy?				

1A		Is the security policy approved at the apporpraite level of organizational heirarcy who has control over the disciplinary jurisdication of those who have to implement it?				
1B		Does the policy statement and attendent action by top management clearly demonstrate their commitment and support to security? If yes, identify all actions and processes that demonstrate commitment and support.				
2	Is the enterprise security policy available for review? If not has there been any third party review and if so is their report available for review?					
2A		If a third party review had taken place, evaluate: a)third party competence to carry out the review; b) the independence of the third party that has carried out the review				
3	Does the organization have documented enterprise security procedures, baselines, standards and guidelines? And are they available for review?					
	3A	If the organization has been certified to or accredited to a global or local information security or related control standard, is the creation and implementation of the security policy fuly in accordance with the requirements of those standards?				
4	Are the operational requirements and security concerns of all operating and support functions in the organization considered while deciding on the contents of the security policy? If yes, seek samples to see how these requirements were documented and met in the final version of security policy					
	4A	Has there been any instance where the operational requirements have dicated the compromise on the stringency of the security implementation and mangagement has accepted the need to meet operational exigencies and considered less than adequate security? If so, identify all such instanes and also indicate what compensating controls have been put in place?				

5	Does the policy include					
5.1	1) Management Statement on information security clearly spelling out the security stance of the organization					
	1A)	Statement on Access philosophy of the organization and if such philosophy is different for different locations or business divisions, are these clearly spelt out?				
5.2	Is there a Disciplinary Action policy Statement that clearly states a list of what would be regarded as violation of security and how are such violations classified? Are appropriate disciplinary actions prescribed for such violations?					
	5.2A	Have there been instances where perpetrators of or contributors to a security incident have been handled in a manner that is not fully in conformity with the requirements of the disciplinary actions as recommended in the policy? If so, has such exception handling been recorded and justificaitons noted?				
5.3	Scope & Applicability: Is the coverage and applicability clearly spelt out in the policy?					
	5.3A	Are there organizational units or locations that have been expressly excluded from the applicability of security policy? If so, is there a process whereby the relevence of bringing these units and locations within the purview of the security policy constantly reviewed?				
5.4	4) High Level Roles & Responsibilities					
5.5	5) Acceptable Usage guidelines for information systems users					
5.6	Information retention policy (e.g. how long to keep data in custody)					
6	Does the User policy address:					
6.1	Acceptable usage					
6.2	E-mail Usage					
6.3	Internet Usage					
6.4	Encryption of Sensitive Data					
6.5	Antivirus Policy					
6.6	Password protection					
6.7	Remote Access Policy					
6.8	Incident Reporting Guidelines					
6.9	Disciplinary action for non compliance					
7	Does the administrator & other IT staff policy address					

7.1	Physical & Environmental Security				
7.2	Network & Systems Security				
7.3	Wireless Security				
7.4	Application Development & Deployment				
7.5	Internet & Third Party Connectivity				
7.6	Vendor Engagement Policy				
7.7	Technology standards for the organization				
7.8	Technology change control				
7.9	Backup & Systems Availability				
8	Does the policy address the following areas for business owners				
8.1	Risk Assessment & Classification				
8.2	Outsourced service providers engagement				
8.3	Business Continuity & Disaster Recovery				
9	Does the policy address the following areas for security staff				
9.1	Monitoring & review of systems security events				
9.2	Systems vulnerability assessment & penetration testing				
9.3	Third party engagement review				
9.4	Incident response				
9.5	Business Continuity Planning & Disaster Recovery				
9.6	Security Awareness & training				
10	Is the policy communicated to the Organization employees via trainings?				
11	Does the policy go through an periodic review and accordingly updated ?				
12	Security Awareness and training for management and end users.				
13	Does the policy addresses concerns related to business ethics				
13.1	Is the Non disclosure agreement formally signed by employees?				
13.2	Does the compliance policy includes disciplinary actions?				

7.5 ASSESSMENT QUESTIONNAIRE - NARRATIVE

The following narrative supports the understanding of the contents and logic that is embedded in the assessment questionnaire. While the questionnaire is structured on the basis of possible process flow that may be found in many enterprises, the narrative is presented to aid an understanding of the concepts covered in this domain.

7.5.1 Overview

Information security policies support to implement effective security in an enterprise. Security policies are a statements that are derived from an alignment of information security to the business requirements, as endorsed by executive management of the enterprise. As it is emerging today, security policies are used as vehicles that communicate executive management commitment to securing information assets. In addition, these policies provide an overview of the security stance of an organization and credibility to security activities.

While the generic reason for having a comprehensive security policy is to demonstrate top management support to security activities and to ensure that appropriate directions are available for implementing the controls in the context of chosen security architecture, it is equally important from a legal perspective. When a corporation or its executive management is sued or questioned by stakeholders in the context of safeguarding assets (including information assets), one of the first things that would sought is to determine if the enterprise had a security policy in place commensurate with the nature and size of the business. This fits well into the concept of 'due care' that is expected of custodians of enterprise information assets. The creation and enforcement of an enterprise-wide security policy would also demonstrate that management went through the process of 'due diligence' and fully satisfies the 'prudent man rule.' It also protects employees so long as they can fully follow the security policies and demonstrate, when questioned, that they had adhered to what executive management expected them to do in terms of implementing security mechanisms. Two approaches are often seen in creation and implementation of security policies: bottom up approach and top down. The former is seen when IT departments (or a few in the department) try to create and implement a security policy. This is frequently done through the use of technology. This may not have the kind of visibility required or even the degree of credibility it deserves but this is very common occurrence. In contrast, top management drives the top down approach, which has the advantages of requisite funding, enforcement and visibility (or awareness). These two approaches still co-exist because IT and executive managements don't talk the same language; Management does not understand all the acronyms and jargons of IT while IT finds it difficult to understand the strategic business language. One quip often heard is that businesses are not in existence to buy more firewalls and spend on upgrading the IDS systems. Managers want a 'business case' established and IT finds it hard to fit into this approach not because they don't understand it fully but because IT still does not neatly fit into

known financial approaches to deciding on 'business cases.' Having said that, it must also be said in fairness to IT that managements also need to understand that their strategic competitive advantage depends significantly on the information technology and processing infrastructure they have deployed.

Guidelines for valuation of assets (used in a variety of ways – for assessing insurance premium, calculating the RTO while performing BIA, implementing access control models…) are best placed in the security policy since it is endorsed at the highest level in the organization. Another important role played by Security Policy is in the process of creating Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), which requires building on the layered defenses that the security architecture would have created. Fine tuning recovery strategy requires the definition of security parameters especially when the recovery is physically carried out at a location outside the premises of the enterprise. Security Policy has a significant contribution to make in this case.

Policies, apart from demonstrating executive managements' commitment to securing information assets, is also used as a vehicle to periodically reinforce security related messages, continuously raise security awareness and push for goal congruence between corporate goals and security goals. It is arguable as to who has to work for the goal congruence; is it to be done by the IT managers responsible for security to align it with corporate goals and objectives or should it be done by top management? The policy is also to be used for defining the various human interfaces of security. Primarily, the policy sets the framework for security organization structure, description of job responsibilities, constituting security teams (like security implementing team, security assessment team, A&P team, forensics team, assurance team, etc.) Organizations do not have all these teams functioning on a permanent basis but are quickly assembled whenever a security incident occurs or is suspected. Even the definition of what is security incident need clarity to move carefully between the extremities of complacence and over-reaction. All these are addressed in the security policy.

A further function of security policy is to provide clear guideline on how to handle a conflict that might arise when implementing a security mechanism. The conflict could be due to multiple locations in the same organization interpreting their security needs differently or due to different professionals interpreting a security situation differently

or even a basic question like 'Is this a security breach?' The policy assists managers to take a consistent, fair and appropriate stand in the face of these conflicts.

7.5.2 Policy and Trust

Information Security policies, like every other enterprise policy, involves people. Policies are designed and implemented so that the actions and interactions of people among themselves and with the constituents of Information Processing Facilities, Trusted Computing Base, etc. are consistent with the enterprise security stance. The moment we talk of interaction amongst humans, it involves trust related issues. Policy writers take two extreme stand points though most of the policy designers tend to tread the middle path. One extreme is to state that policies are written only because we always think people will not do the right things. Other extreme is to design polices on the presumption that people would do only the right things! As can be readily seen, neither of these extremes are always true. Even if we desire to trust all systems and people, what is witnessed over the past force us to move away and start distrusting people and processes. Software from reliable sources suddenly throws up a bug or someone discovers a Trojan in it or a backdoor carefully concealed! A trusted person gets into a problem when on vacation and the stand-by colleague discovers something odd – leading to a trail of frauds! When a security policy is written, conservatively it may be prudent not to totally trust any person or process to function correctly always and under all conditions. Trust takes time to build. Careful monitoring over long periods can build sufficient trust to break parts of control if such control dilution can add to other advantages - most importantly effectiveness in operations or a general feeling of goodness, which could lead to greater efficiencies in operations. There are no hard and fast rules on trust; it depends on a variety of variables including organizational culture and the sensitivity of information asset being handled. Determining the right level of trust is a delicate and very difficult task; too little of it may lead to high attrition rates or low morale and too much might eventually result in security infractions. Maintaining the right level of trust is a good acid-test for successful mangers.

7.5.3 Some issues of design

Policies affect the way people work. It is therefore a good practice to work on a consensus-based policy development and implementation wherever possible. While it is not always possible to get a consensus on all policy issues due to a number of

factors, it would be worthwhile to get all those who would be affected by the implementation of the policy to review the policy and share their views as to how the proposed policy could impact their work – in terms of productivity, personal efficiencies, adherence to best practices, impact of changes from what is currently happening, etc. At the stage of eliciting this consensus, if it is demonstrated that the implementation of a policy would result in an unfavorable situation, it may be worthwhile re-visiting the policy.

It is important to review the policy with the IT support staff just as being done with users since IT support staff would be involved heavily in the implementation of the policy. Since implementation of a policy is as important as designing it and monitoring it, the IT support function that would be involved in implementation should be fully involved in this process. Often the views of the IT support staff results in significant enhancement to the degree of controls and the manner of implementing controls.

Security Policies, like all other corporate polices and plans tend to get out-dated and obsolete. A clear process of change management needs to be put in place to ensure that any policy changes take place along side any changes in any of the attributes that has an impact on the policy. A clear process of putting in place a version control is also to be built and implemented so that different parts of the organization do not conform to different versions of the policy!

Policies that are not appropriately disseminated are no policies at all. All users and anyone who is in any way connected with a policy implementation should have a copy of the policy and the policy dissemination process should include a way of getting the users and others to acknowledge, in unambiguous terms, that they have received a copy of the policy, studied and understood it and agree to abide by it. This document is a must for the organization to enforce the policy and also ensure that where the policy is violated, no defense is taken in a court of law by the person who violated the policy that he / she did not know of the existence of such a policy. Continuous awareness must be created through a variety of ways including security awareness programs, policy awareness workshops and regular stress in corporate internal communications that adherence to policies will result in better security.
While this chapter's objectives are to help a user assess an existing security policy, it also attempts to give a user enough knowledge to key factors to consider in

formulating a security policy & the critical components that should be included in the security policy.

7.5.4 Security Policy Development Model for Security Policies

7.5.4.1 Establishing a Policy Template

The Risk Assessment Methodology, the classification levels & the security services needed for securing the information systems are good guiding principles to establish a security policy for the entire organization. The Legal department should also ascertain that the statements within the policy are in compliance with the Local Regulations & other privacy laws. The policy should have disciplinary statements that mention the punishment meted out in case there is non-compliance to the policies. The policies could be high-level statements that could talk about the management's intention to treat information security within the firm on priority and it may also be detailed in terms of outlining various controls & strategies the firm may use to secure the information.

7.5.5 The Policy must address:

7.5.5.1 Management Statement on Information Security

This statement shall include the management's commitment & support to information security within the organization. This will also encourage other business units to participate in the information security program for the firm.

7.5.5.2 Disciplinary Statement

The policy must include a statement, which should talk about the disciplinary process which shall be taken in case there is a non-compliance with the policies mentioned below. Disciplinary measures can be up to termination of employment.

7.5.5.3 The security organization & the roles and responsibilities

This section should include the various roles in the information security program. This should include at minimum the role of the Information Security Officer, the information owners, the end users, the systems administrator & the end users.

7.5.6 For the End-Users

7.5.6.1 Acceptable Use of Computer Systems & Resources

This policy talks about how information systems are important to the organization and it also talks about prudent usage of computer systems by the employees. Most organizations have a policy mentioning that all data stored on the organizations computer systems belongs to the organization & that the employee activity may be monitored.

7.5.6.2 E-mail usage policy

This policy talks about prudent usage of e-mail resources. This means that the employees can use the e-mail system for personal purposes as long as there isn't significant usage of the organization bandwidth.

7.5.6.3 Internet Usage

Internet usage is mostly granted to employees requiring access for business purposes. Employees are also advised against posting any comments on websites with the company e-mail id unless authorized to do so.

7.5.6.4 Encryption of Sensitive Data

Employees should be advised to encrypt sensitive information before sending it on the Internet using the firms approved products. They should also confirm the identity of senders and ensure that it is from an authentic source before using information sent to the users.

7.5.6.5 Anti-Virus Policy

The anti-virus policy should advise users about scanning attachments before getting them from external sources. They should also report virus incidents to the concerned people that could help in containing the viruses/worms before they start spreading to other systems.

7.5.6.6 Password Protection Policy

Password protection policy talks about the selection of passwords & password complexity and other parameters like password change frequency; history

7.5.6.7 Remote Access Policy

The remote access policy asks users to ensure that all controls like personal firewalls etc are running well before they connect to the firms systems. This should also create awareness among users about the possible installation of key loggers and other Trojans while connecting to the firms systems from the internet or other untrusted networks.

7.5.6.8 Incident Reporting Policy

This policy should educate the users on possible security breaches and the way these incidents to be reported to the concerned authorities.

Some Companies ask the employees to sign the Intellectual Property Rights agreement so that the Company's IPR is safeguarded. The IPR Agreement needs to be prepared according to the company's business needs and in consultation with legal Department.

7.5.7 For the Information Owners

7.5.7.1 Risk Assessment & Asset Classification

The information owners should be entrusted with the Risk assessment & classification of the information systems in their purview. They along with the representatives form the information security department must classify & label the data by analyzing the threats. In case of shared systems across multiple business units the business managers must co-own the data & all of them must be involved in the risk assessment exercise. Information owners must be entrusted with the responsibility of completing the Risk assessment exercise and the information security representatives must act as consultants in facilitating this process.

7.5.7.2 Outsourced service providers engagement policy

The information owners must notify the information security department about possible engagements with outsourced service providers before establishing a relationship. The information security department should analyze if the service providers meet the minimum criteria required so that the organizations data can be entrusted to the service provider's Service Level Agreements (SLA) Needs to be defined for the Outsourced agency.

7.5.7.3 Business Continuity & Disaster Recovery Policy

The information owners must be advised to make continuity plans in case of exigencies. The BCP team or the Information Security team would facilitate this process. This also requires the information owners to maintain the required call trees and establish DR processes for the businesses information systems.

7.5.8 For the IT Department

7.5.8.1 Physical Security of Information Systems

This policy must advise the IT Department or other departments (Administration) to deploy all possible security controls to protect the information systems from damage, loss & theft. This may require deploying & operating some controls like a PACS (Personal Access Control System). This should also talk about equipment sitting & procedures to be followed when physical access is required (like maintaining a log of all access to the server systems). This should also address procedure for operating environmental controls

7.5.8.2 Network & Systems Security Policy

This should discuss the security mechanisms to be implemented on Network & Server systems. The main criteria for configuration of systems should be that access should be granted to resources as required.

7.5.8.3 Wireless Security

This is an area which is a matter of grave concern. The wireless systems should be properly configured with adequate authorization & authentication methods.

7.5.8.4 Application Development & Deployment

The application development & deployment policy should talk about how security should be a consideration at the time of application development itself. The policy should also discuss means in which the application must first be unit tested , then tested on an integration environment and only after it passes the security tests should it be deployed on the production systems.

7.5.8.5 Internet & Third Party Connectivity

This policy should talk about secure connectivity to the internet & third parties. The organizations acceptable method for external connectivity & the authorization process for the same should be discussed. Some organizations conduct a penetration test on the third party networks before allowing connectivity into their systems.

7.5.8.6 Vendor Engagement Policy

The vendor engagement policy would discuss what minimum security criteria a vendor must adhere to before the organization can establish a relationship. E.g includes a vendor should have a proper background check of all its employees before the vendor representatives work with the organization.

7.5.8.7 Backup & Systems Availability Policy

This policy entrusts the proper functioning of the network infrastructure & backup of information systems to the IT Department.

7.5.9 For the Information Security

7.5.9.1 Monitoring & Review of System Security Events

The information security team should be advised to check the security events on a regular basis and report breaches or incidents serious in nature to the management. The information security team should regularly monitor for any non-compliance to the security policy as well & work with the business units to have those rectified

7.5.9.2 Systems Vulnerability Assessment & Penetration Testing

The information security department is often entrusted with the responsibility of conducting vulnerability assessment & penetration tests. This policy talks about how these must be carried out with proper authorization.

7.5.9.2.1 Third Party (Vendor & Outsourced Service Providers) Engagement Review

The information security team may be required to go onsite & conduct reviews of the Services providers & vendors to ensure that they comply to the minimum security criteria as required by the organizations. This policy details the information security roles in the process.

7.5.9.2.2 Incident Response

The incident response policy details the method of investigating any reported security breaches. How & when law enforcement agencies must be contacted & who should be responsible for communicating with the media should be covered.

7.5.9.2.3 Business Continuity Planning

The information security department should also be facilitating the BCP for various business units & should review test results & appraise the management about the same.

7.5.9.2.4 Security Awareness & Training

This is an often-overlooked subject; the information security department must be responsible for training all users in the organizations. They must also design & constantly update their security awareness programs.

8 ENTERPRISE INFORMAITON SECURITY ORGANIZATION & MANAGEMENT

8.1 INTRODUCTION

Information security organization is an important part of the management control struture in an organization. Assessment of the organization structure and management responsibilities are important since these determine if the organization can be aligned to the security stance of executive management. This also stems from the belief that security cannot be achieved only by technology or services and it needs to be ingrained into the overall organizational funtioning. One sure way of examining if executive management has taken congnizence of the need for a comprehensive security stance is to assess the secuirty organization.

8.2 PRE-REQUISITE

Organizational structure of entire organization, IT department, enterprise security organization, internal audit. Document containing formally approved roles and responsibilities, job description for enterprise security functions, any third party assessment/review etc...

8.3 OBJECTIVE

The primary objective of this assessment is to assess the fomal organizational controls that are related to organizational structure. Also, to evaluate management support to the security functions, identify segregation of duties, third party security and to address outsourcing security concerns.

8.4 ASSESSMENT QUESTIONNAIRE

This section contains a set of suggested evaluation check list that are expected to broadly fit the ISSAF based assessment process. Recognizing that each organization has its own unique processes, technologies and information processing architecture, it is possible that the ISSAF evaluation may need further steps to be performed. It is also possible that some of the suggested checks may need amplification. The assessor who is carrying out the ISSAF based evaluation should

therefore use these check lists as guides and evolve a process that best fits the organization being reviewed.

	Evaluation Check	Yes	No	N/A	Evaluation Performed and Results
1	Management Support				
1.1	Does the organization have a formally approved enterprise security organization?				
1.2	Is there adequate management support for the information security within the orgainzation?				
1.3	Has the Chief Security Officer/Chief Information Security Officer (CSO/CISO) been formally authorized to ensure that other departments implement recommendations made with respect to security?				
	1.3A Does the CSO / CISO have a role in the determination of the implementation process of the Enterprise Security Policy?				
	1.3B Is the performance of the CSO /CISO related or linked to the successful implementation of the enterprise security policy?				
1.4	Are the responsibilities for each of the roles in the information security department clearly defined?				
	1.4A Are all personnel including users of information systems clearly informed of their "security related" roles and obligations?				
	1.4B Is adherence to security policies and "good security practices" considered as part of the assessment of overall performance of all personnel who use information system in their regular work cycle?				
1.5	Does the IT department organization chart and position description clearly define relationships with various departments in general and in particular, the following departments?				

1.5A	The HR department… For instance, is there a clear rsponsibility for the HR department to insist on the IT department certificate of "no-access privileges" before an employee is relieved from the services of the organization?				
1.5B	The various business departments... Does the IT / IT security organization have a clear relationshp that indicates that whenever business processes are altered, it needs to be routed through IT Security department for process security clearance?				
	Legal Department … Is there a clear process of interaction between the Legal Department and the information security department to ensure that the security processes are in line with the requirements of local, regional, industry and national laws				
	The employees of the company … is there a clearly defined security awareness program that is regularly reviewed and updated so that all employees of the enterprise are informed of their appropriate role in maintaining the security of the organization in accordance with security policy?				
	Administration Department (This generally takes care of the In-house activities and facility management in some companies)				
2	Segregation of duties				
	Is there any conflicting or overlap of the roles that can potentially cause the security to collapse? E.g. Enterprise security personnel reporting to IT department.				
	Are there proper segregations of duties within the information security department?				
	Is there any overlap of responsibilities due to this segregation of duties?				
	Are two-person control exercised within the company?				
	Are mandatory vacations implemented for enterprise security personnel?				

	Are peer review performed on enterprise security if applicable?				
3	Third party security concerns				
	Is there any formally approved policy regarding third party access to enterprise information systems (Physical and Logical)?				
	Is there any compliance review performed to ensure third party access to enterprise information systems are based on approved policies?				
	Are there formally signed off documentation for approvals and reviews on third party access?				
4	Outsourcing				
	Is there any legally defined contract between both parties for outsourced security services / solutions?				
	Has this contract been reviewed by the legal department for any legal and regulatory compliance?				
	Does the contract contain Non disclosure clause relating to enterprise information assets?				
	Is there any clause specifying damages to be paid in the event of non compliance?				
	Has enterprise performed a security evaluation of outsourcer's information systems used in delivering the services? If not has there been a third party review of outsourcer's information systems in delivering the services.				
	Is there any process to evaluate the services provided against the service level agreements?				
	Does the SLA or the agreement clearly permit the enterprise staff or auditor to assess and review the security settings of the party to which service delivery is being outsourced?				
	Is there any process to terminate the contract?				

8.5 ASSESSMENT QUESTIONNAIRE - NARRATIVE

The following narrative supports the understanding of the contents and logic that is embedded in the assessment questionnaire. While the questionnaire is structured on the basis of possible process flow that may be found in many enterprises, the narrative is presented to aid an understanding of the concepts covered in this domain.

8.5.1 Introduction

The security organization plays a vital role in the effective implementation of policies & in maintaining the overall security posture of a company. Most companies generally consider information security as information technology security. The scope of information security is much more broader than just IT security since information in an organizational context extends beyond data processing and computers and therefore involves a lot of interaction with other business departments. For such reasons, some argue that it is best to have the Information security aligned to the Operations Department. Organizational status and independence of the information security function has a significant impact on the effectiveness and efficiency of the security function. Traditional organization theory has it that the higher the head of a function reports to, the greater is the independence of that function. While this has been challenged in a few studies, we can safely recommend that for optimal levels of organizational independence, the head of Information Security Organization should report to the head of the organization. Everything else is a compromise. There are a few who argue that information security being too technical a matter, the head of security operations should ideally report to the CIO. That approach merits little attention since the CIO is responsible for the efficient and effective use of the information assets for furthering business objectives and the function of protecting information assets is too specialized to be bracketed with operational responsibilities. It also matter as to how information is viewed in the organizational context – is it seen as a support function, or as an enabling function or as a driver or as a function that directly contributes to creating and sustaining strategic competitive advantage. This perception best drives the organization structure of the security organization and its responsibility – authority paradigm.

There are a number of organization driven controls (also referred to as Administrative Controls) that add to the overall security of the organization's information assets without necessarily resorting to technology for conceptualization or implementation.

8.5.2 Segregation of Duties

Segregation of duties is a very important administrative control in information security. This is achieved by ensuring that no complete operation cycles are completed by a single individual or no operation cycles that have significant security content is completed by a single individual. The various duties constituting a

transaction cycle is segregated and given for completion by two or more people who are normally peers. If the duties are segregated the chances that certain privileges may be misused are reduced greatly. If the system administrators' role is to create user accounts and give access to system users & also ensure optimal performance of the systems. All this activity can be logged and monitored by staff dedicated to doing system monitoring. Only collusion by individuals from the two roles can bypass the security provided by this approach.

Structure based Controls

Similarly it might make sense to split up the duties in the information security organization as well. E.g. having a separate Information Risk Management team & information security team might help in segregation of duties. The information risk management team can conduct risk assessments and advise the various business groups on the steps needed to be in compliance with the company's Information security policies. The information security staff should be made responsible to see to it that required controls have been implemented & have the information risk management team report on their effectiveness. This avoids any complacency in the information security team & an authentic report is created because this is done by the IRM whose goals are to find & report on the security flaws within the information systems deployed.

Another important part, which determines the company's security is the Internal Audit Department. This department should never be aligned to the information security and should ideally report to the CEO of the company. The internal audits responsibilities are to check compliance with the organizations security policies & report any anomalies found to the concerned authority. The audit is generally a half yearly or yearly exercise & can be considered as very rigorous checks of the controls deployed within the company.

8.5.3 Two-person Controls

Another form of administrative control that harnesses the organization structure is two-person controls. In this situation, the rationale is similar to that which justifies segregation of duties. However, unlike segregation of duties that require two persons to do different but sequenced operations to complete a process cycle, in the case of two person controls, two persons simultaneously perform certain operations so that in the absence of one, the other cannot complete the process or operation.

8.5.4 Peer Review

Unlike a supervisory review which comes with its share of psychological and behavioral issues, the concept of peer review of security operations have come to be accepted amongst security professionals as a good organizational control mechanism. In this process, the work of one person is reviewed by his/her peer. The peer is often as knowledgeable as the person who performed the operation. A healthy competition exists which assists the organization to have a higher degree of expertise brought into play. Of course, it also grants the organization the additional layer of security since the peers, being professionals, would bring to light any attempted actions by any person that would result in a security infraction; whether such action is with malicious intent or due to ignorance or negligence.

8.5.5 Mandatory Vacations

This form of administrative control has been recommended for quite some time now has yielded good results in organizations that had implemented it. This control stems from the belief that anyone involved in a security infraction would be able to hide it successfully so long as he/she is able to be present at the place of security violation and can continue to cover up the violation. It is therefore recommended that every person involved in any operation that has a security element in it should be asked to go on regular vacation. The obvious reason being that while the person is on vacation, his/her successor who handles the operations would find any security infraction that had been carefully concealed by the earlier person.

8.5.6 Information Security Roles and Responsibilities

The effectiveness of any Information Security Management framework is dependent on the personnel who administer the security implementation. This would depend on how effectively the enterprise assigns and manages the roles and responsibilities for the implementation and management of Information Security.

The assessment of an Information Security Framework would also comprise of a review of the specific roles and responsibilities allocated to specific groups or individual personnel of an enterprise. Some of the key roles are responsibilities are listed below along with specific responsibilities that would be ideally allocated to such roles.

8.5.6.1 CHIEF INFORMATION SECURITY OFFICER

The Chief Information Security Officer (CISO) is the senior most position in a security management organization within an enterprise. The CISO's role will at a minimum include the following responsibilities:

- Identification of the strategic direction of Information Security within the enterprise
- Ensuring alignment of information security objectives with the strategic IT plan and the strategic business objectives of the enterprise
- Ensuring alignment of the security management objectives with the risk management objectives of the enterprise
- Ensuring the alignment of the information risk management framework with the risk management framework of the enterprise
- Ensuring appropriate security management organization and infrastructure is implemented in the enterprise to ensure that the information risks of the enterprise are appropriately managed
- Ensuring the effectiveness of the information risk identification and management process of the enterprise

8.5.6.2 PHYSICAL SECURITY MANAGER

The Physical Security Manager's role is responsible for the management the security of the physical facilities related to Information Technology implemented within an organization. Such responsibilities will at a minimum include the following:

- Implementation and management of physical access controls at each of the facilities of the enterprise
- Implementing and sustaining suitable environmental controls to ensure that an appropriate environment is provided for the infrastructure of the enterprise
- Ensuring the upkeep of the facilities in accordance with any enterprise facilities management policies or applicable best practices

8.5.6.3 INFRASTRUCTURE SECURITY MANAGER

The Infrastructure Security Manager's role is responsible for the management of security of specific infrastructure components of the IS infrastructure of the enterprise. This would include:

- Implementation and management of logical security of infrastructure components comprising of the following:
  - All hardware
  - All security infrastructure devices/components

- Coordination with the Network and Application / Database Security Managers for configuration management
- Maintenance and management of the configuration of the components
- Implementation of the Information Security Policies, Procedures and Minimum Baseline Standards for configurations
- Conduct of periodic reviews of the security configurations of the components
- Appropriate application of the change management processes for management of patches, upgrades, installation and maintenance activities pertaining to the specific components under his control

8.5.6.4 NETWORK SECURITY MANAGER

The Network Security Manager's role is responsible for the management of security of specific network and telecommunication components of the IS infrastructure of the enterprise. This would include:

- Implementation and management of security of network and telecommunication components comprising of the following:
  - Routers
  - Bridges / Switches
  - Network Cabling
  - ISP connectivity
  - Enterprise sites connectivity
  - Other network components as applicable
- Maintenance and management of the configuration of the components
- Implementation of the Information Security Policies, Procedures and Minimum Baseline Standards for configurations
- Conduct of periodic reviews of the security configurations of the components
- Appropriate application of the change management processes for management of patches, upgrades, installation and maintenance activities pertaining to the specific components under his control

8.5.6.5 APPLICATIONS & DATABASE SECURITY MANAGER

The Application and Database Security Manager's role is responsible for the implementation and management of application security and logical security of both applications and databases of the Information Systems used within the Enterprise. The specific responsibilities would include the following:

- Maintenance and management of the configuration of the applications and databases
- Implementation of the Information Security Policies, Procedures and Minimum Baseline Standards for configurations
- Conduct of periodic reviews of the configurations of the applications and databases
- Appropriate application of the change management processes for management of patches, upgrades, installation and maintenance activities
- Management of user access to the applications and databases

8.5.6.6 SECURITY COMPLIANCE MANAGER

The Security Compliance Manager's role is responsible for ensuring the compliance to the Information Security Policies, Procedures and associated Standards, Guidelines and MBS by all personnel of the enterprise. This is one of the most critical roles in the Security Organization and Management process of an enterprise's security posture. The Security Compliance Manager's responsibilities will include the following:

- Performing periodic security reviews and assessments of the technology infrastructure of the company
- Researching and recommending best practices of Information Security management and implementation within the Enterprise.
- Being a proactive catalyst to identification and management of Information Security within the enterprise

9 ENTERPRISE SECURITY & CONTROLS ASSESSMENT

[This page is intentionally left blank.]

PERSONNEL SECURITY

[This section is not complete yet]

INTRODUCTION

People are greatest assets of any enterprise and require specific attention to recruitment, promotion, personnel clearance, training, performance evaluation and job change termination.

PRE-REQUISITE

OBJECTIVE

The objective is to assess:

- That security responsibilities are addressed at recruitment stage and in contracts and monitored durring recruitment.
- That potential recruits are appropriately screened.
- That all employees and third party users of information processing facilities sign a confidentiality agreement

ASSESSMENT QUESTIONNAIRE

This section contains a set of suggested evaluation check list that are expected to broadly fit the ISSAF based assessment process. Recognizing that each organization has its own unique processes, technologies and information processing architecture, it is possible that the ISSAF evaluation may need further steps to be performed. It is also possible that some of the suggested checks may need amplification. The assessor who is carrying out the ISSAF based evaluation should therefore use these check lists as guides and evolve a process that best fits the organization being reviewed.

	Evaluation Check	Yes	No	N/A	Evaluation Performed and Results
	Is personnel screening implemented by controls? - Reference check eg one business and one personal - Check for correctness of				

	candidate's resume - Identify check by passport or similar document				
	Is the employee's terms and condition of employement: - States responsibilities with respect to information security - States legal responsibilities and legal rights are clearly defined				

TECHNICAL CONTROLS AND SECURITY ASSESSMENT

[This page is intentionally left blank]

A UNDERSTANDING ASSESSMENT TRENDS

[This page is intentionally left blank]

B PENETRATION TESTING METHODOLOGY

The ISSAF Penetration testing methodology is designed to evaluate your network, system and application controls. It consists three phases approach and nine steps assessment. The approach includes following three phases:

- Phase – I: Planning and Preparation
- Phase – II: Assessment
- Phase – III: Reporting, Clean-up and Destroy Artefacts

B.1 PHASE – I: PLANNING AND PREPARATION

This phase comprises the steps to exchange initial information, plan and prepare for the test. Prior to testing a formal Assessment Agreement will be signed from both parties. It will provide basis for this assignment and mutual legal protection. It will also specify the specific engagement team, the exact dates, times of the test, escalation path and other arrangements. The following activities are envisaged in this phase:

- Identification of contact individuals from both side,
- Opening meting to confirm the scope, approach and methodology, and
- Agree to specific test cases and escalation paths

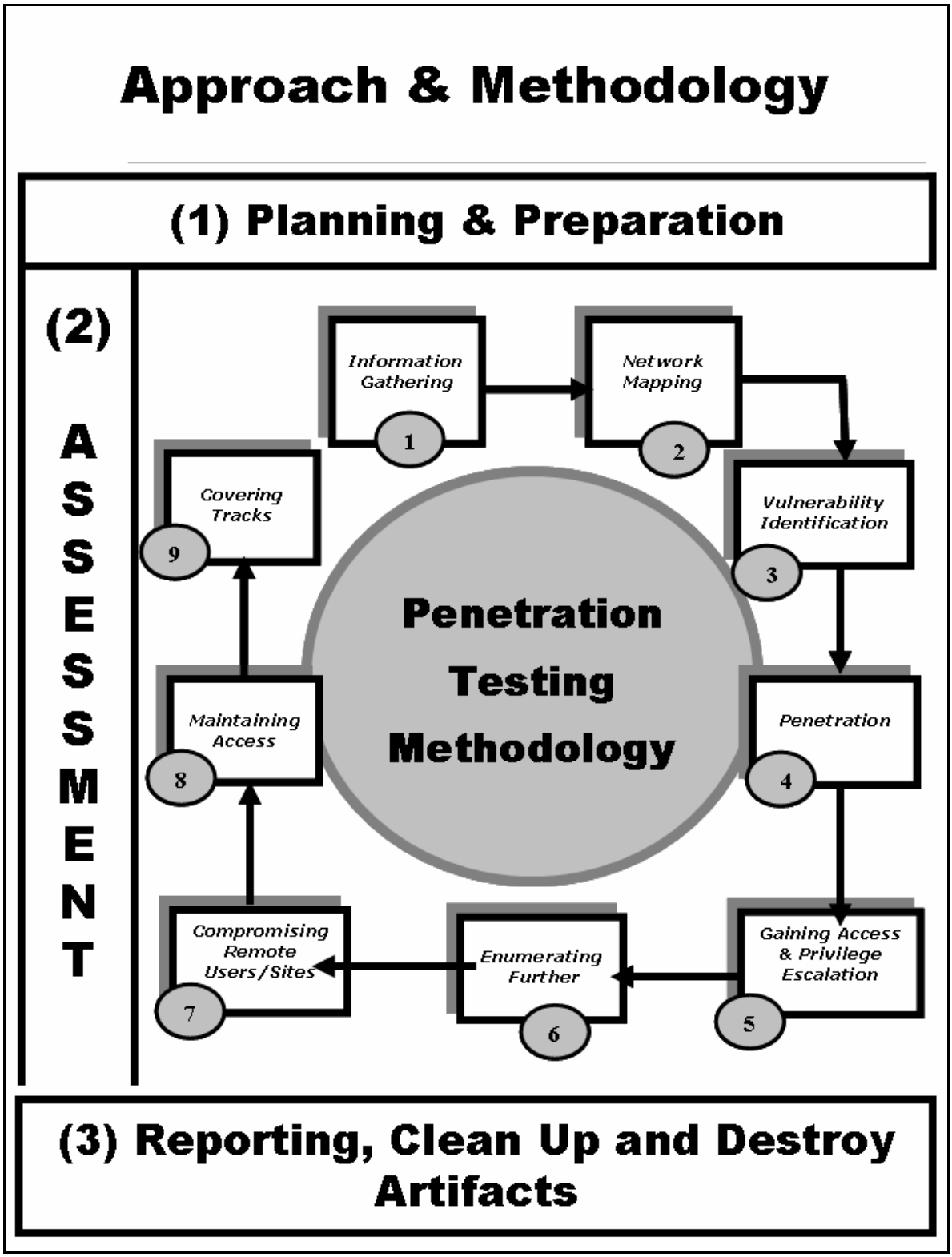
B.2 PHASE – II: ASSESSMENT

This is the phase where you actually carry out the Penetration test. In the assessment phase a layered approach shall be followed, as shown in figure below. Each peel represents a greater level of access to your information assets. The following layers are envisaged:

1. Information Gathering
2. Network Mapping
3. Vulnerability Identification
4. Penetration
5. Gaining Access & Privilege Escalation
6. Enumerating Further
7. Compromise Remote Users/Sites
8. Maintaining Access
9. Covering Tracks

   Audit (optional – not a requirement of ISSAF penetration testing methodology)

The execution steps are cyclical and iterative hence represented by the circular arrows in the assessment phase in the figure below:



B.2.1 Information Gathering

Information gathering is essentially using the Internet to find all the information you can about the target (company and/or person) using both technical (DNS/WHOIS) and non-technical (search engines, news groups, mailing lists etc) methods. This is the initial stage of any information security audit, which many people tend to overlook. When performing any kind of test on an information system, information gathering and data mining is essential and provides you with all possible information to continue with the test. Whilst conducting information gathering, it is important to be as imaginative as possible. Attempt to explore every possible avenue to gain more understanding of your target and its resources. Anything you can get hold of during this stage of testing is useful: company brochures, business cards, leaflets, newspaper adverts, internal paperwork, and so on.

Information gathering does not require that the assessor establishes contact with the target system. Information is collected (mainly) from public sources on the Internet and organizations that hold public information (e.g. tax agencies, libraries, etc.)

This section of the assessment is extremely important for the assessor. Assessments are generally limited in time and resources. Therefore, it is critical to identify points that will be most likely vulnerable, and to focus on them. Even the best tools are useless if not used appropriately and in the right place and time. That's why experienced assessors invest an important amount of time in information gathering.

B.2.2 Network Mapping

Following the first section, when all possible information about the target has been acquired, a more technical approach is taken to 'footprint' the network and resources in question. Network specific information from the previous section is taken and expanded upon to produce a probable network topology for the target. Many tools and applications can be used in this stage to aid the discovery of technical information about the hosts and networks involved in the test.

- Find live hosts
- Port and service scanning
- Perimeter network mapping (router, firewalls)
- Identifying critical services
- Operating System fingerprinting
- Identifying routes using Management Information Base (MIB)

- Service fingerprinting

To be effective, network mapping should be performed according to a plan. This plan will include probable weak points and/or points that are most important to the assessed organization, and will take into consideration all information obtained on the previous section.

Network mapping will help the assessor to fine tune the information previously acquired and to confirm or dismiss some hypotheses regarding target systems (e.g. purpose, software/hardware brands, configuration, architecture, relationship with other resources and relationship with business process).

B.2.3 VULNERABILITY IDENTIFICATION

Before starting this section, the assessor will have selected specific points to test and how to test them. During vulnerability identification, the assessor will perform several activities to detect exploitable weak points. These activities include:

- Identify vulnerable services using service banners
- Perform vulnerability scan to search for known vulnerabilities. Information regarding known vulnerabilities can be obtained from the vendors' security announcements, or from public databases such as SecurityFocus, CVE or CERT advisories.
- Perform false positive and false negative verification (e.g. by correlating vulnerabilities with each other and with previously acquired information)
- Enumerate discovered vulnerabilities
- Estimate probable impact (classify vulnerabilities found)
- Identify attack paths and scenarios for exploitation

B.2.4 PENETRATION

The assessor tries to gain unauthorized access by circumventing the security measures in place and tries to reach as wide a level of access as possible. This process can be divided in the following steps:

- Find proof of concept code/tool

Find proof of concept code available in your own repository or from publicly available sources to test for vulnerabilities. If the code is from your own trusted repository and thoroughly tested, you can use it, otherwise test it in an isolated environment.

- Develop tools/scripts

Under some circumstances it will be necessary (and cost effective) for assessors to create their own tools and scripts.

- Test proof of concept code/tool
    - Customize proof of concept code/tool
    - Test proof of concept code/tool in an isolated environment
- Use proof of concept code against target

The proof of concept code/tool is used against the target to gain as many points of unauthorized access as possible.

- Verify or disprove the existence of vulnerabilities

Only by testing vulnerabilities will the assessors be able to confirm or disprove vulnerabilities definitively.

- Document findings

This documentation will contain detail explanations of exploitation paths, assessed impact and proof of the existence of vulnerability.

B.2.5 Gaining Access and Privilege Escalation

In any given situation a system can be enumerated further. Activities in this section will allow the assessors to confirm and document probable intrusion and/or automated attacks propagation. This allows for a better impact assessment for the target organization as a whole.

B.2.5.1 Gaining Access

B.2.5.1.1 Gain Least Privilege

Gaining least privilege access is possible by obtaining access to unpriviledged accounts through several means, including:

- Discovery of username/password combinations (e.g. dictionary attacks, brute force attacks)
- Discovery of blank password or default passwords in system accounts
- Exploit vendor default settings (such as network configuration parameters, passwords and others)

- Discovery of public services that allow for certain operations within the system (e.g. writing/creating/reading files)

B.2.5.1.2 COMPROMISE

Reaching the target of the assessment (be it a specific system or a network) may require that intermediate systems are compromised as well, in order to bypass their security measures that may be potentially protecting access to the assessor's final target. These possible intermediate hops can be routers, firewalls, domain member servers or workstations, to name a few.

B.2.5.1.3 FINAL COMPROMISE ON TARGET

This step is the final compromise. The final target has been breached and is under complete control of the assessor. The final goal is to obtain administrative privileges over the system, in the form of administrative accounts such as Administrator, root, SYSTEM, etc.

B.2.5.2 Privilege Escalation

It is often the case that only low privileged access is obtained to a system. In that particular case the mapping of local vulnerabilities has to be performed (as opposed to network based vulnerabilities), proof of concept exploit obtained or developed, tested in an isolated environment, and applied on the compromised system.
At this stage the goal is again to obtain administrative privileges.
The main barriers to face are the level of patching and hardening of the system; and system integrity tools (including antivirus) that can detect and in some cases block the action of the proof of concept exploits required.

B.2.6 ENUMERATING FURTHER

- Obtain encrypted passwords for offline cracking (for example by dumping the SAM on Windows systems, or copying /etc/passwd and /etc/shadow from a Linux system)
- Obtain password (plaintext or encrypted) by using sniffing or other techniques
- Sniff traffic and analyze it
- Gather cookies and use them to exploit sessions and for password attacks
- E-mail address gathering

- Identifying routes and networks
- Mapping internal networks
- Perform steps 1 to 6 again with this system as starting point

B.2.7 COMPROMISE REMOTE USERS/SITES

A single hole is sufficient to expose an entire network, regardless of how secure the perimeter network may be. Any system is as strong (in this case, as secure) as the weakest of its parts.
Communications between remote users/sites and enterprise networks may be provided with authentication and encryption by using technologies such as VPN, to ensure that the data in transit over the network cannot be faked nor eavesdropped However, this does not guarantee that the communication endpoints haven't been compromised.

In such scenarios the assessor should try to compromise remote users, telecommuter and/or remote sites of an enterprise. Those can give privileged access to internal network.

If you are successful in gaining access into remote sites, follow steps 1.1 to 1.7, otherwise move to the next step.

B.2.8 MAINTAINING ACCESS

Note: the use of cover channels, back door installation and deployment of rootkits is often not performed as part of a penetration test, due to the risk involved if any of those remains open either during or after the testing, and are detected by an attacker.

B.2.8.1 Covert Channels

Covert channels can also be used to hide your presence on systems or on the network. Covert channels can be either protocol-tunnels (like icmp-tunnel, http-tunnel etc…) of can (ab)use VPN tunnels. Perform following steps to use covert channels:

- Identify Covert Channel Which Can Be Used
- Select the Best Available Tool for the Covert Channel
- Methodology - Setup the Covert Channel in the Target Network
- Test the Covertness of Channel Using Common Detection Technique

B.2.8.2 Backdoors

Backdoors are meant to be able to always get back to a certain system, even if the account you used to hack the system is no longer available (for example, it has been terminated). Backdoors can be created in several ways. Either by using root-kits (see further), by opening a listening port on the target system, by letting the target system connect to your server, by setting up a listener for a certain packet sequence which in turn will open up a port.

B.2.8.3 Root-kits

Root-kits will allow you to have even more power than the system administrator does of a system. You will be able to control the remote system completely.

Often rootkits also allow file, process and/or network socket concealment, while still allowing the individual in control of the rootkit to detect and use those resources.

B.2.9 COVER THE TRACKS

Note: it is normal practice during penetration tests to act as open as possible (except when requested by the customer) and to produce detailed information and logs of all activities, so the section below is mostly for reference purposes.

B.2.9.1 Hide Files

Hiding files is important if the security assessor needs to hide activities which have been done so far while and after compromising the system and to maintain back channel[s]. This is also important to hide tools so that these don't need to be uploaded to the target server each time.

B.2.9.2 Clear Logs

The importance of this stage is easily understood but usually understated. After an attacker has successfully compromised a system, he will like to keep it without alerting the administrator, for obvious reasons. The longer the attacker stays on a compromised system, the better the chances that he will be able to achieve his goals further in the network.

During the process of compromising the system, some suspicious and/or erroneous activities are logged. A skilled attacker knows that logs need to be doctored. He modifies them to cover his tracks and delude his presence.

Note: This is only effective if no remote Syslog servers are in use. If these are, these remote Syslog servers will have to get hacked & cleared as well.

Methodology

- Check History
- Edit Log files

B.2.9.3 Defeat integrity checking

In cases where static integrity checking by systems such as Tripwire has been implemented, it is very difficult to make any changes to the system without those being detected and reported.
However, if the deployment of the system integrity tool was incorrectly done, for example by leaving the file with the signatures of valid files and programs in the same server, it will be possible to modify the system and regenerate the signatures.

B.2.9.4 Defeat Anti-virus

Nowadays, on most workstations and servers, there is Anti-Virus software protecting the system against well known malicious software (like exploits, viri, worms, etc); the focus of this step in penetration testing is to be able to disable or defeat AV software so that the assessor is able to perform activities unhindered, and the possibility to reactivate the AV later.

In most centrally managed AV solutions, the AV software is restarted after a certain amount of time when it is stopped by an assessor. The “grace period” allows the assessor to perform several tasks in order that the AV software remains disabled for longer periods of time.
Possible things that assessors can do (most of these require Administrator level access):

- Create a batch file so that the AV services are stopped every 30 sec
- Disable the AV services
- Block the central management port

B.2.9.5 Implement Root-kits

Root-kits, like POC exploits, should be customized to be able to completely cover the assessor’s activities. In most cases if there is an AV patrolling, root-kits (usually on

win32) will be detected before installation. So, modifying the root-kits is required in most situations. It's also important to notice that some root-kits won't work on different system setups. For example your root-kit may work on win2k-SP3 but it can't cover anything on SP4.

AUDIT (OPTIONAL)

System audits can tell even more about potential security vulnerabilities than a single penetration test. Therefore, system audits should be performed after completing a penetration test. The system audits should check for running services, open ports, established connections, file system permissions, logging and/or remote logging, auditing as per the detailed check list for a particular system.

B.3 PHASE – III: REPORTING, CLEAN UP & DESTROY ARTIFACTS

B.3.1 REPORTING

Minimal reporting should consists of followings:

B.3.1.1 VERBAL REPORTING

In the course of penetration testing if a critical issue is identified, it should be reported immediately to ensure that organization is aware of it. At this point criticality of issue should be discussed and countermeasure to safeguard against this issue should be provided.

B.3.1.2 FINAL REPORTING

After the completion of all test cases defined in scope of work, a written report describing the detailed results of the tests and reviews should be prepare with recommendations for improvement. The report should follow a well documented structure. Things that should be definitely in the report are the following sections:

- Management Summary
- Scope of the project (and Out of Scope parts)
- Tools that have been used (including exploits)
- Dates & times of the actual tests on the systems
- Every single output of tests performed (excluding vulnerability scan reports which can be included as attachments)
- A list of all identified vulnerabilities with included recommendations on how to solve the issues found.

- A list of Action points (what recommendation to perform first, what is the recommended solution)

For more detail refer to the vulnerabilities section

B.3.2 Clean Up and Destroy Artifacts

All information that is created and/or stored on the tested systems should be removed from these systems. If this is for some reason not possible from a remote system, all these files (with their location) should be mentioned in the technical report so that the client technical staff will be able to remove these after the report has been received.

10 PHYSICAL SECURITY ASSESSMENT

Description

Proper Physical & Environmental Security ensures that access to systems hardware & other elements vital for systems functioning like the electric power service, the air conditioning and heating plant, telephone and data lines, backup media and source documents is controlled. This also ensures maintaining the proper environment for optimal systems performance through cooling & humidification.

Objective

[Text]

Requirement

[Text]

- Understand Organization's environment
- Technical Requirements

Expected Result

10.1 METHODOLOGY

- Review of Access Control System
- Fire Protection
- Environmental Control
- Interception of Data

10.2 REVIEW OF ACCESS CONTROL SYSTEM

Description

Objective

Expected Results

Pre-requisites

Process

- Barriers
- Guards
- PACS
- CCTV Monitoring
- Employee Training

10.2.1 Barriers

Review if there are adequate barriers in and around the facility to restrict the uncontrolled movement of personnel & data. Barriers could be in the form of walls, partitions, perimeter fences etc.

10.2.2 Guards

Review if the security guards challenge the entry of personnel to sensitized areas.

10.2.3 PACS

Is there a Physical Access Control System deployed which can control the access of personnel to sensitized areas. The PACS can be proximity card/magnetic card based or even based on biometrics (fingerprint identification). The PACS system should ideally be centralized & personnel should be granted access to the areas they require only on adequate approvals from their managers. The logs of all PACS should be monitored for violations. Anomalous activities should be recorded, investigated & if necessary be escalated to the concerned authority

10.2.4 CCTV Monitoring

CCTV (Closed Circuit Television Monitoring) can be used to monitor all entries & exits of sensitized areas from a single location. All entries/exits should preferably include even emergency exits that can be source for unauthorized entries. There could be dedicated personnel monitoring the CCTV system who can raise an alert on suspicious activities. There are cameras, which work on motion sensors that track movement in its coverage area. When there is movement the screen at the monitoring end is updated. The tapes or video must be preserved for long durations to track historical events.

10.2.5 Employee Training

All employees must be trained on the physical security aspects & they should challenge visitors accessing sensitized areas without proper authorization & escort.

10.3 FIRE PROTECTION

Fire detection equipment is required for quickly detecting a fire & extinguishing it. It is also important to accurately pinpoint the location of the fire.

Process

- Fire Detection Systems
- Fire Suppression Equipment
- Fire Extinguishers

10.3.1 Fire Detection Systems

Smoke Detector & Heat sensors should be used for detecting the presence of a fire & these in turn should be connected to a centralized alarm system. Smoke detectors & Heat sensors detect the fire at a nascent stage which is very helpful in suppressing the fire. The alarm system would help pinpoint the area of the fire so that adequate action can be taken to suppress the fire. The fire alarms should be located at a place that is attended by personnel round the clock. Employees must also be trained to respond to the fire alarms & evacuate when necessary.

10.3.2 Fire Suppression Equipment

Various type of fire suppression equipment like GAS/ Water Based systems are available which should be deployed. Among the GAS based suppression systems we have the FM-200 (HFC-227ea)_ CEA-410 or CEA 308_ NAF-S-III (HCFC Blend A)_ FE-13 (HCFC-23)_ Aragon (IG55) or Argonite (IG01)_ Inergen (IG541) as replacements for Halon based suppression systems. The Water based suppression systems could be a ‘dry pipe’ or ‘closed head system’ which use water sprinklers to suppress fires. The water-based systems are generally not very suitable where there is a presence of expensive electronics computer equipment like server rooms. The suppression systems could be directly integrated with the alarm systems so that they are energized the moment a fire is detected.

10.3.3 Fire Extinguishers

Portable extinguishers (Powder based/ CO2 based) must be placed at easily accessible points which can be used in cases of fire emergencies. These extinguishers must be regularly serviced & the pressure levels of the extinguishing medium must be checked. Employees must also be trained for the use of fire extinguishers.

10.4 Environmental Control

HVAC: Heating Ventilation & Air Conditioning or in short maintaining the environment is very important from a systems availability perspective.

Process (Steps to complete this Process/Task/Test Case)

- Air Conditioning & Humidity Control
- Water Detection
- Ups & Power Conditioning
- Interference

10.4.1 Air Conditioning & Humidity Control

There must be a centralized system which controls the air temperature through the use of thermostats. Air temperature can be maintained between 22-24 Degrees Celsius in normal working areas & 15-23 Degrees Celsius in Computer/Server rooms. Humidity should be maintained at 40 -60%. This is important for optimal functioning of the equipment as higher or lower temperatures may damage the electronic circuits. Similarly if the humidity level drops the dryness in the atmosphere may generate static charges that could permanently damage electronic circuits. The Temperature & Humidity should be controlled by an integrated alarm system that is continuously monitored.

10.4.2 Water Detection

Plumbing leaks can cause flooding of equipment rooms. Utmost care must be taken to isolate the plumbing system from the areas where the data centers are present. Optionally a water detection system may be installed under the false flooring of a data center that would enable detection of water before it encroaches the floor of the data center & adequate action can be taken to stop the water flow.

10.4.3 Ups & Power Conditioning

UPS & Power conditioning: Electrical surges, spikes are among the most frequent reasons for critical equipment failure. Surge suppression equipments must be deployed which can effectively condition the power to the required levels & frequencies. UPS or Uninterruptible power supplies must be used to ensure continuous supply of power to critical equipment. Electric power from multiple service providers may be used so that there is no dependency on a single provider. If there are prolonged power cuts, backup generator sets should be used to supply continuous power to the systems.

10.4.4 Interference

Interference: EMI (electro-magnetic interference) can severely hamper the communications. If high voltage power cable are running very close to the network communication cable the interference generated from the power cable can cause errors in the data communication resulting in degraded performance.

COUNTERMEASURES

Contributors

Links

10.5 INTERCEPTION OF DATA

Depending on the type of data a system processes, there may be a significant risk if the data is intercepted. There are three routes of data interception: direct observation, interception of data transmission, and electromagnetic interception.

Objective

Expected Results

Pre-requisites

Process

- Data Observation
- Interception of Data
- Electromagnetic Interception

10.5.1 Data Observation

Critical computer systems that display sensitive information on the screens must be kept in sensitized areas. Their displays must not be visible to attackers outside the sensitized area .e.g if a computer system on which significant merger related information is being processed is located near the window; then this data may be available to spies just across the street that can look at the screen.

10.5.2 Interception of Data

Interception of Data: Data passing through communication networks may be tapped. If there are common ducts used by various organizations in a single building which unsecured, attackers are pretending to be tenants who are using the same duct could tap into the cables & be able to access vital information passing in & out of the organization. Therefore cables require to be properly secured while passing through common ducts.

10.5.3 Electromagnetic Interception

Electromagnetic Interception: Computers while processing information emanate electromagnetic radiation. An attacker using an antenna & a receiver can monitor

and retrieve classified or sensitive information as it is being processed without the user being aware that a loss is occurring. These sorts of data interception methods are also know as TEMPEST. These attack methods are very complex & the organization should consider the financial implications before implementing TEMPEST shielding mechanisms which block electromagnetic radiation.

10.6 GLOBAL COUNTERMEASURES

10.7 FURTHER READINGS

11 ENTERPRISE SECURITY OPERATIONS MANAGEMENT

Introduction

The implementation of a comprehensive Information Security management framework includes both technical and manual security processes that need to be synchronous to each other to ensure completeness of the management of security. Operations Management includes the management of the IT administration and service delivery processes of the enterprise. A review of the IT operations in any security framework assessment is essential to ensure that security operational processes that support the information security management of the enterprise are appropriately implemented and adhered to in order to ensure that such controls and security measure are effectively meeting the enterprise's information risk management objectives.

11.1 CAPACITY MANAGEMENT

Capacity Management relates to the process of management of the IT infrastructure capacity to ensure continuous availability of the technology infrastructure of the enterprise. This would typically involve the management of the capacity of hardware and software components to ensure that there is no disruption to the activities of the business caused by any technological capacity restrictions. Such activities would include:

- Review and ensure that appropriate processes exist for planning and acquiring new systems, systems upgrades or new versions of systems considering the capacity requirements of the enterprise
- Assess whether capacity usage is constantly monitored in order to ensure availability of IT services and to detect any unauthorized activities in the IT environment. This is particularly important considering the risks of DoS attacks or similar other attacks being executed against the enterprises infrastructure.
- Ensure that capacity monitoring and planning considers all the components of the technology infrastructure of the enterprise such as hardware, software and networking.

Domain	Capacity Management

Introduction	Capacity management ensures that IT resources are used in an efficient manner with regard to availability. It ensures appropriate disk quota, response times, processing and network and system capacity.
Pre-requisite	Statistical reports from capacity utilisation trend monitoring processes Stress testing report on systems, applications and on network components Volume capacity document Tools for stress, volume and capacity testing
Objective	To identify gaps in minimum baseline standard To assess capacity of systems, applications and network components

	Evaluation Check	Yes	No	N/A	Evaluation Performed and Results
1	Is there any policy and processes for capacity management? If so is that available for review?				
2	Is the policy and processes for capacity management ensures that the minimal standards stated in the service level agreements are fulfilled?				
3	Is the capacity management process covers all critical components?				
4	Is the organization predicted resource bottlenecks related to business needs?				
5	Is the capacity and availability plans established based on service level agreements?				
6	Is there any process to test new software on performance and capacity before implementing them?				

11.2 VULNERABILITY MANAGEMENT

Networks connected to the Internet are probed and scanned for vulnerabilities every minute. These could be deliberate attacks, as in the case of automated scanners or crackers running scans, or a consequence of infected systems propagating worms onto the enterprise network. Worms are the single most dominant threat on the Internet today—and their sophistication levels are increasing rapidly. Nimda and Code Red were worms that exploited multiple vulnerabilities in systems to gain entry into and cripple large networks and parts of the Internet. These worms scan flaws in web servers and open shared networks to proliferate. Correspondingly, crackers use known vulnerabilities in networks to break into them. Today, with improved scanning algorithms, it is possible for worms on the Internet to reach saturation levels in shorter periods than before. Known vulnerabilities are typically those published by software vendors. In most cases, patches for these worms are available. The timely installation of such patches and the reconfiguration of perimeter systems and other

layered defenses can help an organization combat this menace. An effective organization wide vulnerability management strategy treated as one of the most vital components of any enterprise information security program is essential. This sections emphasizes a few steps that organizations must take toward building an enterprise wide vulnerability management strategy. Some of these steps may overlap with other organizational processes, such as asset identification, patch management, configuration management and release management.

ISSAF recommends a 4 step methodology that enables the organization to effectively manage vulnerabilities affecting its IT environment.

Phase 1- Identification of Asset, Technology, Assessment Tools & Frequency

The IT assets need protection from vulnerabilities need to be identified. The Risk Assessment of the assets dicussed in other sections of ISSAF can highlight the criticality of these assets and which assets need maximum protection from vulnerabilities. The threats also play an important part in this e.g Internet Based Banking application vulnerabilities could be more easily exploited as compared to an application on the intranet because of direct HTTP access to the web servers. The Technologies that they are using also need to be identified. This in turn helps one identify the appropriate vulnerability assessment tools. The enterprise management strategy will also be the important factor that would help the organization choose a tool. The frequency of assessments also needs to be identified. Internet applications could be assessed more frequently than other intranet applications.

Phase 2- Assessment – Scanning, Penetration Test , Results Analysis

After identifying the systems once could assess the environment by conducting first an Filtered scan (Normal operating state where firewall is enabled) & then conducting a unfiltered scan (All ports in the firewall are opened). This would measure the ability of the firewall in blocking out some attacks. A penetration test could also be conducted before collating all these results into a detailed vulnerability assessment report.

Phase 3 – Remediate – Patch Management, Define/Improve Baselines & Comply with Baselines

The previous phase identifies the IT vulnerabilities. The vulnerabilities generally stem from unapplied patches or from improper configurations. The organization needs to

define a patch management strategy to roll out essential patches. The other improvements that may be required a re redefinition of the configuration baselines and its effective implementation that should be managed through the change & release management processes.

Phase 4 – Monitor

Once the vulnerabilities are fixed the environment needs to be continuously monitored for changes to the IT environment (assets, technologies) and new vulnerabilities that are discovered & released by software/hardware vendors.

11.2.1 Patch Management

Domain	Patch Management
Introduction	Patch management covers the tools/utilities, policies and processes for keeping systems latest with new software updates which are released after software is developed. Pro-active security patch management is essential to keep enterprise environment secure and reliable. A patch management process covers configuration changes, applying software updates and provides recommendations to safeguard.
Pre-requisite	Documents related to identifying new patches, vulnerabilities, patch testing and patch implementation.
Objective	To evaluate patch management process for an enterprise.

	Evaluation Check	Yes	No	N/A	Evaluation Performed and Results
1	Does the organization have explicit and documented policy and processes for handling patches?				
2	Is the patching policy and process specifies what techniques an organization will use to monitor for new patches and vulnerabilities and who will be responsible for monitoring them?				
3	Is the organization has a methodology for testing and secure implementation of patches?				
4	Does the patch management process define what patches will be implemented first and on which all systems?				
5	Is the methodology for handling patches includes? All necessary Inventories in the organization Vulnerability and patch monitoring? Patch prioritization techniques Patch testing Patch management training Automatic patch implementation				

11.2.2 Configuration Management

Domain	Applications Security
Introduction	Applications security ensures that operational applications supporting a business process are purchsed, developed, deployed and maintained in a secure manner
Pre-requisite	Minimum baseline standard established for each component Current configuration items from each component
Objective	To identify gaps in minimum baseline standard for each component To identify gaps in current confirmation items

	Evaluation Check	Yes	No	N/A	Evaluation Performed and Results
1	Have the following been considered during application design				
1.1	Structure design methodoloty used				
1.2	Processing requirements of application				
1.3	Performance requirements				
1.4	cosiderations for operational configuration and transaction processing requirements				
1.5	consideration for use of code in other applications				
1.6	ease of installation				
1.7	Operational requirements				
1.8	Consideration relating to application processing at multiple locations				
1.9	Future change requirements				
1.10	Security requirements				
1.11	Auditabililty considerations				
1.12	Help text and training manuals				
1.13	external third party requirements				
1.14	System Desing Documentation				
1.15	Independent examination for security requirements				
1.16	Data communications requirements				
1.17	System requirements specification document				
1.18	Secuirty requirements specification document				
2	Checks for incomplete, incorrect or inconsistent data processing with in application, and between other applications/systems				
2.1	Is the application developed in house				
2.2	Is the application purchsed from a vendor				
2.3	Is there available a complete security requirements specification document.				

2.4	Is there an internal development, maintenance, testing and user support team				
2.5	Was the experience of personnel that developed the application evaluated				
2.6	Is there appropriate segregation of responsibilities between developers inclusing the testing team				
2.7	Is the source code strictly controlled				
2.8	Is there appropriate segregation of testing, development and production facilities				
2.9	Is there sufficient staff to support the application database and the underlying operating systems				
3	Is application development outsourced?				
4	Do external contract staff for development sign confidentiality agreements and NDA's?				
5	Are there sufficient escrow agreements undertaken with the application vendor?				
6	Are audit trails and logging performed on development, source code library and operational systems				
7	Each line of code has been reviewed or a walkthrough performed				
8	Are application program staff aware of security requirements for the application				
9	Comprehensive testing is performed before the application is deployed for production				
10	Does testing include to verify that access control, audit and validation mechanisms function correctly				
11	Does testing include reaction to error conditions and out of sequence records?				
12	Is access to development source programs restricted to programmers that are developing the software				
13	Are program libraries regularly backed up?				
14	Are all program changes authorised by appropriate management?				
15	Is there a design for choosing passwords during development?				
16	Are devlopment user-ids shared?				
17	Is there automatic terminal time out facility available?				
18	Are there sufficient procedural controls?				
19	Is data input into application subject to appropriate validation controls? Are the following validation checks considered:				
20	out of range checks				
21	invalid characters in fields				

22	missing or incomplete data				
23	exceeding data volume limits				
24	unauthorised control data				
25	session or batch controls				
26	balancing controls				
27	validate system generated data				
28	check transfers between computers				
29	hash totals of files				
30	programs run at correct time				
31	programs run in correct order				
32	Is there message authentication performed?				
33	Does implementation of a new system or upgrade to an existing system is performed with appropriate change menagement? Are the following considered:				
34	S/w update by program librarian				
35	Executable code only				
36	Evidenced acceptance & testing				
37	Audit log of library updates				
38	Previous s/w revisions maintained				
39	Is system test data appropriately controlled and protected?				
40	Is test data subject to same controls as live data?				
41	Is a change control procedure is place?				
42	Is the security change of operating systems reviewed for impacted on the application systems?				
43	Are vendor supplied packages modified?				
44	Does acces to program source libraries restricted to program librarian?				
45	Is a formal risk analysis performed before performing the modifications?				
46	are programs identified for trojan code and covert channels				
47	is output data from programs validated?				
48	Is cryptography considered for applications?				

11.2.3 Change Management

Domain	Change Management
Introduction	Change management process ensures that the integrity of data, application programs and system security settings are maintained as per the required standards and meet accepted levels.
Pre-requisite	
Objective	To ensure that there are no unauthorized changes to programs, data and security settings.

	Evaluation Check		Yes	No	N/A	Evaluation Performed and Results
1	Is there a formal technical change management procedure in place? And if so is that available for review?					
2		Where the change management process undergoes a change, does it get discussed and approved at the highest level in IT management and user management?				
3		what is the role of executive management in monitoring the adherence to change management and have there been cases where executive management has demonstrated its commitment to implementing change management in its entireity?				
4	Is all the changes aligned with company's standard configuration management procedure?					
5	Are emergency changes permitted without adherence to the formal change management process being adhered to in its entireity?					
6	I	If emergency changes are permitted, who has the authority to declare something as an emergency change and in effect therefore circumvent going through the formal change management cycle?				

7		If any person is permitted to declare the need for emergency changes to be carried out without going through change management cycle, does that person have a clear mandate as to what are the circumstances where such emergency changes are permitted?				
		Where emergency changes have been permitted, is there a process of time-bound validation of those emergency changes and who are authorized to validate them?				
8		Where emergency changes have been permitted, is there a process of post facto business justification process? Does a reward punishment system exist to deal with those making decisions in favor of emergency changes that does not go throuhg the entire change management cycle?				
9	Is the production environment separate from development and staging environment?					
10	Is personal formally submitting and implementing changes?					
11	Is segregation of duties been followed by users and also by staff responsible for making changes into production environment?					s

11.3 ENTERPRISE INCIDENT MANAGEMENT

Enterprise Incident Management relates to the identification, investigation and resolution of security incidents related to the Information Systems Infrastructure of an enterprise. The philosophy of incident management requires that all incidents irrespective of their criticality are logged and investigated to ensure that they do not pose a security concern/risk to the enterprise. A review of the Enterprise Incident Management Processes includes:

- Ensure that the enterprise has adequate infrastructure and processes to identify and record all systems events
- Ensure events are logged, investigated, escalated and resolved in accordance with the Information Security Policies of the enterprise
- Event Logs include the following at a minimum:
  - Security Device Logs (Firewall, IDS, IPS etc)
  - Network Device Logs
  - Server Logs (Applications, Databases, OS, Email, Web server, Proxy Server, SMTP Servers)
  - Secure Transmission and Storage of Event Logs
- Ensure that monitoring procedures provide for appropriate escalation procedures
- Ensure monitoring of logs on daily, weekly or monthly basis as is applicable.
- Ensure events are appropriately classified as Security Incidents (Un-authorised access attempts at server and client levels, IDS event logs of attempted connections) or Operational Events (Abnormal Information Systems Events such as abnormal termination, errors, failures, connectivity issues, etc.…)
- Ensure the process provides for taking necessary actions to prevent recurrence of security incidents through appropriate measures
- Security Incidents are routed to Security Incident Management Process in 6.5.4.3
- Operational Events are routed to Operations Events Management Process in 6.5.4.4

11.3.1.1 LOGGING

Logging is one of the most important activities related to the process of monitoring Information Systems Security within an enterprise. This would involve logging of all the occurrence of events (whether authorized or unauthorized, normal or abnormal) within the Information Systems of an enterprise. These event logs would then form

the basis for review and assessment for identification of events that result in a security implication to the enterprise. The review of a logging must ensure that the following activities are conducted at a minimum:

- Review the incident management procedures of the enterprise and ensure that all technology events are appropriately recorded in a central database either using automated solutions such as Enterprise Management Systems or through a helpdesk function.
- Ensure that the incident management procedures require the central events database to be reviewed to distinguish normal operational events or potential security events. Such reviews should ensure normal operational events are routed to the IT operations staff for resolution, whilst potential security events are routed to the Chief Information Security Officer and his team for investigation and resolution.
- Assess whether the process for incident reporting ensures that all system faults or suspected system faults must be reported and logged.
- Ensure Helpdesk logs are periodically reviewed to ensure that all faults reported have been satisfactorily resolved and the Helpdesk call closed.
- Ensure fault resolutions are reviewed to ensure that Information Security and Controls have not been compromised in the process of implementing such resolutions.
- Review the audit logs have been activated on critical technology components such as servers, applications, databases and network. Ensure that these logs produce meaningful information that can be used in investigating security events.

11.3.1.2 MONITORING

Monitoring is the process of continuous review of the event logs of various technology components of the enterprise. This would involve a review of the audit trails, event logs, incident logs, helpdesk logs amongst other logs as application to the enterprise. Depending on the implementation of the logging process (i.e. centralized or decentralized) this activity can be performed either by one or many individuals across the enterprise. The most significant component of the process of monitoring is the responsibility of performance of this activity. The process would necessarily require the involvement of the Information Security Officer and the Compliance Manager to ensure that security incidents are identified and appropriate action is initiated to resolve them.

11.3.1.3 SECURITY INCIDENT MANAGEMENT

The Security Incident Management process would stem from the logging and monitoring processes mentioned above to ensure that identified security incidents are managed in accordance with the risks that such incidents pose to the enterprise. The process of Security Incident Management must be performed by the Information Security Officer (ISO) and should at a minimum involve the following:

- Definition of Security events / incidents, this would involve the formalization of a definitions document that identifies all events / incident types that have a security implication and considered as critical to the enterprise
- Allocation of responsibilities for logging of events or incidents reported. This could be a part of the helpdesk functionality or in larger enterprises, through a security helpdesk function that is specifically constituted for handling security events or incidents
- Constitution of a security response team, this comprises of a team of security personnel who would respond to the a report of a security event or incident
- Classification of Security events or incidents, this involves the classification of security events in order of their impact on the organization
- Risk Assessment and Incident Response - This is a process of security incident management wherein the security response team assesses the risks associated with an identified security incident to the Information Security of the enterprise. Depending on the criticality of the risk identified, the security and controls to be implemented are determined. In the event the incident requires further investigation, processes such as Computer Forensics and Investigations are applied.

11.3.1.4 OPERATIONS EVENT MANAGEMENT

Operations Event Management relates to the process of responding to events that are operational in nature. Such events stem from the IT infrastructure and technology being used in the enterprise and may comprise of routine IT operations events such as abnormal performance, terminations, poor response amongst many others.

However, it is extremely important that the operations events are also assessed for security implications so as to ensure that any operations events that may arise from security violations are identified and remedied in accordance with a response relative to a security incident. Furthermore, operational event remediation may also at times introduce security flaws and vulnerabilities which need to be prevented at the time of

remediation itself so as to reduce the probability of such vulnerabilities being exploited against the security interests of the enterprise.

For evaluation of security implications if any for an operational event, the process of operations event management must be routed to the Risk Assessment in Security Incident Management (refer 11.3.1.3 Security Incident Management)

11.4 User Access Management

User Access Management relates to the process of managing user access to the Information Systems of the enterprise. This would include the management of user access of the following:

- New User Creation
- Existing User Access Modifications
- User Access Profiles creation and modifications
- User Access Termination

A review of the user access management process would essentially comprise of the following:

- Review of User Access Policies
- Review of User Access Management roles and responsibilities
- Review of User Access creation, modification and termination for the following:
  - Business Applications such as ERP
  - Enterprise Applications such as Email
  - Access to Local Area Network
- Review of the process for periodic reviews of user access to ensure that transitional processes of the organization that impact job responsibilities do not result in the users having unauthorized access
- Review the process and results of User Access Logs monitoring processes to ensure that unauthorized activities have been appropriately detected and remedied

11.5 Audit & Review

Information Systems Security is a rapidly transforming environment wherein new vulnerabilities and risks are introduced each day resulting in the pressing need for constant monitoring and assessments to ensure that security management infrastructure of the enterprise is awake to this challenge and can respond in a manner that appropriately addresses the technology risks that impact the enterprise.

Given the rapid advancements in technology, enterprises find it difficult to maintain adequate technological skills or to sustain continuous education to develop the expertise internally. As a result to maintain its information security capabilities the enterprise often relies on external parties or dedicated internal groups for the periodic assessment of its Information Systems Security. Such reviews would typically involve the following:

- Internal IT Audit Review, comprising of reviews of specific areas of IT security performed by internal resources
- Internal Security Assessment, comprising of technology specific reviews performed by specialist IT security personnel
- Third party Information Security Assurance Reviews, comprising of security assessments performed by third party contractors in areas that require advanced technology and security specializations

Accreditation involves the process of benchmarking and reviewing the IT security implementation within an enterprise against the ISSAF.

11.6 Review of Logging / Monitoring & Auditing Processes

11.7 Logging

11.7.1 Importance of logging & audit events

11.7.1.1 What are Logs?

Logs are simply data that is recorded during the operation of a program. Logs can contain usage data, performance data, errors, warnings, and operational information. Logs can be written to files or databases, either in an easily readable format or in a proprietary format that must be read using a certain program and can be stored into the internal machine or a separate machine.

Most server software today includes some logging mechanisms. In Unix Systems you can enable the syslog.

11.7.1.2 Why Logs Are Important?

Logs are often the only way to tell what is happening and happened on in a system. It is important to identify all programs on all the computers that a business or company

depends on and then gather the available log files for analysis, as deemed necessary and when required.

Log files are the only way to store the history of what happened within a system. Log files are often the only way to detect and trace an intrusion by a hacker or someone, so that we can trace the reason behind a server failure, gather data for capacity planning for increasing hard drives, or determine which Web pages were visited by the users.

Without logs, it is very difficult (if not impossible) to know what is going on in a system.

Logs can be captured in the same machine and kept or can be stored in a separate logging machine. Many Workstations, Servers can be allowed to capture in a centralized (separate) machine.

This can be done either by manually copying the log files to a central machine(s) or by automating the copying process. From this central machine(s), the log data will be maintained. If a company wants to log its necessary to do the following:

Working with logs requires you to:

Decide which logs to capture.

Choose an analysis/viewing tool.

Determine log capture frequency.

Where the logs will be stored (local or remote workstation)

Who will monitor the log and what action will be taken

11.7.1.3 How to Approach Log Capture and Analysis

Logs can contain huge amounts of data. Logging and analyzing everything can result in information overload or sometimes slowing down, where either the system or the people involved cannot handle the amount of data.

As a result, it is important for the System Administrators to decide exactly what information is required so that only the required data can be logged, captured, and

analyzed. To ensure that needed data is captured in an organized and timely fashion, it is important to know which logs contain what data, and where these logs are located.

Accuracy is also an important factor. Some systems create a separate, new file containing the log entries every day; others delete older log entries when the log file reaches its maximum size or wraparound. Understanding the logging policy of each system ensures a consistent and accurate capturing methodology. There should be a logging policy for every important servers and workstations in a Company.

In many real-world computing scenarios and applications, sensitive information must be kept in log files on a separate machine so that even someone tampers the local machine the log data is lost and if its stored in a separate machine they will gain little or no information from the log files and to limit his ability to corrupt the log files.

We describe a computationally cheap method for making all log entries generated prior to the logging machine's compromise impossible for the attacker to read, and also impossible to undetectably modify or destroy.

If you want to log everything everyone does it would impact the performance of your system so its not necessary to log everything .But you can log like

1. Who has logged into the system (Via ftp, telnet, rsh or rlogin in a linux or unix system etc.,)
2. What access he has done in the system
3. What files are uploaded and downloaded in the system. (using scp, ftp rcopy, ssh etc)

I do not think you will find any built in method of seeing everything anyone has done.

11.7.2 Examples of audit events

For example in a Microsoft Windows Server every event generated by auditing will appear in the Event Viewer. Administrators should decide how the event logs generated will be stored. Each of the settings can be directly defined in the Event Viewer or in Group Policy.

11.7.3 Events to Audit

Microsoft Windows 2000 provides several ways of auditing for securing the events. When designing the audit process you will need to decide whether to include the following categories of Security Audit Events.

a. Logon events
b. Account logon events
c. Object Access Events
d. Directory Service Events
e. Privilege Use Events
f. Process tracking Events
g. System Events
h. Policy Changes Events

For Example if you enable the logon events it includes both the computer and user logon events. You will have separate security event log entry for computer account and the user account if a network connection is attempted from a Windows based NT and similar Systems. Windows 9x based computers do not have computer accounts in the directory and they do not generate the logon event entries for their network logon attempts.

Some examples of logon events that appear in the Security Event log is below (For Windows 2000 Serve):

Event ID	Description
528	A user successfully logged on to a computer
529	The logon attempt was made with an unknown user name or a user name with bad password
530	An attempt was made to log on with the user account outside the allowed time
538	A user logged off
536	The Net logon service is not active
537	The logon attempt failed for other reasons.

Similarly for Linux and other OS the administrators have to see the respective manuals and provisions for setting up the logs for protecting Information.

11.7.4 How logs should be protected from tampering.

To ensure that the event log entries are maintained for future reference and without tampering, Administrators should take a number of steps to protect the security of the event logs. These should include:

1. Define a policy for the storage (location), how logs are overwritten and maintenance of all event logs. The policy should define all required event log settings and be enforced by Group Policy. This varies from OS to OS. So appropriate mechanism should be used.

2. Ensure that the policy includes how to deal with full event logs, especially the security log. It is recommended that a full security log require the shutdown of the server. This may not be practical for some environments, but you should certainly consider it for perusal.

3. Ensure that your security plan includes physical security of all servers to prevent an attacker from gaining physical access to the computer where auditing is performed. An attacker can remove audit entries by modifying or deleting the physical *.evt files on the local disk subsystem or he may try to remove the /var/log entries in the unix system.

4. Implement a method to remove or store the event logs in a location separate from the physical server. These can include using cron or batch files to copy the event logs to CD-R or write once, read many media at regular predetermined intervals, or to other network locations separate from the server.

If the backups are copied to external media such as backup tapes, or CD-R media, the media should be removed from the premises in the event of fire or other natural disasters.

5. Prevent guest users /access to the event logs by enabling the security policy settings to prevent local guests from accessing the system, application, and security logs. Only the Administrator or root user should have access to the log files. For all other users the permission needs to be disabled.

6. Ensure that the system events are audited for both success and failure to determine whether any attempts are made to erase the contents of the security log. Use History command in Linux to see what happened after the user uses the ‘su’ or root equivalent command.

7. Enforce use of complex passwords and extra methods such as smart card logon by all security principals that have the ability to view or modify audit settings to prevent attacks against these accounts to gain access to audit information.

8. Use Log rotate for rotating the logs. Use tar command to compress the logs and save so that you can have less space consumed for logging.

11.7.5 Log retention periods as per regulations & policies

Usually the logs are maintained as per the requirement and policy of the company. Tools like logrotate in linux can help you to rotate the logs at predetermined time.

In the linux environment you can logrotate (compress) at weekly,daily etc.,)

11.8 IMPORTANCE OF MONITORING OPERATIONS WITH EMPHASIS ON SEGREGATION OF DUTIES

11.8.1 How exclusive rights to system admin could be misused

If a Administrator enables the root or equivalent access to other users by knowing or unknowingly they can delete the logfiles or some files.So its very essential to give access permissions to anybody only after considering the realtime requirments and with proper approval.

11.8.2 Talk briefly about granting only the access controls required for the job role.

A guest user is not required to access the log files. Similarly a backup operator need not be required to see the log files. Only the system Administrator with root permission needs to be seeing the log files. So in general the log files access to others should be kept minimum unless necessary.

11.8.3 Why id & passwords should not be shared (due to accountability of individuals actions)

There are potential chances that somebody can misuse the login by having the passwords. So it's advisable not to share the ids and passwords.

AS part of the security awareness programs, the users should be allowed to realise that any login attempts and similar access by their user id's and password they will be accountable for the same.

Some people used to send the login ids and passwords by email. Since email communication is using plain text somebody can sniff the data. So it's advisable not to send the ids and password via mail, telephone conversation.

They can use alternate mechanism by saving them in a file and zipping it and sending to customers or by sending through post etc.

11.9 ROLE OF MONITORING STAFF

In every there should be a separate person in charge of logging and monitoring. He should be made to see the logs and monitor for potential security threats and ensure the logs are safely kept without tampering. He should also ensure that the logs are backed up and kept in a separate media and outside the facility for future reference.

11.9.1 Why they should monitor all critical activity?, Why they should monitor changes.

They should monitor since the potential threat to the systems can be via insiders or hackers. No logs should be accessed by others and using utilities like Tripwire and similar can help to identify the files for knowing whether it's changed.

Also if the log is misused the users can access the data and delete. At any point of time the log needs to be intact to get the correct information. So its necessary to monitor and maintain logs safely.

11.9.2 How activity of these accounts must be reviewed

11.10 USAGE OF PRIVILEGED OR SHARED ACCOUNTS

11.10.1 How access to these accounts must be logged?

11.10.2 How activity of these accounts must be reviewed?

11.11 IMPORTANCE OF AUDIT

11.11.1 Internal auditing organization & reporting structure

Adequate security is a basic requirement for every e-commerce or networked system. This applies to all the important components... like the LAN, Firewall, Routers, Internet, and so on.

But how do you ensure that the security is appropriate and up to detail? How do you know that there are no major exposures? How do you audit it? So Audit only reveals how secure the systems are.

A computer and information security audit can be an extremely difficult undertaking. The growing complexity of information systems requires an extremely comprehensive and detailed audit program. A separate internal Audit teams must be formed and they should conduct internal audits at predetermined time for having compliance.

11.11.2 Audit checks for compliance to security ppolicies & violations of any applicable regulations

External Auditors like PWC,KPMG can be asked to audit the companies for BS7799 Compliance. Its necessary at the time of audit that the log maintenance and audit logs are there as proof of the security measures taken in a company.

A computer audit must embrace a variety of requirements. Consideration of risk is of growing importance, but fundamental to the whole security audit program is compliance with the audit checklist of the company and of course the organization's information security policies.

11.11.3 Escalation of audit findings

The escalations found in the audit finding needs to be informed to IT managers and Security managers for improvement and they should be evaluated and should protect the Information Security. The Management should support the audit findings by allocating funds and persons to carry out the audits and administrators to implement the security plans according to the company requirements that align the goals and vision of the company.

11.11.4 Follow-up on audits

The follow-up on audits should be done once the required findings are evaluated and should evaluate the current implementation. Regular audits enable the Company to see whether the required policies are maintained. Incase if the company goes for Recertification of a Standard it's required to have the audit practices in routine.

New Additions

Analyzing the log generated by the servers, network equipments, and perimeter defense devices is the most difficult thing in the security arena. It is comparatively easy to configure a device and make it working and forget about it. A comprehensive log analysis methodology needs to be in place to make sure that the devices are doing what they are asked to do.

The art of log analysis can be gained only with time and understanding of how things work. What to log depends on the devices that you are planning to monitor. The more detailed information you get the more dept your analysis may go. It is important to consider that the logging options of the devices when you consider perimeter defense equipments.

NTP and its Role

Imagine the case if we have logs from all the servers, routers and other perimeter protection devices, but the administrator gave less importance to the time and all these devices are in different time zone and have different time. In this case we have everything but almost useless.

It is important to have all networking devices, perimeter protection devices and the server to synchronize for time. It is extremely important for an Organization to have NTP server which synchronizes with one of the stratum4 or better NTP server and all the devices synchronize with these NTP Server. Depending upon the IT environment you can have multiple NTP servers and devices can synchronize with these servers.

Centralized Logging

When ever possible centralized logging option needs to be preferred over the local logging. Consider the case of the perimeter protecting device like firewall, routers etc they have only minimum storage capacity and can store only less information. A

Security administrator should consider logging these device logs to a centralized logging server.

A log server gives a central point of administration for logging and alerting. The importance of centralized log server comes when we consider the fact that, if an intruder breaks into a system the first thing they will do is to cover their tracks by clearing the system logs. If the log entries have already been shipped out to a remote server, then the attacker needs to strive for long to clear his/her trace.

In case attacker compromised the centralized log server then he/she will have complete picture of your network and what each and every device is doing. So it is extremely important to make sure that your centralized log server is protected to the maximum possible. These are points that needs to be considered when deploying the log server

- The log server should have lot of disk space
- Should not have any trust relationship with any other devices.
- Should not run any other services apart from the syslog services
- Should be physically secured
- Management of the device should be from local console.
- It should be a fully armored and strip down operating system
- It should be on a protected segment
- Access to this server needs to be on a controlled basis

Some measures can be made to protect the logs in your machine. This example is given taken into consideration of the syslogd. When an attacker compromises a system he/she will look into the /etc/syslog.conf to check where things are logged and clear away his tracks. So it will be handy if you can fool the attacker by configuring syslog to take the configuration from some other location rather than the default /etc/syslog.conf location. (This doesn't mean that the attacker wont know where it is being logged it will delay the process.)

Firewall Logging

The firewall and route ACL logs provide a great amount of information. But the most of the firewall and the router ACL will not log the TCP flags and state with in the packet. This is an important piece of information which needs to be analyzed for getting a complete picture of what is happening. It is important to make sure that you

log the deny ip any any rule. On a minimal the following fields needs to be logged by any perimeter protection device

- Source and Destination IP
- Transport (TCP, UDP, etc)
- Source and Destination port
- Date and Time
- Action (permit and Deny)

The log analysis will be easy if the following fields can be also logged by the devices.

- Option fields (TOS, TTL, ID etc)
- Flags (SYN, ACK, PSH etc)
- Interface
- Window, Sequence number
- Some payload content.

The log analyst should also understand the packets that are logged by each of the devices. Some devices (for eg:- Checkpoint) logs only the initial packet of the connection, this may be lead to inaccuracies in case the log analyst is not aware of this. When considering the logging option IPtables has gone much ahead of other firewalling devices. It can provide you with the minimal and bogus field and has the ability to do log prefixing which is extremely good for a log analyst to track down future activity from that IP Address and alerting.

Log Review

It is extremely important to understand what the normal traffic to your environment is before starting the log analysis. This can be achieved by continuous monitoring the logs for one week or more. While doing the log review it is extremely important to look at the time factor as well. Consider the case you are missing events for some times on a busy server. What can cause this, crash in the syslog daemon, no activity for that period or somebody cleared the logs for that period. It is easy to clear logs from the syslogd logs files, but difficult in case of windows event logs.

Alerting

The big question one needs to ask, Am I patient enough to go through the huge logs that I am receiving. Most of them feel that the job is a boring one and wishes to do

something else. So it is your responsibility to come up with something which helps you in log analysis.

Alerting is easy and less time consuming way to inform the security administrator that further investigation is required. An alert for example can be generated for a DNS zone transfer. This prompts you to investigate further into the logs. Alerting is nothing more than a pattern matching and will alert of a zone transfer only in case it is programmed to do so.

The great pattern patching tool that you can use is grep. (Grep is available for windows as well).

Alerting Tool - Swatch

Swatch is freeware log analysis tool. It looks through the log files looking for the pattern that the security administrator has defined. It can generate customized alerts like send e-mail, dial pager etc.

Event Correlation

Now we have logs from all the devices and the servers on the centralized logging server, whether it will be handy to have a event correlation tool that will help to correlate events generated by multiple devices and servers.

SEC, simple event correlator is free and platform independent event correlation tool written in perl. Netforensics is other commercial tool which does event correlation. It is extremely important to understand the device support by each of these tools to make sure that the tool understands the logs generated by your device.

Appendix

This appendix is used to describe the log monitoring technique used by me to get the event log generated by windows servers. Anyone can use and modify this.

Aim: To analyze the security logs generated by windows 2000 server and mail back the result. The events ID of concern are 528 and 529.

Tools used:

- Dumpevt from somarsoft
- Blat – mailing system for windows
- Custom made script

Dumpevt: Windows NT program to dump the event log in a format suitable for importing into a database. This program gives the output of the log files in the comma separated format.

Usage:

```
C:\dumpevent>dumpevt

Somarsoft DumpEvt V1.7.3, Copyright ⌐ 1995-1997 by Somarsoft, Inc.

==>Missing /logfile parameter

Dump eventlog in format suitable for importing into database

Messages written to stdout

Dump output written to file specified by /outfile or /outdir

Parameters:

 /logfile=type      eventlog to dump; can be app, sec, sys, dns, dir, or rpl

 /logfile=type=path backed up eventlog file to dump

 /outfile=path      create new file or append to end of existing file

 /outdir=path       create new .tmp file in specified directory
```

```
/all            dump all recs (default is recs added since last dump

/computer=name  dump eventlog for specified computer (default is local)

/reg=local_machine  use  HKEY_LOCAL_MACHINE  instead  of
HKEY_CURRENT_USER

/clear          clear event log after successful dump

Specify formatting parameters in DUMPEVT.INI file
```

Blat: Blat is a Public Domain Windows console utility that sends the contents of a file in an e-mail message using the SMTP protocol.

Script: Custom made one to mail the result

To extract the windows security event log dumpevt.exe is used. The command used to extract the windows security event log is

c:\dumpevent\dumpevt.exe /logfile=sec /outfile=c:\report\ouput.log

This will produce a log file, output.log, having the security event log in comma separated format. This log is zipped using the gzip utility and mailed to the concerned person.

To use blat, first it is required to specify the SMTP server and the mail address

(Blat -install <server addr> <sender's addr> [<try>[<port>[<profile>]]] [-q)

The following bat file is used to zip the comma separated event log created by dumpevt.exe and mail to the concerned person. This bat file is schedule to run at 00:00 hours every day.

```
c:\ dumpevt.exe /logfile=sec /outfile=c:\report\ouput.log

c:\ gzip.exe c:\report\output.log

c:\ blat c:\report\report.txt –to thanzeer@test.com  -attach c:\report\ouput.log
```

Now the logs has been zipped and received on my mail box. I used the map drive of a Linux machine to store this log and will remove from the server once the analysis is over.

I used the pattern matching tool in Linux grep to get the details that I require. Following is the script that I used to extract the information and mail back to me.

```
# Script name log analyze #

gzip -f -d /usr/aa/eventlog/output/output.log.gz

rm -rf /usr/aa/report/$1/*

cat /usr/aa/eventlog/output/output.log.gz |grep $1|grep 528| cut --delimiter=^ --fields=2-8 >> /usr/aa/report/ouput/loggedinuser.txt

if [ `ls -s /usr/aa/report/ouput/loggedinuser.txt |cut -c1-4` -gt 0 ]; then cat /usr/aa/report/ouput/loggedinuser.txt | mail -s 'loggedin user Account for '$1 aa@test.com; fi

cat /usr/aa/eventlog/output/output.log.gz |grep $1|grep 529| cut --delimiter=^ --fields=2-8 >> /usr/aa/report/output/invaliduser.txt

if [ `ls -s //usr/aa/report/output/invaliduser.txt |cut -c1-4` -gt 0 ]; then cat /usr/aa/report/output/invaliduser.txt | mail -s 'Invalid user Account for '$1 aa@test.com; fi
```

The above mentioned script has one variables as the input - the date. This script is called by another script which passes the date information to this.

```
#!/bin/bash

# Passes the date argument 1 to the log-analyze script

if [ `date -d yesterday +%m` -gt 10 ]

then

arg1=`date -d yesterday +%m/%d/%Y`

/usr/aa/script/log-analyze web2 $arg1
```

The argument passed is yesterdays as I will get last days report on the next day. And the first argument is filename.

With this I will get two mails every day from all my servers stating the invalid accounts and the logged in users. You can add much more event id to this and use this script to get a summary of the security event log each day.

Note: I am extremely poor in programming and this can be done in much better way using some other programming language.

12ENTERPRISE CHANGE MANAGEMENT

12.1 INTRODUCTION

Enterprise Change Management is a collection of policies, processes and procedures that support management provided directives regarding the implementation and management of information security within the enterprise. They support these directives through controlling, planning, reviewing, approving, tracking and measuring changes within the organization. These directives are often mandated by regulatory compliance efforts.

Unplanned and uncontrolled change within an organization is often sited as the largest contributor to, or cause of, system downtime. Uncontrolled change occurs in all organizations, large and small. The ability to quickly implement change is often rewarded in smaller organizations for providing speed of response, and viewed as "being pro-active", when in most cases, it is actually reactive, poorly planned and executed, and increases operational risk. I call it the "Cowboy Syndrome". There is no control or planning in the wild, wild, west, where it's every buckaroo for themselves, leaving strategy and accountability to the wind.

Author and IT Service Management expert, Harris Kern, reports that in a 2005 survey of 40 corporate IT infrastructure managers, 60% admitted that their change handling processes are not effective in communicating and coordinating changes within their production environment. Among the key findings of the study:

- Not all changes are logged 95%
- Changes not thoroughly tested 90%
- Lack of process enforcement 85%
- Poor change communication and dissemination 65%
- Lack of centralized process ownership 60%
- Lack of change approval policy 50%
- Frequent change notification after the fact 40%

I recommend the introduction of formal change management to all organizations using a phased approach, allowing the IT teams to adapt to the introduction of new processes and procedures over time.

12.1.1 Objectives

The ultimate goal of a successful Change Management process implementation is to lower the amount of introduced risk into the environment as much as possible, and to reduce the amount of unplanned work as a percentage of total work done. Organizations that are constantly fighting fires see this figure at 65 percent or higher.

The objectives of the Change Management process are to establish a review and approval process for changes that are to be introduced into the business environment, technical infrastructure, and its supporting processes and procedures. This allows management the opportunity to align changes with strategic, tactical and operational objectives, as well as with policies, standards, procedures and guidelines in use within the enterprise.

The objectives for this document are to provide an overview of the Change Management process, to provide guidance for implementing supporting processes, and the insight and knowledge required to perform a base Change Management audit.

12.1.2 Purpose

The complexity of the IT environment and the increased connectivity between infrastructure components, end points and applications increases the risk of network instability and service interruption due to the impact and timing of even seemingly minor changes.

The number of major and minor changes within a typical IT environment is expected to increase over time, and the risk of outages to business users of IT services increases in significance as more and more users come to rely on technology for daily operations.

It has been widely recognized that Change Management is an approach that can identify and mitigate many of these risks, and improve the overall efficiency of IT in delivering reliable services. There are often dependencies between changes introduced for operational reasons and as a result of projects. In many cases, major efficiencies can be realized by coordination and planning between these sources of change.

The Change Management process enables communication, impact analysis, and scheduling that can reduce unintended and unexpected impacts on users.

Many project-based initiatives compete with the day-to-day operations groups for resources in terms of technology (Server/Desktop/Infrastructure/Support) as well as staff and skills. Effective Change Management can balance these activities against operational requirements.

The initial implementation should focus on the creation of a process that creates basic outputs such as:

1. A single mandatory change approval process that is used by all of IT.

2. A set of standard requirements that must be met in terms of:
   - Description of the change
   - Identification of dependent and related systems
   - Description of anticipated impacts
   - A communications plan
   - A detailed deployment plan
   - Maintenance documentation
   - Training requirements
   - Metrics for measuring success and impacts

3. A shared Change Calendar listing all changes to the Production Environment

12.1.3 Benefits of Change Management

- Minimizes disruption and problems inherent in the introduction of change.
- Adds auditable records of all changes and their approvals.
- Eases detection of unauthorized and unexpected change for security purposes.
- Provides increased visibility into, and record of, system evolution.
- Increases the volume of system documentation available.
- Facilitates the speed and success of major change delivery.
- Ensures that the integrity of the business needs of the Firm are met.
- Allows tighter alignment of the IT environment with business objectives.
- Reduces User Impact due to change.
- Provides for better use and allocation of IT Resources.
- Allows optimization of deployment through bundling of related changes.
- Increases IT's capacity to implement change effectively.
- Improves user satisfaction with service reliability.
- Increases compliance with Sarbanes Oxley, Bill c-198 and other regulations.

12.1.4 Risks

Some of the typical risks encountered when implementing Change Management:

- Lack of upper management support.
- Resistance to new processes and change.
- Incomplete requests submitted, slowing down the process.
- Rubber-stamping approval of changes without thorough review.
- Lack of appropriate tools (typically CMDB and Audit Tools).

12.1.5 Definition of Success

All stakeholders should view change Management as a beneficial, responsive process that enables and improves the ability to deliver reliable services.

All Changes will be documented, approved, and scheduled using the defined Change Management Process.

The Change Management Process will minimize problems and disruption, improve the speed of service delivery, and ensure the integrity of the IT environment, in support of the business needs of the Firm.

Metrics will be defined to measure the achievement of these goals.

12.1.6 Metrics

Various metrics should be collected to gauge the success of the process, areas for improvement, trends, measure downtime and overall effectiveness of the process. Metrics for Change Management will evolve over time according to the business' needs, however a minimal set of metrics is provided below:

- Total Change Requests submitted.
- Total Change Requests executed.
- Total Change Requests by month.
- Total Change Requests by type.
- Total Change Requests by owner.
- Total Change Requests successfully implemented.
- Total Change Requests unsuccessfully implemented.

Advanced Metrics:

- Total Change Requests rejected.
- Reasons for Change Rejection
- Total Changes rolled back.
- Unauthorized Changes detected.
- Total records in Configuration Management DataBase.

12.1.7 Pre-requisites

In order to be successful, Change Management will require a documented and formalized security policy, including a policy update schedule, as well as an audit and review report of the security policy.

If a complete copy of the security policy can't be obtained, request an outline of areas covered in the policy, or at least the table of contents of the policy.

Recommended: Audit or review reports of enterprise configuration management policy, Configuration Management DataBase and asset management data.

The importance of asset data is pivotal from a Change Management perspective, as well as from a Security perspective. In order to properly manage an asset, one has to be aware of its existence, be able to *find* it, *understand* its configuration, and *be certain* that it has not been changed or removed without authorization.

Without accurate and complete asset information, including component listings, relationship information, and configuration data, it is virtually impossible to assess system and network vulnerabilities, or to take remediative action once a vulnerability is suspected or reported.

As a Change Management process matures, it will evolve into a Change Control process, where critical systems are audited on a day-to-day or even hourly schedule. This provides incredible control, and can expedite a security investigation exponentially. **An unauthorized change is a security breach**.

12.1.7.1.1 General Requirements

In order to be successful, the Change Management process needs to be supported and endorsed by management. A Change Management Policy must be developed, and the IT Executive must approve any changes to the processes or procedures involved in writing.

12.1.7.1.2 Technical Requirements

Change Management requires the following technical elements:

- Change Control Spreadsheet for tracking current change requests.
- Opportunity Evaluation Form for building major change proposals.
- Preliminary Analysis Form for refining major change proposals.
- Request For Change Form for detailing all change requests.

Recommended:

- Configuration Management DataBase for tracking configuration and change items.
- Change Control Auditing Software for detecting unauthorized changes.

12.1.8 Summary

Change Management is a complex and involved process that provides many significant benefits to an organization. It can swiftly move forward regulatory mandated exercises, provide clarity into systems that are very complex, and increase the ease of audit. Many sub-processes, including asset management, configuration management, service delivery processes and communication processes, directly support the Change Management process.

12.1.9 The Framework

12.1.9.1 PHASE 1 - PREPARING FOR CHANGE

The first phase of a Change Management implementation resembles the triage system used by hospitals to allocate scarce medical resources. The primary goal of this phase is to stabilize the environment, shifting from firefighting to proactive work that addresses the root causes of problems.

- IT must identify the most critical systems.
- IT must identify systems that are generating the most unplanned work.
- Plan and take appropriate action to gain control of these systems.

Outputs:

- Critical systems identified and configurations documented
- Change characteristics profile
- Organizational attributes profile
- Change management strategy guidelines
- Change management team structure
- Sponsor structure and responsibilities

12.1.9.2 PHASE 2 - MANAGING CHANGE

The second phase focuses on the planning, design and implementation of work that addresses the root causes of problems.

Outputs:

- Communications plan
- Sponsor roadmap
- Training plan
- Coaching plan
- Resistance management plan
- Master change management plan
- Project team activities

12.1.9.3 PHASE 3 - REINFORCING CHANGE MANAGEMENT

The third phase focuses on measurement, process refinement, and continuous improvement.

Outputs:

- Gap analysis report
- Compliance audit reports
- Corrective action plans
- Post action review for continuous improvement

12.1.10 Change Management Phase Diagram

In each phase, provide guidelines, steps, and action plans for the change management team. Assessments and worksheets help to pinpoint the unique characteristics of your change management program. Templates help to develop critical change management plans in a standard and repeatable manner.

12.1.11 Psychology of Change

When change is first announced, people generally have common reactions. If you can understand what they are thinking, then you are better prepared to address their concerns.

12.1.11.1 NEEDS

The principles in Maslow's Hierarchy explain that when something happens and we feel we might be threatened, we revert to checking lower-level needs. We ask questions such as:

- Safety: Will I still have a job?
  Will I lose control?
- Belonging: Will I have to change my work methods?
  Will I lose teammates?
- Esteem: Will my social status change?
  Will I have less influence?
- Identity: What does this mean about who I really am?
  What is my role?
- Prediction: What will happen now?
  Can I see a new future?

12.1.11.2 VALUES

Our individual needs lead us to seek rationality. It is easy to allow these thoughts to revert to stress values if not addressed.

Those affected by process and procedural changes will tend to be highly critical of the people who are implementing the changes, and the actions they take, if we do not see value in the changes, perceive the changes as a threat, or do not understand the reasons for the changes. We assess the values of these people, and whether their actions are moral or ethical, using our own standards. Even if we do not agree with the outcomes, it is very important for us to perceive the process as fair.

12.1.11.3 GOALS

Even if we safely get past considerations of individual needs and values, we must also consider the impact of the change on our personal and organizational goals.

- How will it affect my current work? Can I finish it off? Should I bother?
- How will it affect my future prospects?
- How will it affect my value to the company?
- Should I be looking for another job?

12.1.11.4 PROCESS MATURITY

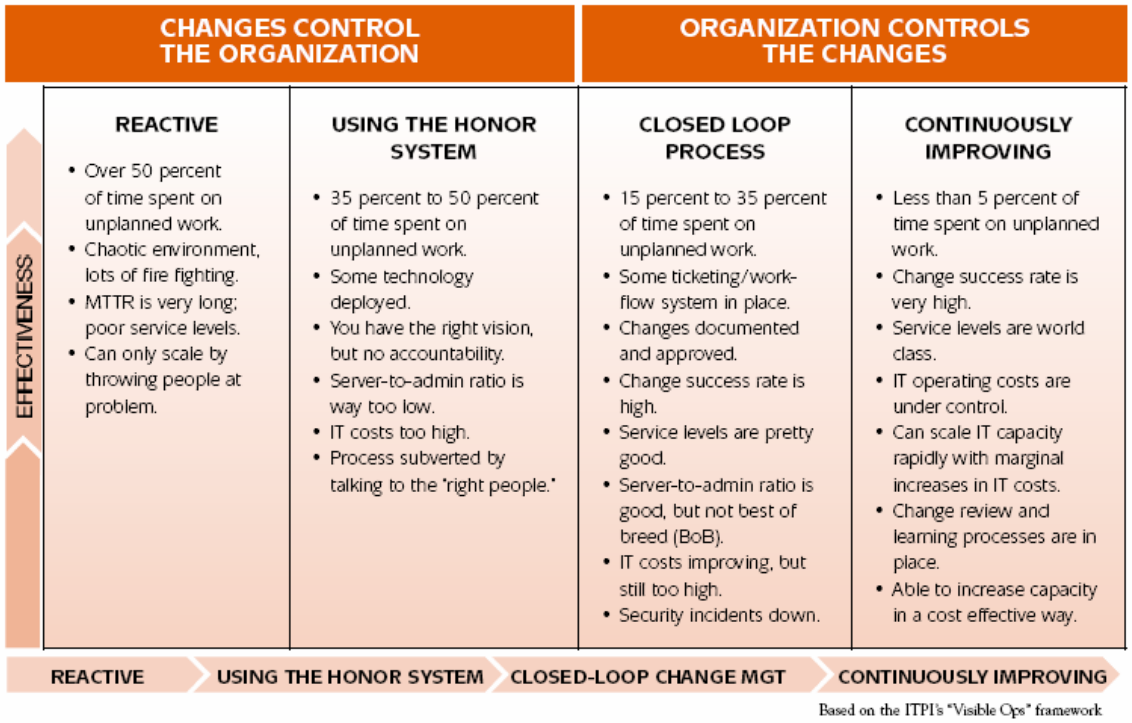
The management of change is an evolutionary process. Do not become discouraged as you start developing your change management processes. The solutions may require changing people, processes, and technology over time in order to get it right.

The following illustrates the typical stages of the change management process:

- **Oblivious to change**
  - Hey, did the server just reboot?
- **Aware of change**
  - Hey, who just rebooted the server?
- **Announcing change**
  - I'm rebooting the server. Let me know if that will cause a problem.
- **Authorizing change**
  - I need to reboot the server. Who needs to authorize?
- **Scheduling change**
  - When is the next maintenance window? I'd like to reboot the server.
- **Verifying change**
  - Looking at the logs, I see the server rebooted as scheduled.
- **Managing change**
  - Let's schedule the server reboot to week 45 so we can coordinate the maintenance upgrade and reboot for the same time.

The granular goals of Change Management are to reduce the amount of time spent on unplanned work, reduce the number of self-inflicted problems, reduce risks, and modify how problems are solved so that change is ruled out early in the recovery process.

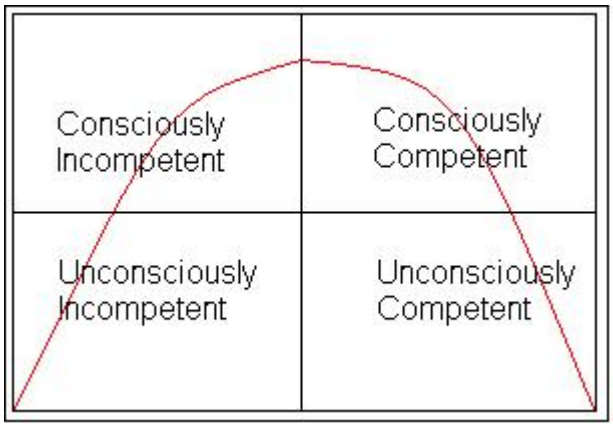
By increasing the change success rate and reducing Mean Time To Repair (MTTR), you not only decrease the amount of unplanned work, but also increase the number of changes that can be successfully implemented by the organization in a shorter span of time.



12.1.11.5 TEAM LEARNING MATURITY

In "Bringing Peace into the Room: How the Personal Qualities of the Mediator Impact the Process of Conflict Resolution" (D. Bowling & D. Hoffman eds. 2003), Peter Adler, a well-known mediator, describes the four stages of skill development:

1. Unconscious incompetence,
2. Conscious incompetence,
3. Conscious competence, and
4. Unconscious competence.



He illustrates these stages by following the efforts of a person who is learning to surf.

Our intrepid surfing student sees some surfers "playing" in the waves, and they make it look so easy. He buys a board and a pair of shorts. He is totally prepared to conquer the sea. He is unconsciously incompetent, because he doesn't know the basic precautions that should be taken, what level of knowledge, hard work, and skill is required for the task.

After his first day out, with much effort, the new surfer may be half-standing, half-crouching on the board, twitching and fighting for balance with each swell of the water. The surfing student has realized that it is a little harder than he originally thought. His muscles are throbbing, and he is feeling the effects of a little sunburn, too. He is still ignorant of the deeper skill level required to master surfing. He can identify the skills that he has yet to learn that will improve his performance. He has found the conscious incompetence stage of skill development.

At the third stage of the cycle, the surfer can skillfully catch a wave, knows a lot about the equipment, the best places and times to surf, and has a good time each day on the beach. He still returns home exhausted by his efforts, and as long as he is thinking about his entries, exits, moves, maneuvers, and is aware of his surroundings, he can hold his own. Our surfer is now consciously competent.

With continued practice and time on the board, he eventually crosses an invisible barrier, and surfing seems to get easier. He takes on bigger waves at exactly the right moment on a beach he knows as well as the back of his hand. He comes off the wave energized and exhilarated, not exhausted. He can estimate the size and precise timing of the next wave, and intuitively moves to the correct position to catch a wild ride. Surfing is now second nature. He has found the fourth level of competency – unconscious competency.

Learning about Change Management, and any other process is synonymous with this example. Practice, refine and learn to gain the necessary skills, find the right tools, and master the art and the science.

12.1.11.6 MANAGING RESISTANCE

Many factors contribute to employee resistance to change. The top five are:

1. Employees are not aware of the business need for change. Employees do not understand why a change is being made, or how the change will impact them.
2. Lay-offs announced or feared as part of the change. Employees are concerned about being unemployed and the financial implications involved.
3. Employees are unsure if they have the skills needed for success. Employees may be concerned about new responsibilities, changing technologies and whether they would be able perform well under a new measurement system.
4. Individuals are comfortable with the current state. Employees want to maintain the personal rewards and sense of comfort provided by the status quo.
5. Employees feel overworked or undervalued. Employees believe they are being asked to do more with less, or do more for the same pay.

Manager resistance to change is attributed to a number of different factors as well.

These are the top reasons cited for mid-level manager resistance:

1. Loss of power and control. Managers may perceive change as having a negative impact on their span of control and on their careers.
2. Overloaded with current responsibilities. Managers already have many responsibilities and the change creates more to manage. In some cases there is already too much change going on in the organization.
3. Lack awareness of the need for change. Managers may not understand the business need for change or the risks of not changing.

4. Lack the required skills. Some managers may not have the skills to manage change or employee resistance. Other managers lack the skills required to succeed in their new roles. They resist because they feel unprepared to manage the change.
5. Fear, uncertainty and doubt. Managers may lack clarity surrounding the change. They are skeptical about the change or fearful and uncertain about the future.

There are several important lessons to derive from these two lists.

- The reasons employees resist change are different than the reasons managers resist change.
- Resistance is not a uniform phenomenon - understanding the 'why' of resistance will allow you to better execute the 'how' of overcoming the resistance.
- Often, change managers and project teams believe resistance stems from disagreement with the future state, but research shows that most causes of resistance are related to the current state, and not the actual 'change' or future state a project or process is creating.
- Teams can take actions to mitigate many of the reasons for resistance.
- Proactively identifying potential resistance and its causes can help teams build buy-in early on, and minimize resistance as the change is introduced.

12.1.11.7 RESISTANCE RELATED ARTICLES

- Rationale for resistance: What people tell themselves.
- The nature of opposition: Knowing your 'enemies' in change.
- Signs of resistance: Spotting subtle signs of dissent.
- Dealing with resistance: A range of methods for use.

12.2 METHODOLOGY

12.2.1 Phase 1 – Prepare:

Outputs:

- List of assets.
- List of critical assets & relationships.
- Change characteristics profile.
- Organizational attributes profile.
- Change management strategy guidelines.
- Change management team structure and responsibilities.
- Sponsor structure and responsibilities.

Activities:

- Define your change management strategy.
- Prepare your change management team.
- Develop your sponsorship model.

12.2.1.1 INTRODUCTION

At this stage, you are laying the groundwork for your Change Process. Start by cataloging your assets. Then identify the systems and business processes that are critical to the business as well as the ones that generate the greatest amount of firefighting efforts. When problems are escalated to IT operations, which servers,

networking devices, infrastructure or services are constantly being revisited each week (or worse, each day)?

These items are your list of "most fragile objects". These are the systems that must be protected from uncontrolled changes, both to curb firefighting and to free up enough cycles to start building a safer and more strategic route for change.

For each fragile object (i.e. server, switch, router, PC, etc.), do the following:

1. **Reduce or eliminate access:** Block access to these fragile objects to all except those that are formally authorized to make changes. Because these assets have low change success rates, you must reduce their volume of change.

2. **Document the new change policy:** Keep the change policy simple: "Absolutely no changes to this asset unless authorized by me." This policy is a preventive control and creates an expectation of behavior. It allows you the opportunity to review and approve all changes. Amend the policy as we move forward.

3. **Notify stakeholders:** After the initial change policy is established, notify all of the stakeholders about the new process. Make sure the entire staff sees it. Email it to the IT team, print it out, and post it next to the fragile system.

4. **Create a change window:** Work with the stakeholders to set specific times when changes may be introduced. The goal here is to establish a practice of expected maintenance windows, and to start coordinating ALL maintenance into these windows.

5. **Create an audit window:** Trust, but verify. Collect all of the authorized change records, and examine the system for any unauthorized changes.

6. **Reinforce the policy:** If any unauthorized changes are found, identify the person(s) responsible for making the changes. Reprimand them for their policy breach, and have them do additional paper work to justification the changes. Most often, Change Management is circumvented as a way to avoid what is considered excessive paperwork. If circumvention of the process is seen to generate more paperwork than following the process, it stands a better chance of being followed.

   Repeated policy breaches may need to be reviewed as a performance issue.

12.2.1.2 CREATE THE CHANGE MANAGEMENT TEAM:

Continue to develop the change management process by creating a Change Advisory Board (CAB), comprised of the relevant stakeholders of each critical IT service. These stakeholders are the people who can best make decisions about changes because of their understanding of the business goals, as well as technical and operational risks.

12.2.1.3 IDENTIFY AND INVOLVE THE SPONSOR:

Identifying and involving the sponsor sometimes occurs before the Change Management Team is officially formed, but either way, you will need a sponsor from upper management. Look for a “C” level executive or one of their direct reports.

You want to connect to someone that understands the business, is in a position to connect to decision makers, and has the authority to make strategic and financial commitments. Seek a sponsor that will gain buy-in based on the value that the process will bring to the organization.

Participants in a 2005 study conducted by The Change Management Learning Center (http://www.change-management.com/best-practices-report.htm) were asked to identify their greatest contributor to overall Change Management project success.

Number one greatest contributor: Active and visible sponsorship.
One half of those that responded ranked their sponsors as average to poor when asked to evaluate how 'active and visible' the sponsor was during the change process, and only half of the participants felt their sponsors understood the role and responsibilities related to managing change.

What it means:
For the third consecutive study, the role of the sponsor was highlighted as the greatest contributor to overall project success. In the 2005 study, this was cited three times more frequently than any other factor. The conclusion is that as change agents, we need to make sure our sponsors understand how important their involvement is, and what effective sponsorship looks like.

The 2005 study provides the most complete and concrete checklist of sponsor activities available. The itemized list is a great foundation for a 'sponsor checklist' you can use with your sponsors. Change Management Teams must act as enablers to ensure that sponsors are executing and sending the 'right' messages. I would encourage anyone interested in implementing a successful Change Management process to purchase a copy of this report and checklist.

12.2.1.4 CHANGE MANAGEMENT MEETINGS:

Start weekly Change Management meetings to authorize changes and daily change briefings to announce changes. This creates a forum for the CAB members to make decisions on requested changes.

The CAB will authorize, deny, or negotiate a change with the requester. Authorized changes will be scheduled, implemented, and verified. The goal is to create a process that enables the highest successful change rate throughout the organization with the least amount of bureaucracy possible.

12.2.1.5 DO'S AND DON'TS

Here are some tips for effective change management.
Items to do:

- Do perform post-implementation reviews to determine success or failure.
- Do track the change success rate.
- Do use the change success rate to learn and avoid making risky changes.
- Do make sure everyone attends the meetings, otherwise auditors have a good case that this is a nonfunctioning control.
- Do categorize the disposition of all changes. All outcomes must be documented once a change is approved. Three potential outcomes are:
    - Change withdrawn - the change requester rescinds the change request, along with the reason why. This should not be flagged as a failed change in change metrics.
    - Aborted - the change failed, document what went wrong.

- Completed successfully - the change was implemented and is functioning appropriately.

Items not to do:

- Do not authorize changes without reviewing rollback plans. Think ahead about how to recover from a problem rather than during implementation.
- Do not allow, "rubber-stamp" approvals. Review RFC's fully.
- Do not let change owners off the hook - understand what caused issues.
- Do not send mixed messages. The first time the process is circumvented, incredible damage can be done to the process.
- Do not expect to be doing complete Change Management from the start. Constantly refine the processes.

12.2.1.6 CREATE A CHANGE REQUEST TRACKING SYSTEM:

A prerequisite for any effective Change Management process is the ability to track requests for changes (RFC's) through the authorization, implementation, and verification processes.

Paper or spreadsheet based tracking systems quickly become impractical when the organization is large or complex, or when the number of changes is high. Because of this, most effective groups use a database to track RFC's and assign work order numbers. Some refer to these applications as ticketing systems or change workflow systems. The primary goals of a change request tracking system are to document and track changes through their lifecycle and to automate the authorization process. The system can also generate reports with metrics for later analysis.

Each change requester should gather all the information the Change Manager needs to decide whether the change should be approved. In general, the more risky the proposed change is, the more information that is required.

For instance, a "business as usual" change, such as rebooting a server or rotating a log file, may require very little data and oversight prior to approval. On the other hand, a high-risk change such as applying a complex security patch on a critical production server may require good documentation of the proposed change, but also extensive testing before it can even be considered for deployment.

12.2.1.7 DEFINE ROLES & RESPONSIBILITIES

Everyone involved in Change Management and implementation should understand their role and responsibilities, as well as the roles and responsibilities of the rest of the team. Roles and responsibilities should be clearly defined, documented and shared. This will improve the ability of the team to communicate, provide and request information, and encourage collaboration and accountability.

For instance:
The Change Manager is a management role, focused on process management and reporting. This is not necessarily a full time responsibility, depending upon the size and complexity of the organization, but to ensure that the process is working, it does require someone to be on site full time to deal with Change related issues as they arise.

The Change Coordinator is an administrative role, focused on the day-to-day operation of the Change Process. This is not necessarily a full time responsibility, depending upon the size and complexity of the organization, but to ensure that the

process is working it does require someone to be on site full time to deal with Change related issues as they arise.

Change Management Fundamental Roles

Role	Responsibilities
Executive:	• Reviews RFC for strategic soundness. • Approves/Rejects RFC. • Authorizes resources (time, budget, staff). • Reviews reports.
Change Manager:	• Chairs the Change Advisory Board (CAB) meetings. • Acts as the focal point of the Change Management process. • Ensures all changes are adequately assessed to minimize risk and impact on the business. • Reviews Requests For Change (RFC) to ensure key criteria are provided, tactically sound, strategically aligned with business objectives. • Assesses risks. • Enforces standards and procedures. • Works with internal and external Service Providers to ensure completion of risk and impact analysis, workload estimates and test recommendations. • Provides a list of RFC's for review at CAB meetings. • Provides initial approval or rejection of RFC. • Identifies conflicts in the change schedule. • Reports metrics to Executive.
Change Coordinator:	• Reviews the initial Change Request (RFC) to ensure all relevant data is provided. • Enforces standards and procedures. • Logs and maintains the requests through lifecycle. • Maintains the Change Calendar. • Maintains the Change Process Metrics. • Identifies conflicts in the change schedule. • Updates Change Owners regarding status of changes. • Provides agenda and minutes of CAB meetings.
Change Owner:	• Reviews RFC for operational soundness. • Submits RFC to Coordinator. • Documents issues, risks, solution and alternatives. • Plans implementation. • Oversees implementation. • Reports success to Change Manager/Coordinator.
Change Submitter:	• Develops initial Change Request (RFC). • Completes RFC form details for change owner. • Revises RFC as per CAB/Executive request. • Researches issues, risks, solution and alternatives. • Reports success to Change Owner.
Change Implementer:	• Often Change Owner or Submitter. • Inputs into solutions and detailed plans. • Implements RFC per plan. • Reports success to Change Owner.

12.2.2 Phase 2 - Managing Change

12.2.2.1 INTRODUCTION

The second phase focuses on the planning, design and implementation of work that addresses the root causes of problems.

Identify the Business Owners of the systems and data that are to be subject to the Change Management process, and develop your Communications Plans to involve and alert them to planned, required and completed changes.

12.2.2.2 OUTPUTS:

- Communications plan
- Sponsor roadmap
- Training plan
- Coaching plan
- Resistance management plan
- Master change management plan
- Project team activities

12.2.2.3 ACTIVITIES:

- Develop change management plans
    - Communications plan
    - Sponsor roadmap
    - Coaching plan
    - Resistance management plan
    - Training plan
    - Master change management plan
- Take action and implement plans
    - Change management implementation

12.2.3 Phase 3 - Reinforcing Change Management

12.2.3.1 INTRODUCTION

The third phase focuses on measurement, process refinement, compliance, and continuous improvement.

Keep everyone accountable and responsible for playing by the rules. The goal is to continue fostering a culture of change management within the organization. To do this, change monitoring must be in place so that you can build trust, but verify. You will use this instrumentation to detect and verify that changes are happening within the specified change management process, to reinforce the process, and to deter unauthorized changes.

As the Change Manager, you must be aware of all changes on all infrastructure devices that you are managing: servers, routers, network devices, databases, etc. Each detected change must either map to authorized work, or it must be flagged for investigation.

Critical questions that need to be answered are:

- Who made the change?
- What did they change?
- Was the change successful, and implemented according to plan?
- Should it be rolled back? If so, then how?
- How do we prevent it from happening again in the future?
- Are there any lessons to be learned for future application?

The key to creating a successful culture of change management is accountability. If the change process is repeatedly bypassed, management must be willing to take appropriate disciplinary action.

12.2.3.2 OUTPUTS:

- Compliance audit reports
- Corrective action plans
- Post action reviews
- Success metrics
- Change metrics
- Up time & down time metrics

12.2.3.3 ACTIVITIES:

- Collect & analyze feedback
- Diagnose gaps & manage resistance
- Planning & implementing corrective actions
- Audit of configurations & changes
- Celebrating successes
- Reporting results

12.2.4 Metrics & Reports

When defining metrics to measure and report on Change Management and other IT services, it is important to consider how the data will be used. This may seem obvious, but all too often performance reports are produced to satisfy an imprecise demand from management for 'information' without any clear indication of what is actually required.

To create effective performance reports, identify the groups or functions that will use the reports and then establish their particular requirements. Put simply, we need to ask:

- What is the "look of success" for this audience?
- What information would be perceived as useful?
- How will the report be used?

These questions must be answered in order to confirm that the 'usefulness' of the report is firmly based on how the information facilitates the effective management, use, or enhancement of IT services.

Once we have a clear view of the information required, the next step is to work out how to produce the report from the raw data of the selected metrics. We need to ensure that measurement of all the required supporting metrics is practical, and determine how to convert and correlate the data to produce meaningful reports.

It is also important that users can easily understand the service reports. An essential part of the design process is to present the information in a straightforward way that clearly shows the relationship between the information and the underlying data.

One further consideration when choosing metrics is that they, and the targets associated with them, drive the behavior of staff involved in delivering IT services. Managers must recognize that this behavioral effect can be either positive or negative. For instance, using the metric 'Availability of the Capacity Plan on a Specified Date' is likely to have a positive effect on the performance of the Capacity Management team. However, this effect could become negative if too much

emphasis is placed on this metric, or the time frame is too tight, putting the team under pressure to produce the Capacity Plan on time even if it is not complete or up to appropriate quality standards. One alternative would be to introduce a balancing metric: 'The Capacity Plan is complete and of acceptable quality.'

We will identify the typical requirements of the three principal groups that utilize service reporting:

1. IT Operational Management
2. Users and Business Management
3. IT Executive Management

For each group, we address what information is useful and how it can be used to support their objectives. We also identify examples of the types of metrics that are required to generate this information.

Metric and Indicators	Guidelines
Number of changes authorized per week, as measured by the change management log of authorized changes.	In general, more changes indicate more change productivity, as long as the change success rate remains high. The trend (up, down or steady) should make sense in the business context. High-performing organizations can sustain over 1,000 successful changes per week.
Number of actual changes made per week, as measured by detective controls such as monitoring software.	The number of changes actually implemented for the week should not exceed the number of authorized changes.
Number of unauthorized changes.	These are changes that circumvented the change process. This is measured by taking the number of actual changes made and subtracting the number of authorized changes. Where detective controls are not present, no reliable measurement of actual changes can be made. In this case, the number of unplanned outages can be used as a substitute measure. Lower is better, but typically the only acceptable number of unauthorized change is zero; one rogue change can kill an entire operation or create material risk.
Change success rate, defined as successfully implemented changes (those that did not cause an outage, service impairment, or an episode of unplanned work) as a percentage of actual changes made.	Higher is better. When changes are not managed and not adequately tested, change success rates typically are around 70 percent. High-performing organizations not only regularly achieve change success rates of 99 percent, but failed changes rarely cause service interruptions or unplanned work.
Number of emergency changes (including patches), determined by counting the number of changes that required an urgent approval during the week using the change review board or emergency change process.	Lower is typically better. Many emergency changes indicate that the "real way to make changes" is to use the emergency change process either for convenience or speed. Emergency changes typically have a higher failure rate and generate unplanned work or rework. An increase in emergency changes may indicate that there are other problems. When emergency changes comprise more than 10 percent of total changes, the organization is almost certainly a low performer. In particular, two organizations that had catastrophic "front page news" IT failures were typically expediting more than 25 percent of their change requests.
Percentage of patches deployed in planned software releases.	When patches are deployed in planned software releases, they do not cause production disruption and have much higher change success rates. Higher is typically better. Paradoxically, high-performing IT organizations often have the lowest rate of patching. They often mitigate vulnerability risks without requiring changes to production systems (e.g., blocking the vulnerability at a firewall).
Percentage of time spent on unplanned work.	Planned work is time spent on authorized projects and tasks. Unplanned work includes break/fix cycles, rework, and emergency changes. Lower is better. High performing IT organizations spend less than 5 percent of their time on unplanned work. In contrast, hundreds of other organizations spend 30 percent to 40 percent of their time on unplanned work.
Percentage of projects delivered later than planned.	Lower is typically better. When organizations are spending all their time on unplanned work, often there is not enough time to spend on planned work such as new projects and services, thus causing project results to be delivered late.

12.2.4.1 PROCESS TRENDS

The ITIL Service Support processes (Service Desk, Incident, Problem, Change, Configuration, and Release Management) focus mainly on the day-to-day operation and support of IT services. Even if the ITIL framework is not fully implemented, tracking trends in these process areas as best as possible can highlight changes in workload patterns as well as in the way in which the IT function is coping with demand.

Managers can use process trend information to help plan resource requirements, reallocate resources, and identify other forward-looking actions that may be necessary to maintain service quality. The basic metrics required indicate demand for and performance of the various process areas. Trends in these metrics provide **Key Performance Indicators (KPI's)** for their respective processes.

Change Management metrics could include:

- The total number of periodic and cumulative changes.
- The number of emergency changes.
- The number of changes that were backed-out.
- Any unauthorized changes detected.

Configuration Management metrics could include:

- Total number and classifications of assets.
- The number of changes applied to the CMDB.
- The average and maximum times between receipt of the RFC and the update being applied to the CMDB.
- Uptime and downtime of critical assets.

12.2.4.2 PROCESS EXCEPTIONS

Process exceptions occur when the normal service management process cannot handle a particular event or circumstance. They are almost always indicated by an escalation to a higher level of management to resolve the issue.

Examples include escalation of incidents that seem unlikely to be resolved within their TRT, and the escalation of RFC's that have been rejected by the Change Management process as being too risky, too expensive, or because they cannot be scheduled within the required period. A certain number of process exceptions are to be expected, but the number should be kept under close review, as an increase may indicate that there is an underlying problem that needs to be investigated and resolved.

Investigate an elevated number of process exceptions in order to establish whether they represent a random blip or are indicative of an endemic problem. If the latter, the process should be altered, or some other action taken, to reduce this indicator.

Defining 'process exception' for each service management process is necessary in order to measure the occurrence of exceptions. This metric is a useful KPI for the process.

12.2.4.3 MITIGATION OF RISKS AND ABILITY TO MINIMIZE THEIR IMPACT

The assurance that risks to the availability of IT services have been identified and mitigated appropriately should be provided by:

- Availability Plan.
- IT Service Continuity Plan.
- Evidence of successful testing of the Continuity Plan.
- Security Assessment Report.
- Security Audit Report.
- Number of changes that were backed out.
- Review and update of the Security Profile Matrix.

Monitor the creation and update of these documents, their review, the testing activity, and correction of issues found. The reasons for any delay in the process should be investigated and corrective action taken.

The metrics that support the provision of this information are:

- Plans and reports are produced on schedule and meet quality criteria.
- IT Service Continuity Plan has been tested on schedule.
- All outstanding issues with IT Service Continuity and Security Management have been corrected within a defined period.

12.2.4.4 INTERNAL MEASURES OF PROCESS PERFORMANCE

Internal measures of various aspects of process performance can be used as KPI's to provide valuable information about how well the process is working and highlight improvement opportunities. For example, the length of time between passing an incident to a second-line support group and work being started shows the 'waiting time' for handling that incident. Unless the average waiting time is very short, there is a potential opportunity to improve the efficiency of the process by reducing or eliminating it.

Process performance measurements can also provide pointers to issues that may not yet have affected the outcome of the process. If there is an increase in the average waiting time for an incident, the service manager can investigate and decide what, if anything, to do about it.

Before deciding what to do in response to a KPI measurement or trend, it is important to have a clear understanding of the factors that have caused the deviation from the norm. Having a number of KPI's that measure different aspects of the process often helps to develop this understanding. Consider the following example:

> If the average time to resolve incidents affecting a particular IT application shows a sudden increase, the reason for the increase may not be immediately apparent. Another KPI may shed light on this trend, such as the number of IT staff that have been re-assigned to projects in the last three months from the group that supports this application.

While service reports may present information based on a range of KPI's, the metrics required to provide this information are the KPI's themselves.

12.2.4.5 REPORTING FOR USERS AND BUSINESS MANAGEMENT

Providing users and managers with reports covering the IT services that support their business processes is important. As users of the services, they need unbiased

information on the quality delivered so that any under or over achievement can be recognized and addressed.

Relevant information may also enable the identification of potential improvements in services or the way that they are delivered, and to propose changes in response to changing business requirements. It should also help manage their dependency on services and the costs of using them.

Service information often required by users and business management is:

- Actual service level achievement against SLA targets.
- Clearly stated reasons for service level failures and a description of the action being taken to prevent recurrence.

The following additional information is recommended for business management only:

- Usage information for services.
- Service trends and anomalies.

Information on actual service level achievement compared to SLA targets gives users an objective view of the quality of IT services and enables them to engage in discussion with their managers and IT. Measuring just the service levels actually experienced by users is critical. If there are differences between the reported and the real service levels, there is a risk that users will lose trust in the process.

IT is accountable for meeting SLAs, acting to investigate any service level failures, and taking action to prevent recurrence. Business management should review this information with IT, and ensure through constructive dialogue, that IT is actively managing service quality to meet agreed targets.

Because this report is based on measurement rather than perception means that it provides an accurate record of the services and can be used as the basis of any discussion about required changes or enhancements. The metrics required to provide this information are the Key Global Indicator (KGI) metrics specified in the SLA.

12.2.4.6 Clearly Stated Reasons for Service Level Failures

Users will want to know what went wrong when service level failures occur, what is being done about the failure, and what can be done to stop similar failures in the future. Making this information available to the users creates a climate of open communication. It also means that service managers have no place to hide. If repeated failures occur and the corrective action is always the same, business management can justifiably ask for a more effective response.

12.2.4.7 Reporting for IT Executive Management

IT executive management is responsible for governing services delivered by the IT function. They are accountable for achieving KGI's for the value to the business of the IT services delivered and for the effective management of IT-related risks.

- Risk management measures.

12.2.4.8 Risk Management Measures

IT executive management needs to know that risks to IT services have been properly assessed, that each risk has been reviewed by operational management, and that a decision has been made to mitigate the risk, transfer it, or accept it. They also need to know that an effective IT control framework has been implemented for risk

mitigation and management, and that information concerning risk management has been communicated within IT and business.

IT executive management should investigate the reasons for any indication that risk assessment or risk management activities are not being properly completed with operational management, and ensure that they are urgently addressed.

The metrics required to support this report include those aimed at operational management. In addition, measurements of the effectiveness of IT controls are needed. These can be produced by undertaking or commissioning an assessment using an industry-standard framework such as COBIT (Control Objectives for IT) to provide a consistent structure.

12.2.4.9 ITIL METRICS

Metric	For
Key Goal Indicators (KGIs) from the SLA	OM, BU
Terms and conditions of service supply from supplier contracts	OM
User satisfaction metrics from questionnaires or user polling	OM
Service Desk metrics such as the numbers of the different types of user requests and their distribution throughout the working day	OM
Incident Management metrics such as the number and types of incidents, number resolved within Target Resolution Time (TRT), and resolved at the Service Desk	OM
Problem Management metrics such as the number of problems open longer than a set period (e.g., 5 days) and 'stalled' problems (i.e., no further action possible at this time)	OM
Change Management metrics such as the number of changes, the number of emergency changes, and the number of changes that were backed-out	OM
Configuration Management metrics such as the number of changes applied to the CMDB and the average and maximum times between receipt of the RFC and the update being applied to the CMDB	OM
Release Management metrics such as the number and types of releases (Emergency, Major, Minor) and their distribution throughout the year	OM
Process exceptions	OM
Process-specific KPIs	OM
Utilization of resources used for service delivery	OM
Risk management plans and reports produced on schedule and meeting quality criteria	OM, EM
IT Service Continuity Plan tested on schedule	OM, EM
All outstanding issues with IT Service Continuity and Security Management corrected within a defined period	OM, EM
Service authorization and utilization metrics which accurately capture the number of users, and ideally, user identities as well	BU
How quickly accurate IT projects can be designed in response to new requirements and the cost estimates produced	EM
Project completion on time and within budget	EM
How quickly service levels can be changed and stabilized at new levels	EM
How frequently IT proposes new or enhanced business processes	EM
Metrics for the effectiveness of IT controls	EM
Metrics that record compliance with IT policies and standards	EM
Spending on IT service delivery, mitigation of risks, and projects to support changes in business processes, together with the staff time allocated to them	EM
Average and peak capacity utilization as a percentage of that available	EM
Numbers of staff and distribution across job roles or skill levels	EM
Number of training course days received by staff, certifications gained, and staff turnover	EM
Where services have been outsourced, service costs and quality metrics	EM

Key: **OM = IT Operational Management, BU = Business Management & Users, EM = IT Executive Management**

12.3 CHANGE MANAGEMENT PROCESSES

- Opportunity Evaluation – Checkpoint
- Preliminary Analysis

- Request For Change – Build Plan – Checkpoint
- Project Planning
- Request For Change – Implementation Plan – Checkpoint
- Scheduling
- Tracking
- Post Implementation Reporting
- Post Implementation Review – Checkpoint

A general rule of thumb for Change Management, if there are monetary costs or third party support associated with a solution, it should follow the OE, PA, RFC, PIR path for implementation.

12.3.1 Opportunity Evaluation (OE)

The Opportunity Evaluation is used to explore and define the issues, concepts, benefits and costs associated with implementing a specific change. This phase of development is most often visited when a change is considered major in scope or impact, or may develop into a separate project. Completion of an OE form assists in the definition and construction of a well thought out Project Charter. Not all changes may require an OE.

This is a checkpoint for reviewing the expenditure of time and effort on exploring an idea. If the idea expressed shows potential value and alignment with goals and objectives, it may be approved for further research, leading to a preliminary analysis.

12.3.2 Preliminary Analysis (PA)

The Preliminary Analysis takes input from the OE, and looks for alternative solutions to a problem or issue. This gives the Executive a menu of solutions to choose from, ranking the pros, cons, risks and benefits of each solution. It also expands on costs, and introduces third party support to the mix.

12.3.3 Request For Change – Build Plan

This is the entry point into the Change Management process for most requests. At this stage, an issue or problem has been identified, and a minimal request is built to plan the implementation of a workaround or solution. The RFC should contain enough information to make a decision as to the expenditure of resources (time, staff) to planning its resolution.

Critical information would include the issue and concept, benefits, urgency, impact and risk. Once approved, the Change Owner is expected to develop the implementation plans, back-out plans, communication plans, and provide supporting information that provide the details of the next phase.

- If the RFC is inaccurate, unclear, or improperly supported, it may be rejected on merit of detail or completeness.
- If the benefits presented are not viewed as substantial it may be dismissed on technical or strategic merit.
- If the change is prohibitively expensive, will cause unacceptable downtime, will take up too much time or resources, it may be rejected on financial or resource merit.
- If the change request does not outline potential alternative options, or show reasonable research efforts, it may be rejected on technical or tactical merit.
- If the change does not fit with tactical or strategic goals, management or mission objectives, established plans of the organization or the IT department, it may be rejected on strategic merit.

This is a checkpoint for strategic, tactical and operational alignment. If the concept and solution are feasible, cost effective, and aligned with goals and objectives, it may be approved for further planning.

12.3.3.1 PROJECT PLANNING

With the RFC approved to build, the Change Owner and planning team should begin to build the implementation plans and supporting documentation. The deliverables for this phase include:

- Detailed project plan.
- Detailed back-out plan.
- Required resources lists.
- Estimated costs.
- Initial deployment schedule (schedule review time into the plan!)
- List of items that will be affected.
- Communication plans.
- Logistical items (food, lodging, travel, etc.)
- Stakeholder approvals.
- Emergency contacts.
- Checklists for testing of services and verification of function.

12.3.4 Request For Change – Implementation Plan

This is the final official stage of approval before a documented request for change is implemented into production. An RFC that is submitted for implementation approval is expected to have been given due diligence from the Change Owner, ensuring that the change as outlined is complete, planned correctly, and that all possible risks have been mitigated.

- If the RFC is incomplete, inaccurate, unclear or improperly planned, it can be rejected on merit of detail or completeness.
- If the solution presented is not viewed as the best solution, or increases risk to other systems, it can be dismissed on technical merit.
- If the change request does not document the exploration of alternative options, or shows inadequate planning, it can be rejected on tactical merit.
- If the change does not fit with the tactical or strategic goals, objectives or plans of the organization or IT department, it may be rejected on strategic merit.

12.3.4.1 SCHEDULING

The RFC will contain a requested deployment time and date. These are REQUESTED times, and should not be considered the final times and dates until the RFC is approved for deployment. The Change Manager and Coordinator should review the calendar to ensure that other changes or operational items will not conflict with the execution of the change. Alternative dates should be supplied or requested in the event of conflict. Watch out for paydays, month-end commitments, quarterly run dates, project impacts, etc.

12.3.4.2 TRACKING

As changes are submitted, rejected, revised, approved, and implemented, they need to be tracked. The Change Coordinator and Change Manager should keep track of

all active RFC's, and request updates on all RFC's that have passed their approved implementation dates.

12.3.4.3 METRICS

Based on the tracking of RFC's, various metrics should be collected to gauge the success of the process, areas for improvement, trends, downtime and overall effectiveness. These metrics should include:

- Total RFC's submitted
- Total RFC's executed
- Total RFC's by month
- Total RFC's by type
- Total RFC's by owner
- Total RFC's successfully implemented
- Total RFC's unsuccessfully implemented
- Unauthorized Changes

12.3.5 Post Implementation Reporting

As RFC's are implemented, rolled back, failed or cancelled, the Change Coordinator and Change Manager should be advised. This is a critical component of the Change Management process and should not be ignored.

12.3.5.1 POST IMPLEMENTATION REVIEW

All RFC's may be reviewed post implementation, including those that are implemented successfully, that are implemented with unforeseen issues, or fail to implement as planned. RFC's that fail or succeed with deviations from plan must undergo a Post Implementation Review in order to gain lessons learned and formulate a new strategy for dealing with the original issue. This is a critical component of the Continuous Improvement process and should not be ignored.

12.3.6 Unauthorized Changes

Any changes that are introduced to the environment outside of the Change Management process should be considered and investigated as Security Incidents. Changes to system configurations are a key indicator of compromise, and could have unforeseen and potentially dire consequences. Systems should be audited for unauthorized changes periodically.

12.4 RFC WORKFLOW

The Request For Change development workflow has been broken down into 3 stages, and this is reflected in the layout of the Request For Change form. The phases are:

- **READY -** Needs are determined and defined. The issue or problem rather than the solution is the focus. Once the 3 major areas of the RFC are complete, the initial review and approval process is invoked to gain authorization to build the plan.
- **SET -** Research is performed to find solutions to the problems or issues identified in the ready phase. The change request is fleshed out in more detail. Project, back-out, and communication plans are created. The final proposal is passed again through the approval process to gain authorization to implement the solution.

- **GO –** The solution is implemented, monitored, and reported. Implementation review and metrics are gathered, lessons learned are recorded, and improvement plans are generated.

12.4.1 READY PHASE

12.4.1.1 DETERMINE THE NEED FOR A CHANGE

The need to implement a change can be generated from a number of sources including Legislation, Policy Change, Business Changes, Problem Correction, Performance/Capacity Requirements, and Infrastructure Changes etc. In each case the need for change must include all relevant information about the need including, the desired outcome, the justification, and any specific prerequisites or requirements.

The need for change can come from any group or person (the Submitter) but will generally come from:

- Users as the result of a new business need, legislative changes or policy change.
- Service Desk as a result of trouble tickets.
- Problem Management as the result of a problem where a Root Cause has been determined.
- IT Operations and 3rd Party Service Providers as a result of the need to upgrade or add hardware or software.

It should also be noted that certain items do not fall into an official Change for Request. See Exceptions.

12.4.1.2 EMERGENCY ENTERPRISE OR STANDARD CHANGE

All Requests for Change fall into three types:

1. Standard - A standard Change is defined as "an accepted solution to a common set of requirements". This would include Changes that are commonly recurring.

   Within the Standard Change type there are two sub-categories:

   - Major, which requires CAB approval.
   - Minor, for which the Change Manager has authority to approve.

2. Enterprise - An Enterprise Change is defined as being "significant". These Changes are large-scale projects that require the approval of senior business managers and the Executive.

3. Emergency - Situations where an existing service is down or will be before the next CAB meeting or when there is a high risk due to tight timelines, where no workaround exists or where a manager has a client requirement that can not be met before the next regular CAB meeting.

If the Submitter feels that the Change meets the criteria of the Emergency Change Process, the Submitter must immediately inform the Change Manager and Change Coordinator of this fact. If the Change Manager agrees, (or the Change Co-ordinator in the Change Manager's absence) the Emergency Change Process will be used for the Change.

12.4.1.3 COMPLETE "READY" SECTION OF RFC (SECTIONS 1, 2, 3)

When it has been determined that a change is required the Submitter must immediately create a Request For Change (RFC). The Submitter must complete sections 1, 2, and 3 of the Request for Change form. An explanation of the fields in each section follows below. For a copy of the current Request for Change form please contact the Change Coordinator.

Note: It is very important to use non-technical terms where possible for all descriptive text. Representatives of various groups will read the information in the course of their review and approval activities.

Failure to provide complete and understandable explanations will result in delays at each step along the way.

12.4.1.4 1.0 CHANGE SUMMARY INFORMATION

12.4.1.4.1 RFC

The RFC number is supplied by the Change Coordinator or by the CMDB, to easily identify a Request For Change and minimize confusion. The format of the RFC number is typically yyyymm-number or a unique number keyed to the CMDB record.

12.4.1.4.2 STATUS

The current status of the Change as updated by the Change Coordinator. Approved Status codes are defined in Appendix E

12.4.1.4.3 CHANGE TITLE

An intutitive, non-technical description (40 to 50 characters) of the Change.

12.4.1.4.4 PROJECT TITLE

If this change is related to a larger project indicate the name of that project here.

12.4.1.4.5 SUBMITTED BY

The contact that makes the request, which may be a business or information technology person. The Submitter will be involved with the Change throughout its life cycle.

12.4.1.4.6 DATE SUBMITTED

Date and time the Request for Change was received or created. The information is supplied by the Change Co-ordinator or the CMDB.

12.4.1.4.7 CHANGE OWNER

The Owner will generally be a Manager within the IT group. The Owner will be involved with the Change throughout its life cycle.

12.4.1.4.8 RELATED RFC'S

If this Change is related to another Change Request, indicate this here. Any Dependencies between RFC (i.e. Successful implementation of one RFC may be a prerequisite input to a subsequent RFC) should also be noted.

12.4.1.4.9 TYPE

Indicate the general type of change requested:

- Minor - A minor change is defined as "an accepted solution to a common set of requirements" that is minor in scope, and will incurr minimal (one hour or less) downtime. Minor changes should not alter the environment significantly. This would include changes that are commonly recurring such as periodic required maintenance for which the CAB can delegate authority to one of its members to approve.
- Major - A major change is defined as "an accepted solution to a common set of requirements" that is major in scope. This would include changes that are commonly recurring such as periodic required maintenance but could incurr downtime (one hour or greater) which requires CAB review and approval.
- Enterprise - An Enterprise Change is defined as being "significant". These Changes are large-scale projects that require the approval of senior business managers. For more details please see the document "System/Service Development Life Cycle Framework".
- Emergency - Situations where an existing service is down or will be before the next CAB meeting, or when there is a high risk due to tight timelines, where no workaround exists or where a client requirement can not be met before the next regular CAB meeting.

This field denotes the type of change being REQUESTED, and is subject to evaluation and change by the Change Manager, or members of CAB.

12.4.1.4.10 DEPLOYMENT DATE/TIME

Date and time for when the person or group responsible for this request wish to start working on it. If a specific date and hour cannot be determined initially, estimate when the change must be made available in production. Though a specific date is desirable, it is acceptable to indicate a time period (e.g. Aug 2003) or an event (e.g. before Year-End Processing). Prior to approval for Deployment, a specific time and date must be established.

Referencing the current change schedule can assist in the determination of this date. ASAP (As Soon As Possible) or TBD (To Be Determined) are not dates and will considered cause to reject an RFC.

12.4.1.4.11 ESTIMATED DURATION

Best estimate of the time needed to complete the change. This should include an allowance to back-out the change in the event of failure.

12.4.1.4.12 URGENCY

The change priority is based on the Submitters perception of the importance of the change and will be:

- High Priority - the Change Requirement is critical to meet business objectives.
- Medium Priority- the Change Requirement is important to the business but not critical to meet the business objectives. Typically these changes relate to productivity and efficiency or minor issues around customer satisfaction.
- Low Priority- these requirements are not essential and may not be assigned or acted upon unless the resources become available, or the request is combined with other changes to the same component.

The nature of the change and the timeliness will determine the Change Category. The Categories are Major, Minor, Emergency, and Enterprise changes.

Note: The CAB reserves the right to alter the specified Category, the Change Manager may re-categorize or return an RFC if he/she disagrees with the category selection.

12.4.1.4.13 IMPACT

(High/Medium/Low) To the best extent possible the Submitter should indicate the Resource Impact of the proposed change and should cover People, Related Applications or Equipment. It is also important that these impacts are very clearly and comprehensively described so that anyone can evaluate and understand them. For example should the change be implemented in all or specific environments.

Note: A full impact analysis done later in the process can confirm any impacts or additional change requirements to other systems, applications, and infrastructure components.

12.4.1.4.14 RISK

Indicate the degree of risk the change will cause to the stability of the IT Infrastructure by choosing Low, Medium, High or Unknown.

12.4.1.5 2.0 Purpose of the Change Request

12.4.1.5.1 Describe the Issue/Concept

Why is a change required? The explanation should demonstrate a clear link to business impact. What is the impact if the change is not made? Scope and design of the change, as much detail as possible should be included here, and specifics of what is actually changing.
Note: Justification information for the change request should be defined in detail and where possible reference impacts of not making the change in quantitative terms (e.g. hours of effort to be saved, number of customer complaints, etc).

12.4.1.5.2 Incident References

Indicate any Incident records that are related to this Change.

12.4.1.5.3 Problem References

Indicate any Problem records that are related to this Change.

12.4.1.5.4 OE/PA References

Indicate any related OE/PA numbers.

12.4.1.6 3.0 Alternative Solutions and Recommendation

12.4.1.6.1 Describe the Alternative Solutions Available

Indicate the alternatives or options you feel are available to accomplish the Change. Include any issues or significant Benefits/Impacts to the Clients and IT

12.4.1.6.2 Recommended Solution and Justification

Of the above alternatives or options, which one do you recommend be used for this Change and why do you so choose. Clearly state the key reasons that influenced your decision.

12.4.1.6.3 Benefits & Impact to the Business

Indicate how this change will affect the Firm on a business level. For instance, will this Change help users perform their jobs more efficiently, if so how? Will this Change save the Firm money, if so how? Will this Change alter the way the Firm or users work, if so how?

12.4.1.6.4 Benefits & Impact to IT

Indicate how this change will affect the IT Team. For instance, will this change help the IT Team perform their jobs more efficiently, if so how? Will this change save the IT Team money, if so how? At this point the Change Submitter submits the Change Request to the Change Coordinator.

Note: RFC's submitted after the 'Change Cut-off' time may be reviewed by the Change Coordinator, but they will not generally be submitted for review at the next CAB meeting.

Again, it is critical that as much information about the nature of the change be made available in plain language. Questions raised in the minds of the

reviewers that are not properly addressed in the request may result in approval delays.

Potential Categories of Benefits

Acceptability — Does the solution meet the needs of the primary users? Does the solution contribute to the operation or improve quality of information for decision-makers?

Accuracy — Does the solution decrease error rates or improve the correctness of information? To what extent does it do either of these?

Adaptability — Does the solution's software allow differing system constraints and user needs to be satisfied? Can the solution's hardware be used for other tasks for which the organization is responsible?

Availability — What is the probability that the software and/or hardware of the solution will be able to perform its designated system functions when required? How long will it take for the solution's software and/or hardware to be implemented and does that date satisfy documented user requirements?

Compatibility — How will existing operations, facilities, equipment, and data requirements be affected by the solution? How much initial training will be required? How will work methods/procedures have to be altered?

Efficiency — Will the solution's software perform its intended mission/functions with a minimum consumption of computing resources? How quickly will it process the data or calculations? Is it fast enough to satisfy documented requirements?

Maintainability — How much will the solution's implementation increase the maintainability of a functional unit? Does this level of maintainability satisfy documented requirements?

Manageability — How will the solution impact the involvement/need for supervisors or quality inspections? Will the solution require a different type of worker than currently used? Are trained workers available? If not, are they readily trainable?

Morale — How will the solution contribute to a positive employee work attitude?

Performance — How will the solution's computer system and/or its subsystems perform their required functions (e.g., with adequate throughput, response times, and/or number of transactions)?

Portability — How easily can the software of the solution be transferred from one computer system or environment to another?

Productivity — How will the rate of production (e.g., number per hour, etc.) increase if the solution is selected? Will the solution decrease the number of staff resources previously needed to produce the same product, or will the solution allow more items to be produced with existing staff resources? Does the rate of productivity satisfy the documented requirement?

Quality — Will a better product be produced by the solution? Will better service be provided? Will the quality of products be more consistent?

Reliability — For software: Will the solution's software be able to perform its required functions under stated conditions for a stated period? For hardware: Is the solution's hardware projected failure rate (meantime between failure/service calls per year) acceptable (i.e., does it meet the requirements of the project)?

Residual Value — Will the hardware and/or software have a value when it is no longer needed for the project?

Safety — Will the software and/or hardware of the solution alternative promote safety in the workplace?

Security — How will the solution's system (hardware and/or software) decrease the chance of fraud, misuse of resources, theft, etc.? Will the system result in fewer precautions being needed? If so, what are they? If the system must handle classified/sensitive unclassified data, is there a solution alternative which provides better security at a "better" cost?

Service Life — Will the solution's hardware and/or software be able to support the stated requirements for the projects estimated system life? Does the solution have a service life that will eliminate the need for replacement hardware and/or software during the estimated system life of the project?

Software Quality — Will the composite characteristics of the solution's software to be used meet the needs/expectations of the primary users?

Upgradability — Will the solution's software be usable on newer or larger hardware platform?

Versatility — Will the solution's software or hardware provide additional capacity/capability beyond that required for the system? If so, is it needed and/or is there an additional cost for the additional capacity/capability not needed by the project?

12.4.1.7 REVIEW FOR COMPLETENESS (SECTION 1, 2, 3)

Once the RFC has been submitted, the Change Coordinator will review it for completeness, clarity and accuracy. Requests that do not pass this review will be returned to the Submitter to address the identified issues.

Generally, the Change Coordinator will review the RFC from the perspective of the various CAB members, especially when examining the purpose of the proposed change. When reviewing for completeness, the CAB will be looking to ensure all required information is included. When reviewing for accuracy, the Change Coordinator will pay particular attention to the Type (Minor, Major, Enterprise, Emergency), Urgency and Risk.

Those RFC's that meet the qualifications of 'minor' can be forwarded for approval by the Change Manager and will bypass the requirement for initial CAB approval requirements. Once the Change Manager has reviewed and approved the minor

change, the Coordinator will be advised in writing, and will advise the submitter, update the change calendar and add the approval to the CAB meeting agenda.

All other Change Requests submitted before the cutoff time will be added to the CAB agenda for review.

12.4.1.7.1 Log and Add to CAB Agenda

If the Request for Change is accepted, the Change Coordinator will log the Request for Change and add it to the next CAB meeting agenda. If the Request for Change is not accepted, the Change Coordinator will return the Request for Change to the Submitter.

12.4.1.7.2 CAB Validation of Concept and Proposed Solution

The Change Advisory Board (CAB) will review all submitted RFC's and meet on a weekly basis to discuss and approve or defer them. The CAB will review them for their importance, impact, technical soundness, and degree of effort.

All CAB Members have the opportunity to raise and communicate any issues and concerns, which then need to be resolved. Experienced CAB Members can identify additional impacts, risks or oversights affecting the systems that they or other groups are responsible for.

An RFC with insufficient data to make an informed decision will be deferred and returned (by the Change Coordinator) to the Submitter.

Note: In some situations the CAB may elect to approve a request conditional upon some action (i.e. add something to the test plan etc.), in which case the Change Coordinator will return the request and indicate the requirement. When the requirement has been met the RFC will be reviewed again, and once approved, the Change Coordinator will mark the request approved and notify the submitter.

Upon approval the RFC they will also be assigned a Priority and Service Provider. The designated Service Provider will use the assigned 'Priority' when scheduling resources.

It is the responsibility of the various Service Providers to manage their workload and work practices.

12.4.1.8 4.0 CAB Approval to Build

Upon the CABs approval to Build, the Change Manager will sign and date the Change Request before passing on requests for major changes to the IT Executive for review and approval.

12.4.1.8.1 IT Executive Validation of Concept and Proposed Solution

If the CAB accepts the Change it will be passed on to the IT Executive for review. If the IT Executive does not approve the Change, the Change Request will be returned to the submitter by the Change Coordinator.

The Change Coordinator, Change Manager, CAB or the Executive will notify the submitter of any request that has not been approved. When possible the submitter will be informed of the areas or issues of concern. The submitter

can update the RFC with information that will address the issues raised and re-submit the RFC.

12.4.1.8.2 EXECUTIVE APPROVAL TO BUILD

Upon the IT Executives approval to Build, the Executive Approver will sign and date the Change Request. The IT Executive will then return the Change Request to the Change Co-ordinator who will in turn pass it on to the Deployment Team to build and test the Change.

12.4.2 SET PHASE

12.4.2.1 UPDATE STATUS AND CALENDAR

Once the CAB and the IT Executive have initially approved a Change, the Change Coordinator will update the status of the Change Request and the Change calendar to reflect the current status of the Change.

12.4.2.2 BUILD AND TEST, UPDATE RFC SECTIONS 4, 5, 6

The Change Coordinator will forward the Change Request to the specified Service Provider of the Change for further planning. The Service Provider will complete sections 4, 5, and 6 of the Request for Change Form.

12.4.2.3 5.0 IMPLEMENTATION STRATEGY

12.4.2.3.1 HIGH LEVEL DESCRIPTION

Scope and design of the change, as much detail as possible should be included here, and specifics of what is actually changing. The Service Provider will build the change and test it as agreed at the time of CAB approval.

CAB approval does not absolve the Submitter of involvement with the change, they should be available to the Service Provider to work on or develop the change.

12.4.2.3.2 DETAILED TASK LIST

Provide a detailed, itemized list of the tasks (project plan) that need to be performed for this change, including:

- A work effort estimate.
- Recommendations for testing.

12.4.2.3.3 LIST CONFIGURATION ITEMS AFFECTED

After some work on the Change Request, information will become available regarding the detailed functional and technical requirements of the change as well as the impact, systems, components and documentation affected.

Note: The Service Provider must keep the RFC they are responsible for up-to-date, since it is used to track progress and determine if the nature or scope of the change has altered.

The Service Provider will use the applicable design methodologies and project management processes depending on the magnitude and nature of the change.

Detailed Requirements that should be added to the RFC include:

- **Functional Requirements:** Detailed functional specification of what the system or object is required to do, or respond to.
- **Performance Requirements:** A measurable quantity that will serve as basis for verifying if the change complies with the required performance for operations (e.g. response time in seconds given a certain load, or the before and after characteristics).
- **Capacity and Volume Requirements:** A measurable quantity that will represent the load requirements (e.g. number of transactions per

second or hour, number of concurrent users, volume of allocated memory, disk space, etc.)

- **Availability and Service Requirements:** How does the change affect, improve or need to maintain the serviceability requirements (e.g. for backup or purging logs and files, disaster recovery, skills required for internal staff, documentation required, 7 by 24 availability, etc.)?
- **System Components** that will be affected by the change: Modules, business processes, critical service deliverables, operation processes.
- **Hardware and Software** that will be modified by the change.
- **Service Level Agreements:** Determine the impact the change might have on current service agreements.
- **DRP Impact of this change:** If new files are being created, sizes changed, steps added, retentions altered etc. What steps have been taken to notify the Disaster Recovery Manager and update the Disaster Recovery plans?
- **Documentation Impact:** covers the impact if any on production documentation. Has the issue been addressed? Has the documentation been updated? Will it be supplied to Documentation control before Deployment?
- **Incident Resolutions:** Are any currently unresolved Incident Resolutions resolved as a result of this change?

This view of the requirements will further assist in the development of testing and acceptance criteria, end-user and support staff training needs, and modification of service levels.

Note: Use attachments to include the detailed requirements and specifications. You can attach the documents that you normally require to do the change building and testing and note their attachment within the RFC.

The summary results of any testing should be included in the RFC since it represents a key review and approval factor. Changes that are intended to improve performance must show the before and after metrics. Failure to provide sufficient detail in a readable format may delay approval.

If the testing indicates an unexpected impact on performance (i.e. elapsed time increase, high CPU usage etc.) the results must be clearly stated here.

12.4.2.4 6.0 LOGISTICAL REVIEW

The purpose is to ensure that all change deployment tasks and resources, task dependencies and impacts to resources and services, are defined, planned, communicated and understood.

The Service Provider needs to consider the following:

12.4.2.4.1 IMPLEMENTATION PLAN

A detailed plan for how the change will be implemented. The level and extent of plan is defined by the process involved and is based on the size and complexity of the change and criticality of the components being altered. This plan should take into consideration any conflicts and limitations based on the combined task schedule for the group including other changes.

Care should be taken to coordinate the Communications Plan with the Implementation Plan.

12.4.2.4.2 TEST PLAN

The test plan in the RFC must be of sufficient detail to allow the reviewers (CAB) to determine if the testing was adequate. The level and extent of testing is defined by the process involved and is based on the size and complexity of the change and criticality of the components being altered.

12.4.2.4.3 BACK OUT PLAN

A detailed plan in the event that the Change is not successful. How will you return to the pre-Change environment or an environment that will assure the functionality of the service in question.

12.4.2.4.4 USER INVOLVEMENT

Will general users be required to do something because of the Change? For instance, reboot, change passwords, update distribution lists, etc.

12.4.2.4.5 COMMUNICATION

(Users, Management, Help Desk) - All communication and training requirements need to be properly specified, indicating content, audience, timelines and responsible parties, including bulletins to business, Help Desk, etc. Any target audiences named in this box must be addressed in the detailed deployment plan, and the communication plan.

12.4.2.4.6 SECURITY

Will the Change have any impact on security issues? Readiness, special procedures, backup procedures, availability of fallback procedures and fallback criteria should be detailed.

12.4.2.4.7 RESOURCES

(Skills, Availability) - Resources include people, hardware, software, maintenance windows, and data. Need to consider availability, communication, coordination responsibilities, knowledge and skills, and security.

12.4.2.4.8 ENVIRONMENT

(Heat, Fire, Power, Access, Space) - Have you determined that the environment is capable of the Change? Is there room in the server room, will the UPS handle the added load, is wiring required, are there safety precautions to take, do you have physical access to the area where the Change will occur?

12.4.2.4.9 TECHNICAL DOCUMENTATION

(Physical/Logical Architecture) - Has the new environment created by the change been documented in detail including written descriptions and drawings as required? Updating of existing responsibilities for procedures and documentation for support, operations, disaster recovery, architecture, training procedures, etc.

12.4.2.4.10 WRITTEN SUPPORT PROCEDURES

The change may impact established Incident Workarounds, how are they to be addressed?

12.4.2.4.11 COST ESTIMATES

This should include cost of hardware, software, personnel, outside contractors, etc. if needed.

12.4.2.5 7.0 IMPACTS AND RISKS

The purpose of impact analysis is to ensure that all the impacts of a change are identified and an approach for addressing each one of them is defined. The Service Provider performs or manages the execution of the impact analysis of change.

The Service Provider uses the Impact Analysis Checklist to list and describe all potential change impacts, as well as whom is to address them in what stage of the change or project cycle. The Impact Analysis indicates which systems and components will be affected and how. Also indicated are the groups who were contacted or who participated in the impact analysis. The Impact Analysis Checklist should be located at the end of the RFC Template.

Note: When conducting the Impact Analysis: Contact as many people as needed. Use application and infrastructure architecture diagrams where they exist

12.4.2.5.1 POTENTIAL IMPACT AREAS

Check off any of the listed Potential Impact Areas you feel apply to the Change.

12.4.2.5.2 MITIGATING ACTION

Provide a detailed explanation of what will be done to mitigate the potential Impact.

12.4.2.6 8.0 COMMUNICATIONS PLAN:

The standard communication template (Contained in the RFC form) must be completed for each change.

In addition, use the Communication Checklist to develop further communication agents for complex, major or project based changes.

12.4.2.7 COMPLETENESS CHECK

Once the development and testing associated with an RFC have been completed the RFC is submitted and reviewed for Deployment. The Change Coordinator will review the RFC for completeness and accuracy. Requests that do not pass the review will be returned to the Submitter (see Build and Test, Update RFC Sections 4, 5, 6) to address the identified issues.

When reviewing for completeness the Change Coordinator will be looking to ensure all required information (see Build and Test, Update RFC Sections 4, 5, 6) is supplied including Detailed Test Plans, Test Results, Implementation, Validation and Back-out Plans.

12.4.2.7.1 CAB APPROVAL OF BUILD, TEST, DEPLOYMENT PLAN

After reviewing initial RFC's, the CAB will turn to RFC's that are seeking approval to Deploy. The CAB will review the RFC in its entirety preferably prior to the meeting, including the original requirements and expected results.

The CAB will pay particular attention to the Test Plan and Test Results looking to ensure that testing has been sufficiently stringent to meet the Risk Level. The Implementation and Back-out Plans will also be closely reviewed. The Change Manager will inform the CAB of any Minor Changes they have approved for deployment.

Note: A Back-out Plan that consists of 'page me' will generally not be acceptable.

An RFC with insufficient data to make an informed decision will be deferred and returned (by the Change Coordinator) to the Service Provider (see Build and Test, Update RFC Sections 4, 5, 6).

The CAB will also review the change in detail and confirm it's dependencies and restrictions along with other Changes available for deployment (from the maintained Change Schedule) to determine when the change can be implemented.

Note: In some situations the CAB may elect to Approve a request conditional upon some action (add something to the test plan etc.), in which case the Change Coordinator will return the request and indicate the requirement.

When the requirement has been met the Change Coordinator will mark the request approved and notify the CAB.

12.4.2.8 9.0 CAB APPROVAL TO DEPLOY

Upon the CABs approval of the Change to Deploy, the Change Coordinator will sign and date the Change Request before passing it on for IT Executive approval.

12.4.2.8.1 EXECUTIVE REVIEW OF BUILD, TEST, DEPLOYMENT PLAN

The Change Coordinator will pass all CAB approved RFC's to the IT Executive for approval.

The Service Provider and the Submitter will be notified of any request that has not been passed by the Change Coordinator or not approved by the CAB. When possible they will be informed of the areas or issues of concern. The Service Provider is required to update the RFC with information that will address the issues raised and re-submit the RFC (see Build and Test, Update RFC Sections 4, 5, 6).

12.4.2.8.2 EXECUTIVE APPROVAL TO DEPLOY

Upon the IT Executives approval of the Change to Deploy, the Executive Approver will sign and date the Change Request before passing it on for IT Executive approval. The IT Executive will then return the Change Request to the Change Coordinator who will in turn pass it on to the Deployment Team to implement the Change.

12.4.3 GO PHASE

12.4.3.1 UPDATE STATUS AND CALENDAR

Once the CAB and the IT Executive have approved a Change, the Change Coordinator will update the status of the Change Request and the Change calendar to reflect the current status of the Change.

12.4.3.2 IMPLEMENT THE CHANGE PER PLAN

Those involved in the implementation of the Change are expected to update the RFC with the status of the implementation. Operations will validate successful implementation. Validation involves checking to see if the Change has been successfully introduced into production. For example, the provision of a list indicating the name of the item being changed, version numbers and compile date (if a program) is sufficient for validating the Change.

Implementation Status:

- Implemented – the implementation was completed without incident.
- Implemented with issues – the implementation was completed but problems were encountered that were addressed without back-out.
- Implementation failure – the implementation failed and/or back out is required.

Note: Operations in this instance refers to the Network group, person or function responsible for the installation.

12.4.3.3 10 DEPLOYMENT SUCCESS/FAILURE

12.4.3.3.1 WAS THE CHANGE SUCCESSFULLY DEPLOYED?

If yes please indicate so. If no, please indicate with a brief explanation of the reason the deployment did not succeed.

12.4.3.3.2 WHAT WAS LEARNED?

If there were any learning outcomes throughout the processes, they should be recorded and shared. Include ALL lessons learned, including:

- Planning aids.
- People that can expedite solutions.
- New or improvements to existing processes.
- New or improvements to existing procedures.
- Layouts, dependencies, workflows, etc.
- Tricks and tips.

12.4.3.4 BACK-OUT CHANGE IF NECESSARY

Operations, with input from the Service Provider and/or the Change Submitter, will make the determination to back-out some or all of a change. The back-out will be performed as defined in the back-out plan.

12.4.4 REVIEW PHASE

12.4.4.1 UPDATE RFC AND REPORT TO CAB

Once a Change has been completed, the Change Coordinator will update the status of the Change Request and the Change calendar to reflect the current status of the

Change. The Change Coordinator will also inform the CAB of the completion of the Change.

12.4.4.2 MONITOR CHANGE

After the completion of a Change, the Operations Team will monitor the effected systems for an appropriate amount of time, being alert to any incidents as a result of the Change. The monitoring time will depend on the system that was changed.

12.4.4.3 POST IMPLEMENTATION REVIEW (PIR)

In the event of a successful implementation and the passage of sufficient time for any associated problems to surface, a PIR may be conducted. In the event of problems being encountered, a PIR must be conducted on a schedule dictated by the severity of the failure. All changes must be monitored for at least one usage cycle of the change to ensure that it functions as desired and does not cause other incidents or issues.

Criteria for Mandatory PIR:

- A material deviation from the deployment plan.
- In the Event the Expected Outcome of the RFC is not Achieved.
- Change Fails to meet User Requirements.
- Change Fails on Implementation.
- Change has unintended impact on other Services/Infrastructure.

A PIR Must address each of the following elements:

- Were the implementation instructions complete and followed?
- Did the change deliver expected results?
- Did the RFC properly reflect the Risk?
- Did the change follow the approved processes?

The Change Coordinator must be informed of any Incidents or Problems associated with the implementation of an RFC. A simple PIR for a successful change can be documented on the RFC form. For a PIR involving an unsuccessful change, the separate PIR form should be used. The major steps in a PIR are as follows:

- Declare intent to complete a full PIR – **CAB responsibility**
- Chair the PIR and Document the Findings – **Change Manager**
- Participate in the PIR – **All IT Staff and vendors** involved in the RFC
- Distribute PIR & Findings - **Change Coordinator**
- Modify processes based on PIR results - **All**

12.4.4.4 UPDATE RFC AND CLOSE

All RFC's deployed will remain open for a least "One Cycle" of the Change. If no incident records are created related to the RFC, it will be closed as 'Successful'. Should an Incident be created the record will remain open until the RFC can be confirmed as the source of the incident at which time it will be closed as 'Failed'.

A Change Request that is Closed, and later found to be the source of incidents/problems will be re-opened and updated to reflect the situation.

12.4.4.5 PUBLISH METRICS AND DISTRIBUTE

On a regular schedule, the Change Coordinator will publish and distribute the accumulated metrics associated with Change Requests. This data can then be used as a point of reference for future Change Requests.

12.4.4.6 IT EXECUTIVE MONTHLY REVIEW MEETING

The IT Executive will meet monthly to review completed Changes and the associated metrics.

12.5 TOOLS

- Opportunity Evaluation Form (Word DOC format)
- Preliminary Analysis Form (Word DOC format)
- Request For Change Form (Word DOC format)
- Standard Impacts Checklist (Word DOC format)
- Communications Plan (Word DOC format)
- Standard Communications Template (Word DOC format)
- Project Planning Software (MS-Project)
- Deployment Plan Template (Project MPP format)
- Tracking and Metrics Spreadsheet (Excel XLS format)
- Change Calendar (MS-Outlook)
- Post Implementation Review Form (Word DOC format)
- Change Manager's Checklist (Word DOC format)
- Change Auditing Tool (Tripwire, BMC Patrol)
- CMDB (Heat, Remedy, Other)

12.5.1 Recommended Technologies

Organizations intending to use the Change Management to effectively manage change in their production environments can use specialized technologies to aid in this process.

- RFCs can be submitted to the change manager using e-mail programs.
- Templates for RFC's can be created in Word, Excel, or on Web forms.
- The calendar function of email clients can also be used to manage changes in each phase of the process, and alerts can be set up for the authorization, development, deployment, and change review processes.
- Drawing and diagramming software such as Visio can be used to detail workflows and plans.
- Asset management tools such as SMS or Altiris can assist the change owner in defining the scope of a change and the affected services.
- SMS and Altiris also provide software distribution mechanisms that can enable automation of deployment. The change manager can also use these tools to report on the progress of a change following release, and in the review process.
- MS-Project is a tool that enables the change owner and manager to manage both simple and complex changes.
- NetMeeting and other online meeting tools allow the CAB to meet virtually in order to approve or reject RFCs.

12.5.2 Change Manager Checklist

Provided here is a quick checklist for a Change or Project Manager to evaluate the effectiveness of the Change Management Process and how to revise the specific plans. The checklist contains items to consider for documenting change requests, handling them within a change process, and ensuring approved changes are included in the project deliverables.

It is important to note that this checklist is provided for a quick review of a single change, and not a detailed audit of the process itself. This is intended as a functional or tactical guide for the Change Manager only. Auditors may use this document, but will want to examine the associated procedures in more detail.

ID	Y/N	Items to consider
1		Has the RFC been completed?
2		Has the change request been prioritized?
3		Has an approach been identified to handle the change?
4		Has a workaround been identified if the change is not implemented?
5		Has an independent reviewer reviewed the change request to determine whether or not it is worth evaluation for action?
6		Has an estimate been developed for effort, cost, schedule, & resource?
7		Have the estimates been authorized by the CAB & Executive?
8		Have the estimates been communicated to the requestor?
9		If the change is denied, has the requester been notified?
		The following steps are to be considered only if authorization was given.
10		Has the change been incorporated into a project work plan?
11		Does the change require additional resources?
12		Does the change impact project schedules?
13		Has the work been performed to address the change?
14		Has the work been reviewed with all effected parties?
15		Has the change been validated to ensure correctness?
16		Have revisions been placed under configuration control?
17		Have the change and configuration records been updated?
18		Has the CAB been notified that the change has been implemented?
19		Have the change records been updated to reflect completion?
20		Has the requestor been informed of the final status?
21		Is a Post Implementation Review required?

12.5.3 Change Coordinator Checklist

Provided here is a quick checklist the Change Coordinator to evaluate the completeness of the Request For Change documentation. The checklist contains items to consider for reviewing change requests, and ensuring that deliverables and impacts are clearly defined.

It is important to note that this checklist is provided for a quick review of a single change, and not a detailed audit of the process itself. This is intended as a functional or tactical guide for the Change Coordinator only. Auditors may use this document, but will want to examine the associated procedures in more detail.

ID	Y/N	Items to consider
1		Does the RFC have any incomplete fields?
2		Has the change request been properly prioritized?
3		Are there other changes scheduled at or close to the selected implementation date?
4		Has a workaround been identified if the change is not approved?
5		Has an estimate been developed for effort, cost, schedule, & resource?
6		Is the implementation plan included?
7		Are the implementation plans clear?
8		Is the communication plan included?
9		Have alternatives been explored?
		The following steps are to be considered only if authorization was given.
10		Has the change been incorporated into a project work plan?
11		Does the change require additional resources?
12		Does the change impact other project schedules?
13		Has the work been reviewed with all effected parties?
14		Has the change been validated to ensure correctness?
15		Have revisions been placed under configuration control?
16		Have the change and configuration records been updated?
17		Has the CAB been notified that the change has been implemented?
18		Have the change records been updated to reflect completion?
19		Has the requestor been informed of the final status?
20		Is a Post Implementation Review required?

12.5.4 Change Control Auditing Tools

In order to measure change within an organization, it is recommended that auditing tools be implemented to:

- Enforce Change Management processes to increase service availability.
- Maximize system availability with rapid change diagnosis & remediation.
- Provide visibility across heterogeneous infrastructures.
- Swiftly identify authorized and unauthorized changes.
- Provide quick remediative rollback authorized & unauthorized changes.
- Focus remediation efforts when a change has undesired effects.
- Enhance security through notification of undesired changes.
- Enable pinpoint accuracy in identifying change when it occurs.
- Provide the means of instilling accountability for change.
- Identify who made a change, what change was made, when a change was made, and how a change was made.
- Verify that authorized changes are made correctly and completely.
- Deliver vital data for creating configuration libraries that enable verifiable system states, improving processes, capturing audit trails, and enabling forensics.
- Demonstrate regulatory compliance by reporting change status and process integrity across the IT infrastructure.

12.5.5 CMDB – Configuration Management DataBase

The CMDB is really a process enabler with huge architectural dimensions. Ideally it is a trusted, multi-dimensional and current view of inventory, configuration, topological, service, organizational, business and policy-related information to support a whole host of management disciplines, from change and configuration, to service assurance, to asset management, etc.

The CMDB does not have to scan the network and auto-update its configuration item content, however this can be a real time saver in larger environments. At a minimum, the CMDB should provide an import/export facility to allow for import of network and asset management tool reports, and output of current status reports.

12.5.6 Opportunity Evaluation Form

The following form has been used successfully at several companies. The OE is intended to clarify the problem, identify the stakeholders, outline the desired success factors, provide a rough estimate of effort, and gain approval to spend time researching solutions.

Opportunity Evaluation (OE) Form

OE #:	
Priority:	
Status:	

1.0 Opportunity Summary:	
1.1 Title:	**(Provide the unique title of the opportunity to be evaluated)**
1.2 Owner/Manager:	**(Who will be responsible for developing this opportunity and plans?)**
1.3 Prime:	**(Who is the principal presenter?)**
1.4 Date Submitted	

2.0 Statement of the Idea
2.1 Describe the Issue/Concept:
2.2 Benefits to IT and the Business?
2.3 What is the Scope of this Idea? (Includes/Excludes)
2.4 Describe the Look of Success for this Idea

3.0 Key Considerations		
3.1 Describe How this Aligns with the Current IT Strategy:		
3.2 What are the Potential Dependencies and Pre-Requisites that could Impact this Idea?		
3.3 Justify the Priority of this Idea		
3.4 What is the Risk of Not Pursuing this Idea?		
3.5 What are the Potential Impacts on the Organization?		
3.6 What Else needs to be Considered if this is Pursued?		
3.7 Actions for Next OE Meeting		
	Assigned to:	
	Assigned to:	

	Assigned to:	
	Assigned to:	
	Assigned to:	

3.8 Required Attendees to Review this OE					
√	**Name**	**Role**	√	**Name**	**Role**

4.0 PA Phase Requirements

4.1 Resource Estimate to Complete PA Phase

FTE Days	
PA Line items	
Special Resources (Detail)	
PA Considerations	

4.2 Date of Initial PA Review Meeting

This OE is due back to the coordinator as a preliminary PA document by:

5.0 Approval to Proceed to PA Phase

Name	Role	Signature	Approval Date

12.5.7 Preliminary Analysis Form

The following form has been used successfully at several companies. It takes its input from the OE form, and is intended to expand the definitions started in the OE, scope the possible solutions, weigh the alternatives, provide a rough estimate of effort cost and resources, provide inputs towards a project plan, and to develop support for the final solution.

Preliminary Analysis (PA) Form

PA #:	
Priority:	
Status:	

1.0 SUMMARY	
1.1 Title:	
1.2 Owner:	
1.3 Driver:	
1.4 Date Submitted:	

2.0 STATEMENT OF THE IDEA (Use OE as baseline)
2.1 Describe the Issue/Concept (from the OE)
2.2 Benefits to IT and the Business – any additions?
2.3 Scope of this Idea (Includes/Excludes) – any refinement?
2.4 Look of Success for this Idea – any refinement?

3.0 OPTIONS
3.1 Potential Alternative Solutions - details overleaf

3.2 Recommended Approach:

3.1 ALTERNATIVE #1:
Approach and Rationale
Pros:
Cons:
Specific Benefits, Impacts, Dependencies etc.
Implementation Approach
Training Requirements (User and IT)
Unknowns

3.1 ALTERNATIVE #2:
Approach and Rationale
Pros:
Cons:
Specific Benefits, Impacts, Dependencies etc.
Implementation Approach
Training Requirements (User and IT)
Unknowns

4.0 DETAIL FOR SELECTED OPTION

4.1 Deliverables
4.2 Project Initiatives
4.3 High Level Project Plan
4.4 Other Dependencies – In/Out
4.5 Costs for Completion
4.6 Quantified Payback (Cost Avoidance, Headcount savings, HW/SW savings, Business benefits)
4.7 Key Success Criteria (What could cause this initiative to fail?)
4.8 Measures of Success
4.9 Any other comments/observations?

5.0 PA REVIEW

5.1 Actions for Next PA Review			
	Assigned to:		
	Assigned to:		
	Assigned to:		
	Assigned to:		
	Assigned to:		

5.2 Estimate to Complete PA Phase	
Original estimate	
Time expended to-date	
Estimate to complete (ETC)	

5.3 Required to Review this PA

√	Name	Role	√	Name	Role

6.0 PA Acceptance

Name	Role	Signature	Approval Date

7.0 Approval to Proceed			
Name	**Role**	**Signature**	**Approval Date**

12.5.8 RFC – Request For Change Form

The following form is an adaptation of a form that I designed and used successfully at several companies. Note that it is broken up into sections. Each section should be complete and accurate, and additional documents should be attached to support the change as required. I have used a spreadsheet rather than a word document so as to aid in reference linking and auto-calculations in certain fields marked in light blue.

REQUEST FOR CHANGE						
DATE					RFC#	
1.0	Change Summary:					
	1.1	Change Title:				
	1.2	Project Title (if any):				
	1.3	Submitted by:		1.4	Change Owner	
	1.5	Date Submitted:		1.6	Related RFC's	
	1.7	Major Stakeholder:		1.8	Stakeholder Signoff:	
	1.9	Submitted For:				
	1.10	Change Type:				
	1.11	Requested Date:		1.12	Approved Date:	
	1.13	Requested Time:		1.14	Approved Time:	
	1.15	Estimated Duration:				
	1.16	Urgency:				
	1.17	Impact:				
	1.18	Risk:				
			Class:	0		

2.0	What is the Purpose of the Change?	
	2.1	Describe the Issue/Concept:
	2.2	Incident References:
	2.3	Problem References:
	2.4	OE/PA/SA References:
3.0	Review of Alternative Solutions and Recommendation	
	3.1	Describe the Alternative Solutions Available:
	A	
	B	
	C	
	3.2	Recommended Solution and Justification:
	3.3	Benefits to the Business:
	3.4	Benefits to IT:

4.0	How will we implement this change?		
4.1	High Level Description:		
4.2	Technical Approvals:		
	Reviewer Requested	Manager's Signature	Approvals
4.3	Required Change Notes:		
	Reviewer	Notes	
4.4	List of Configuration Items:		

5.0	Readiness Checklist		
	5.1	Project Plan Attached?	
	5.2	Test Plan Attached?	
	5.3	Back Out Plan Attached?	
	5.4	Communications Plan?	
	5.5	Security Requirements?	
	5.6	Logistical Requirements:	Travel Food Lodging Staff
	5.7	Cost Estimates	
	5.8	Support Procedures	
	5.9	Technical Documentation	
	5.10	Update Others	
	5.11	Emergency Procedures	
6.0	Impacts & Risks		
	6.1	Potential Impact/Risk:	Mitigating Actions:
	A		
	B		
	C		
	D		
	E		
	F		

7.0	**Communication Planning**	
	7.1	**Draft of PRE-Implementation Communication to Clients:**
	Note: Your Communication should address each of the following topics.	
	What is the Client Win?	How does the Client Prepare?
	What will be Different?	Will there be an Outage? How Long?
	When will it Happen?	Who Do I Call for more Information?
	How will the Client know the Change is Complete/Successful?	

IT is committed to continuous improvement, and in that effort is bringing the benefits of XXXXXXX to the firm.
This will allow you to <FEATURE>.In order to meet this objective, Toronto IT will take action to expedite delivery of this important initiative and to address a number of concerns expressed by you, our client.
The <XXXXX> system will be unavailable on <WEEKDAY> <MONTH DATE, YEAR> from <HH:MM> am/pm to <HH:MM> am/pm.
Should you have questions or require assistance, please call the Service Desk at ext. ????.
Your request will be forwarded to the appropriate resource.

Communication Format:	(Generally e-mail Broadcast)
Sender:	
Date to be Sent:	

	7.2	**Draft of POST-Implementation Communication to Clients:**
	Note: Your Communication should address each of the following topics.	
	What is the status of the change?	What will be Different?
	What is the Client Win?	Who Do I Call for more Information?

IT has completed its implementation of <XXXXXXX> to the firm. This will allow you to <FEATURE>.
You will notice a new icon on your desktop. <EXAMPLE ICON> This is your <XXXXX> application.
Launching it will bring up the <XXXXX> for use.
Should you have questions or require assistance, please call the Service Desk at ext. ????.
Your request will be forwarded to the appropriate resource.

Communication Format:	(Generally e-mail Broadcast)
Sender:	

Date to be Sent:			
8.0	**Service Desk Alert - Change Summary:**		
	8.1	Change Title:	
	8.2	Project Title (if any):	
	8.3	Submitted by:	
	8.4	Change Owner	
	8.5	**Change Type:**	
	8.6	Approved Date:	
	8.7	Approved Time:	
	8.8	Estimated Duration:	
9.0	**What is the Purpose of the Change?**		
	9.1	Purpose:	
	9.2	Incident References:	
	9.3	What clients may experience:	
	9.4	What to tell clients	

10.0	**Approval To Build**		**Signature**	**Date**	**Name**
	10.1	IT Manager – Technical Approval			
	10.2	Change Manager – CAB Approval			
	10.3	Executive Approver – Executive Approval			
	10.4	Approval Notes			
11.0	**Approval To Deploy**		**Signature**	**Date**	**Name**
	11.1	IT Manager – Technical Approval			
	11.2	Change Manager – CAB Approval			
	11.3	Executive Approver – Executive Approval			
	11.4	Approval Notes			
12.0	**Post Implementation Review**				
	12.1	Was the change deployed successfully?			
	12.2	Lessons Learned			

12.5.9 PIR - Post Implementation Review Form

Post Implementation Review (PIR) *v1.0*

Effective <DATE>

RFC:	
Priority:	
Status:	

1.0 Related RFC Information

1.1 Change Title:			
1.2 Project Title (if any):			
1.3 Submitted by:			
1.4 Change Owner:		**1.5 Implementer:**	
1.6 Type:			
1.7 Deployment Date/Time:			

2.0 Participants – Who was involved with Planning/Deploying this Change?

2.1 List Participants:

3.0 Sequence of Events

3.1 Detail the Timeline of Events:

3.2 Where any Significant Other Changes/Activities Occuring in Parallel:

3.3 Impact to the Business Caused by the Failure of this Change:

3.4 Impact to IT:

4.0 Outcomes

4.1 Was the Change Backed Out?

4.2 Was the Plan Followed?

4.4 Were Configuration Items Affected Properly Identified?

5.0 Areas for Improvement

5.1	**Implementation Plan**	
5.2	**Test Plan**	
5.3	**Back out Plan**	
5.4	**User Involvement**	
5.5	**Communication (Users, IS Management Team, Help Desk)**	
5.6	**Security**	
5.7	**Resources (Skills, Availability)**	
5.8	**Environment (Heat, Fire, Power, Access, Space)**	
5.9	**Technical Documentation (Physical/Logical Architecture)**	
5.10	**Written Support Procedures**	
5.11	**Cost Estimates**	
5.12	**Emergency Procedures Updates Completed**	

6.0 Approval of Findings

Name	Role	Signature	Date
	IT Manager Technical Approval		
	Change Manager CAB Approval		
	Executive Approval		

12.5.10 MASTER CHANGE TRACKING FORM

This form is used to track RFC's through the Change Request Lifecycle. It should be used in the absence of a database. The header section (below) defines the appropriate lookup table data and definitions for clarity. A spreadsheet is used, providing lookup tables and drop-down lists to ensure consistency and ease reporting. The portion below is usually hidden from view and referred to as needed only for clarification.

Status	Description: Current Status of an RFC within the Change Process	Approved projects	Approved Owners	Outcome Codes
Reserved	The Change Request is incomplete, but the number has been assigned for Master Scheduling purposes	Desktop	Comms Manager	Cancelled Deployme
Logged	The Change Request has been Accepted and will be Reviewed at the next CAB meeting	Development	Desktop Manager	Successful Deploym
Incomplete	Returned to Originator due to incomplete information	Doc Mgmt	Dev Manager	Pre-deployment Fail
CAB Approved to Build	The Change Request has been Reviewed and Approved by CAB to Build the Change	Accounting Upgrade	Network Manager	Deployed with Incide
Exec Approved to Build	Executive has approved the Request for Change to be Built	Infrastructure	Project Manager	Failed Deployment
Rejected	The Change Request has been Rejected and Returned to the Submitter	Network	Security Manager	Post Deployment Fa
Deferred	Decision have been deferred pending the Inititiator responding to questions from CAB	Operations	ServiceDesk Manager	
CAB Approved to Deploy	The Change (Deployment) Request has been Reviewed and Approved by CAB to Deploy the Change	Security		
Exec Approved to Deploy	Executive has approved the Deployment	Service Enhancement		
Failed	The Change Request was not deployed successfully/immediate testing proved Change did not meet objectives	Network Upgrade		
XFR to OE	This item has been transferred to the SDLC Process as an OE			
Cancelled	This item has been cancelled and cannot be re-initiated without a new RFC			
Closed	The Change Request has been Implemented and a CAB Review completed			

Type	Description: Attributes of the Change that Impact the Approval Process	Approval Requirements
Standard	A regularly recurring type of change with limited impact. Usually a routine or simple task with very limited impact and risk.	Change Manager
Minor	A non-recurring change with limited impact.	Change Manager
Major	A non-recurring change with potentially significant impact. Currently all infrastructure change is considered major	CAB Team
Enterprise	A non-recurring type of change with business cost/impact beyond the scope of CAB to approve	Executive
Emergency	A Major Production Service is down with no workaround, or will be down with no workaround before the next CAB meeting	Change Manager / Executive

This section, directly below the header, is used to input tracking data and to generate reports. Use pivot tables to extract the reports you require. You can link the fields in completed RFC's to automate the update process, saving the need to repetitively type items into this sheet. In this example, procedural formatting is used to highlight change requests that are overdue for updates and do not have a status of "closed". They will appear in red.

RFC Listing

RFC #	Submit	Description	Project	Owner	Type	Status	Request Deploy Date	Request Deploy Time	Next Update Due:	Outcome	Date Closed	Year	Month	12.5.10.1.1	Open RFC Age (Days)	# Days Oper (Clos
1	01-Jan-04	FTP Server Move	Doc Mgmt	Project Manager	Major	Closed	08-Jan-04	9:00:00 AM		Successful Deployment	15-Jan-04	2004	1	Closed	0	14
2	02-Jan-04	TAX-CD Tower Shutdown	Network Upgrade	Network Manager	Major	Deferred	09-Jan-04	10:00:00 AM		Cancelled	12-Jan-04	2004	1	Closed	0	10
3	03-Jan-04	Kayak Print Servers Physical Move	Network	Network Manager	Major	Cancelled	10-Jan-04	11:00:00 AM		Cancelled	14-Jan-04	2004	1	Closed	0	11
4	04-Jan-04	UL/DL Standardization/Optimization	Network Upgrade	Network Manager	Major	Closed	11-Jan-04	2:00:00 PM		Successful Deployment	18-Jan-04	2004	1	Closed	0	14
5	05-Jan-04	PIX Firewall Implementation	Security	Security Manager	Major	Closed	12-Jan-04	10:00:00 PM		Successful Deployment	19-Jan-04	2004	1	Closed	0	14
6	06-Jan-04	Fire Extinguisher & Emergency Flashlight Installation	Security	Security Manager	Major	Cancelled	13-Jan-04	11:00:00 PM		Cancelled	17-Jan-04	2004	1	Closed	0	11
7	**26-Feb-04**	**Archive Data on SAN Disk Array**	**Operations**	**Network Manager**	**Major**	**Exec Approved to Build**	**04-Mar-04**	**2:00:00 PM**				**2004**	**3**	**Open**	**712**	**0**
8	10-Mar-04	SAN disk array maintenance	Operations	Network Manager	Major	Closed	17-Mar-04	2:00:00 PM		Successful Deployment	24-Mar-04	2004	3	Closed	0	14
9	**11-Mar-04**	**Update DNS for www.somesite.com**	**Operations**	**Network Manager**	**Major**	**Exec Approved to Deploy**	**18-Mar-04**	**2:00:00 PM**				**2004**	**3**	**Open**	**698**	**0**
10	**12-Mar-04**	**319th floor Cutover - Miscellaneous Items**	**Network Upgrade**	**Project Manager**	**Major**	**Exec Approved to Deploy**	**19-Mar-04**	**2:00:00 PM**				**2004**	**3**	**Open**	**697**	**0**
11	13-Mar-04	Domain Migration	Network Upgrade	Network Manager	Major	Closed	20-Mar-04	2:00:00 PM		Successful Deployment	27-Mar-04	2004	3	Closed	0	14
12	23-Mar-04	FileShare server restart	Operations	Network Manager	Major	Closed	30-Mar-04	2:00:00 PM		Successful Deployment	06-Apr-04	2004	3	Closed	0	14

In a database environment, report generation is easier and much richer. You can use spreadsheets to get started, but I must restate that a Configuration Management DataBase is a ***requirement*** in a large or busy environment, and highly recommended for all others.

12.6 AUDITING CHANGE MANAGEMENT

12.6.1.1 DESCRIPTION OF THE AUDIT AREA

Change Management is the process by which changes are planned, scheduled, applied, tested, accepted, distributed, and tracked within the production environment.

The process can involve the development, conversion, or modification of new or existing systems or code. Change activities can impact a unit's ability to provide critical data processing and information delivery services to an organization and can interrupt the organization's ability to do business.

It is necessary that each change be controlled throughout its life cycle, from discovery, development, authorization and implementation, and integrated into the production environment in a systematic and controlled manner.

The primary objective of Change Management is to maintain the integrity and reliability of the production environment, while introducing approved changes.

12.6.1.2 AUDIT OBJECTIVES

Address all activities that will result in changes to the production environment, regardless of the source of the change. Activities include application and system development and modification, telecommunications, network system including changes to option settings on servers, line equipment including but not limited to changes in options, additions, and vendor supplied software modifications and upgrades.

The following are minimum procedures that can be used to satisfy the attainment of the audit objectives. The bold-type procedures represent core issues that should be included in audit coverage of the Change Management area in every risk cycle. The subsequent indented procedures are suggested steps that may be taken in order to meet the criteria established in the core issues. Additional procedures may be added to this program as necessary. Procedures to review controls are not included in this program.

12.6.1.3 AUDIT SCOPE

The scope of the Change Management Audit includes:

1. Review of documentation, policies and procedures regarding the change management process.
2. Evaluation of the Change Management Process, including change initiation, development, modification of applications and systems, testing, Quality Assurance, migration to production, back-up and recovery.
3. Information security access restrictions to staging, testing, Quality Assurance, and production libraries.

12.6.1.4 PRELIMINARY DELIVERABLES

A. Audit Checklist
B. Organization Chart
C. Process flowcharts and system narratives.
D. Naming conventions in use for systems and directory structures.
E. Naming conventions for system software, executable, parameter and command language libraries and directories.
F. A report listing the total number of changes during time period under review:
    1. Application: emergency & non-emergency
    2. Non-application: emergency & non-emergency.
G. Samples of all change management logs and forms.
H. Current vendor documentation for any system or software item in use.

12.6.1.5 Sample Audit Checklists

12.6.1.5.1 Individual Change Request Audit Checklist

ITEM	Y/N	DESCRIPTION
1		Has a change request been filed by a member of IT, a project team, or by a stakeholder?
2		Have stakeholders been identified?
3		Have stakeholders signed off on the need, the plan and any outages?
4		Has the change request been fully documented?
5		Has the change request been prioritized?
6		Has an approach been identified to handle the change?
7		Has a workaround been identified if the change is not implemented?
8		Has an independent team or member (not the originator) reviewed the change request?
9		Has an estimate been developed of effort, cost, schedule, and resources been determined?
10		Have the estimates been evaluated and authorized by a Change Advisory Board or other authority?
11		Have the results of the above evaluation been communicated to the requestor?
12		If the change is denied, has the requester been notified?
13		Has the work been performed to address the change?
14		Has the work been reviewed with all effected parties?
15		Have the associated verification activities been performed to ensure correctness?
16		Have revisions been placed under configuration control?
17		Have the change request records been updated to document the changes made?
18		Has the Change Advisory Board been notified that the change has been completed?
19		Have the change request records been updated to reflect completion status?

12.6.1.5.2 COMMUNICATION PLANNING CHECKLIST

Y/N	Due Date	Deliverables/Tollgates	Comments/Relevant Filenames
		Have you prepared an elevator speech?	A quick 2 minute summary of the change and its benefits.
		Do you understand how the overall objectives tie into the project?	Prepare communication explaining the linkages.
		Have you prepared a communication regarding previous activities and how they relate to this initiative?	This helps the end user understand how this change relates to other initiatives
		Have you verified whether external players or systems need to be addressed as part of the strategy?	If yes, prepare communication and mailing strategy as part of the plan
		Have you defined the list of Stakeholders and Resistors and developed a plan to address?	Audience Analysis and Resistance Tracking
		Have you determined a regular interval for communication?	Think carefully about the interval, as there must be enough substance to communicate. Then stick to the promise!
		Have you determined the preferred channels of communication?	E-mail, voicemail, face-to-face, etc.
		Have you determined a means to answer follow-up questions after communications go out?	Email, Question Box or shared network file folder, etc.
		Have you determined a process for follow-up communications?	Select an owner to gather and compile input for communications
		Have you held a kick-off meeting?	Clarify the objectives, roles, timelines, and build excitement.
		Have you identified a theme, system name, training theme that should be incorporated into the communication and training plans?	

12.6.1.5.3 Change Management Audit Checklist

This form provides an audit checklist for an internal or external auditor to evaluate the Change Management process, end to end.

I. DOCUMENTATION, POLICIES AND PROCEDURES		Date	Initial	Pass	Fail	Comment
Objective:						
To ensure a formally documented change management process exists and is maintained to reflect the current process.						
Risk/Exposure:						
Lack of a formal change control process could result in the delivery of inconsistent and unreliable products.						
Tests:						
1.1	Determine if a change management process exists and is formally documented.					
1.2	Determine that each critical application & system has an assigned owner					
1.3	Determine if change management operations has a current, comprehensive list of systems and system owners.					
1.4	Obtain a copy of the change management procedures and verify that they include:					
a	Accountability for managing and coordinating changes;					
b	The change management flows within the organization;					
c	The change management responsibilities of each organizational function;					
d	The deliverables from each organizational component;					
e	Specific timetables for scheduling and reviewing planned changes;					
f	Specific timetables for the retention of historical records;					
g	Handling procedures for all changes, including change back-outs;					
h	The circumstances when normal change management controls can be waived, and the methodology to be followed in those situations.					
1.5	Determine the process used to identify & update documentation as a result of the change(s) made.					
1.6	Determine if a process exists to maintain the change management procedures.					

II. CHANGE INITIATION AND APPROVAL	Date	Initial	Pass	Fail	Comments
Objective: To ensure change requests are properly initiated and approved. **Risk/Exposure:** Unauthorized changes could result in unpredictable business solutions that would not meet the users' requirements.					
Tests:					
2.1 Verify a methodology is used for initiation and approval of changes.					
2.2 Ensure the request form includes the following minimal information:					
a Name of requester					
b Requester's signature					
c Reason for change					
d List of modules that need to be changed					
e Supervisor's name					
f Supervisor's approval (approved by someone above the requester).					
g Project Plans					
h Backout Plans					
I Communication Plans					
2.3 Determine if priorities are assigned to change requests.					
2.4 Ensure estimated time of completion and costs are communicated.					
2.5 Is there a process to control and monitor change requests?					
2.6 Determine through trend analysis if there are systems that have an unusually high number of changes, which could suggest other issues.					

III. MODIFICATION & DEVELOPMENT	Date	Initial	Pass	Fail	Comments
Objective: Ensure modification, development and testing is performed in a segregated, controlled environment (separate from quality assurance (QA) and production). **Risk/Exposure:** Modification, development and testing may adversely affect other systems if not performed in a segregated, controlled environment.					
Tests:					
3.1 Ensure all changes are applied to a copy of the latest production version of the system or application.					
3.2 Verify the separate from testing quality assurance, and production.					
3.3 For software development, determine if more than one programmer can check out programs simultaneously. Verify a process exists to support concurrent development.					
a Does the change management software have a checkout feature?					
b Is the feature used?					
c If the feature is not used, how are simultaneous checkouts controlled?					
3.4 Determine if a version control process exists to ensure the correct module was copied from production.					
3.5 Determine how the programmer is made aware of all the modules that need to be changed.					
3.6 Ensure history records are kept of code check-ins/outs, and deletions, which are made to the production library. Determine if a work order number is associated with the history record (this should be traceable back to the initial request).					
3.7 Verify a process exists that requires Programming Management to review the source documentation or code [if applicable] to ensure changes are appropriate and meet the departments programming and documentation standards.					

IV. TESTING AND ACCEPTANCE	Date	Initial	Pass	Fail	Comments
Objective: To ensure changes made to applications and systems are adequately tested before being placed into a production environment. **Risk/Exposure:** Lack of (or inadequate) testing could result in the migration of unauthorized of applications and systems into production.					
Tests:					
4.1 Verify testing is performed in a separate controlled lab environment.					
4.2 Determine how the subject (code or system) is moved into the testing QA environment.					
4.3 Determine who moves the subject into the testing QA environment.					
4.4 Determine a process exists to "freeze" the subject once migrated into the testing quality assurance environment. This ensures no further changes can be made while awaiting User acceptance.					
4.5 Determine to what extent the User is involved in the testing process (e.g., preparation of tests and data).					
4.6 Ensure the test results are reviewed and approved by the User. Verify the method of User acceptance (e.g., verbal, written).					
4.7 Determine that any changes resulting from user testing triggers a complete re-testing of the system.					
4.8 Verify the existence of back-out procedures. These procedures should outline the process used to back out of the testing QA region, in the event the User does not approve the original changes and additional modifications are necessary.					
4.9 Ensure a process exists to document problems encountered during this phase of the change methodology. Determine how problems are followed-up and resolved.					

V. IMPLEMENTATION	Date	Initial	Pass	Fail	Comments
Objective: To ensure only authorized and approved systems and software are moved into production. **Risk/Exposure:** Unauthorized systems and software migrated into production could adversely impact the production environment.					
Tests:					
5.1 Verify procedures exist to ensure the approved subject from the test environment is the version moved into production.					
5.2 Determine who is responsible for migration of the subject into production.					
5.3 Determine how the subject is implemented into the production environment.					
5.4 Verify the existence of back-out procedures. These procedures should outline the process used to back out of production and reinstall the most recent version of the code or replacement system.					
5.5 Determine if a process exists to reconcile changes scheduled for implementation to those changes actually implemented. Verify who performs this process and how often the process takes place.					

VI. NON-EMERGENCY CHANGE MANAGEMENT COMPLIANCE		Date	Initial	Pass	Fail	Comments
Objective: To verify changes are properly authorized and adhere to the established change control methodology. **Risk/Exposure:** Lack of a change control process could result in un-tested and unauthorized migration of code or systems into production. This could result in delays in production processing, customer dissatisfaction and adversely affect application processing to produce unintended results.						
Tests:						
6.1	Select a sample of non-emergency changes (application/system) that have occurred during the period of review.					
6.2	Using the sample selected, verify the following:					
a	All changes have been formally initiated, completely documented, and approved by the system owner(s).					
b	All changes have documentation stating the subject is ready to be moved from development to testing/QA with the authorized approvals.					
c	All changes have documentation stating that they have been received and reviewed by a QA type function and approved by the User prior to installation into production.					
d	Review User test documentation for adequacy and proper signoff.					
e	Documentation exists showing a source comparison was performed prior to installation into production ensuring consistency between source and object code (if applicable).					

VII. EMERGENCY CHANGE MANAGEMENT	Date	Initial	Pass	Fail	Comments
Objective: To ensure a process exists to control and supervise changes made in an emergency situation. **Risk/Exposure:** Lack of an emergency change process could result in the unauthorized migration of code or systems into production. This may result in delays in production processing, and customer dissatisfaction.					
Tests:					
7.1 Determine if a process exists to control and supervise emergency changes.					
7.2 Determine the use of emergency user IDs. If emergency changes are made through the use of emergency Ids, ensure a process exists to enable and disable them (at a minimum 2 people should be involved in this process - if it is not automated).					
7.3 Ensure an audit trail exists of all emergency ID usage and that it is independently reviewed.					
7.4 Ensure emergency changes are approved by appropriate levels of management, prior to implementation into production.					
7.5 Determine that procedures require that emergency changes are supported by appropriate documentation (e.g., evidence of management approval, code review) within one business day after the emergency is resolved.					
7.6 Verify a list of Business/Operations Management allowed to approve emergency changes exists. Programmers should not be able to initiate emergency changes.					

7.7	Determine if the approval of Business/Operations Management is required prior to the implementation of an emergency change.					
7.8	Ensure back-out procedures exist. These procedures should outline the process used to back out of the production environment.					
7.9	Determine the number of emergency changes made during the audit period under review. Analyze the volume of emergency access requests and determine if it appears to be excessive.					
7.1	Determine if emergency fixes are closed out in a reasonable amount of time.					
VIII. EMERGENCY CHANGE MANAGEMENT AUDIT COMPLIANCE		**Date**	**Initial**	**Pass**	**Fail**	**Comments**
Objective: To ensure a process exists to control and supervise changes made in an emergency situation. **Risk/Exposure:** Lack of a process to control emergency changes could result in unauthorized changes being moved into production. This may adversely affect production processing, and result in customer dissatisfaction.						
Tests:						
8.1	Select a sample of emergency changes that have occurred during the audit period under review. Determine if any of the changes should have gone through the non-emergency change process.					
8.2	Using the sample selected, determine if the changes have been made in compliance with the established procedures.					
8.3	Using the sample selected, verify that the date on the approval documentation is not more than one day after the date on the executable module. (Pre-approved for deployment)					

IX. SECURITY	Date	Initial	Pass	Fail	Comments
Objective: Ensure access to change management libraries is restricted to authorized personnel. **Risk/Exposure:** Unauthorized access could result in the intentional or inadvertent modification and/or destruction of application or system software.					
Tests:					
9.1 Obtain a list of the application and system, production and test/QA source, executable libraries/directories.					
9.2 Review security rules to ensure access has been restricted to authorized individuals.					
9.3 Determine that access to Acceptance Libraries is properly restricted to Users, Production Control and Information Security staff.					
9.4 How often is the environment audited for unauthorized change? How?					

12.7 CONFIGURATION MANAGEMENT OVERVIEW

Configuration Management is mentioned here as it relates and integrates tightly with the Change Management process. Configuration Management involves planning changes to the components of a system, and tracking the implementation of changes. Configuration Management focuses on the systems and components that are subject to change, their status, and relationships with one another. When you embark on a Change Management process, you are building the foundation for and refining a Configuration Management process, and vice versa. You cannot properly implement one process without considering the other.

12.7.1 Introduction

To help ensure network and asset availability, IT organizations have invested in various solutions including fault and performance management systems. Organizations have begun to deploy intrusion detection and prevention systems to counter increasing security threats. While these systems are valuable, they are only part of the solution to keep networks available and secure.

Enterprises also need Configuration Management at the device layer. Industry analysts estimate that 50% to 70% of all network outages are directly attributable to errors introduced during configuration and change. Configuration Management enables visualization into network devices, providing information on location, vendor, version, status, and revision history.

Configuration Management tools increase network availability and improve security by validating network device configurations, reporting and validating changes, and preventing errors from being introduced during the change process. These tools also provide notifications when unauthorized changes are made and provide complete history reports.

Configuration Management can be complex and confusing due to the number of different systems and components that makes up the IT environment. By keeping the process simple we can keep costs under control and focus on what really needs to be done.

The following basic set of rules will aid in the introduction of Configuration Management:

1. No changes are permitted without approval and an assigned task.
2. All changes made will be communicated to management and business owners via e-mail.
3. Change Owners will document the change in a formal Request For Change form, and save it to a central storage location.
4. The latest configuration profile will be stored in a central storage location.
5. Configuration changes are tracked by project, task, category, person/group and component (Configuration Item or CI).
6. No task is complete until the Configuration Management detail update is completed.

This set of principles does not require a high-tech solution, but should be incorporated into all configuration management solutions. It is preferable to use a central system that can crawl the network to verify and update configuration data.

12.7.2 Objectives

The objectives of Configuration Management are to:

- Identify all components of a system,
- Track all components of a system and their status at discrete points in time,
- Control all movement of components within the system,
- Ensure that only properly approved changes are made to systems,
- Perform status accounting; record and report change processing and status.

To ensure that all components of the system in a large environment are migrated correctly through each of the development, test, and production environments. This is a large and complex task, especially when multiple configurations or components are involved. This task is made much easier if proper procedures are in place and are followed.

12.7.3 Tools

Configuration Management without a central storage facility increases complexity dramatically as well as risk. In a fragmented environment there is a lack of a coherent view of the current state of the enterprise architecture design. Using a CMDB to record and track configuration changes and an auditing package like Tripwire will reduce risk and provide a validation of current configurations.

A helpdesk can only function properly if the help desk operator has easy access to the latest configuration data. IT helpdesks with a tight coupling to the Configuration Management process function more effectively. The helpdesk can assist to ensure a functioning Configuration Management process by continually auditing and reporting the differences between an expected configuration and an actual configuration of IT systems.

The primary tools used for Configuration Management are:

- CMDB (Configuration Management DataBase)
- Configuration and change auditing software
- Standard sub-volumes on which the correct version of each component is stored in each environment,
- Tools to track the location and status of each component,
- Procedures and tools to facilitate the promotion, demotion and backing out of component changes,
- Forms to document and control changes made to systems.

Configuration Management Checklist

The checklist helps ensure that the appropriate items have been included for effective configuration management.

ITEM	Y/N	DESCRIPTION
1		Is there a configuration management (CM) plan for the system development effort? Does it include the following: • Roles and responsibilities for CM • Configuration identification activities • Software build activities • Change control activities • Status accounting activities • Audit activities • Reporting and reviews activities • How to integrate changes to items outside the control of the project that affect the items in this project, and vice versa.
2		Is there someone to perform the configuration management activities?
3		Are sufficient tools and funding for performing the CM activities?
4		Are all configuration items identified and documented?
5		Is there a CM library of software baselines?
6		Are software builds done according to plan and schedule, using the baseline library?
7		Are changes to baselines controlled?
8		Are baseline audits planned and conducted?
9		Is a documented change control process being followed that supports the following: • Documenting a requested change • Reviewing a requested change by a change control board • Examining impact to the project if a change is approved • Modifying project plans to incorporate any approved change • Tracking a change request from submission to completion
10		Is there a functioning Change Advisory Board, with joint representation of supplier, acquirer, and customer (as appropriate)?
11		Are standard reports on CM activities prepared and made available?
12		Do quality assurance personnel review CM activities and results?
13		Are measures made to determine status of CM activities?
14		Are issues of interface control between components and outside components being identified and addressed?
15		Other?

12.8 GLOSSARY OF TERMS

CMDB Configuration Management Data Base: Logical database containing complete and accurate information about items used in IT service delivery (hardware, software, services, etc.)

COBIT	Control Objectives for IT: Reference standard of good practice issued by the IT Governance Institute.
CSF	Critical Success Factor: Condition that needs to be met for a successful initiative.
ITIL	IT Infrastructure Library: Service management framework that encapsulates best practice.
KPI	Key Performance Indicator: A metric that provides information about the 'health' of a process or service.
KGI	Key Goal Indicator: A metric that provides information about achievement of process or service goals and outcomes.
MTBF	Mean Time Between Failure: The average time expected between component or system failures. Life expectancy of the item, usually indicated by manufacturer.
RFC	Request For Change: A standard way of submitting requirements into the Change Management process.
SLA	Service Level Agreement: Agreement between the IT function and users of IT services that documents service characteristics and target service levels.
TRT	Target Resolution Time: The target time for resolution of an incident (an event that has or potentially will cause a negative service impact).

12.9 REFERENCES

Capability Maturity Model Integration (CMMI).Carnegie Mellon University, Software Engineering Institute. Available at http://www.sei.cmu.edu/cmmi/cmmi.html.

CMMI: Guidelines for Process Integration and Product Improvement. Addison Wesley, 2003. Specifically refer to the configuration management process area.

COBIT [Control Objectives for Information and related Technology] 3rd Edition Executive Summary, July 2000. **Erreur ! Référence de lien hypertexte non valide.**. Specifically refer to AI-6: Acquisition and Implementation: Manage changes, and DS-9: Delivery and Support: Manage the configurations.

Information Technology Infrastructure Library (ITIL). Office of Government Commerce. Refer to http://www.ogc.gov.uk/index.asp?id=2261and http://www.itsmf.com/. Specifically refer to the volume *Best Practice for Service Support*, Chapter 8, Change Management (2000).

ISO/IEC 17799 Information Technology Code of Practices for Information Security Management, First Edition. ISO/IEC 17799:2000(E). December 2001. Specifically refer to Sections 8.1.2 Operational change control, 10.5.1 Change control procedures, 10.5.2 Technical review of operating system changes, and 10.5.3 Restrictions on changes to software packages.

Analysis of Benefits and Costs (ABC's) Guideline, Volume 2, U.S. Department of Energy Assistant Secretary, Management and Administration Directorate of Administration Office of ADP Management, June 1988

Microsoft Service Management Functions Operations Guide: Change Management. Microsoft Corp., 2004. Available at: http://www.microsoft.com/technet/itsolutions/techguide/msm/smf/smfchgmg.mspx.

Systems Assurance and Control (SAC). The Institute of Internal Auditors Research Foundation, August 2003. Information and table of contents available at http://www.theiia.org/esac/index.cfm.

Visible Ops Handbook: Starting ITIL in Four Practical Steps. IT Process Institute, 2004. Information is available at http://www.itpi.org/visibleops

Changing Minds website: http://changingminds.org

The Change Management Learning Center:
http://www.change-management.com/best-practices-report.htm

IT Service Management: Selecting the Right Metrics for Performance Measurement
http://www.ins.com/downloads/whitepapers/ins_white_paper_itsm_metrics_0404.pdf

13 ENTERPRISE SECURITY AWARENESS

The rationale

There is strong and growing evidence that information security, despite its apparent technological overtones, depends more on people than on technology. Improving security is largely about changing the attitude and behavior of individuals; most of who are users.

Every security awareness program aims to increase the level of security consciousness and skills on various usage scenarios throughout the organization to a point where security becomes second nature to the users of information systems. Another aim of any security awareness program is move to a situation where for every user, good security practices becomes a routine so that all users behave consistently in accordance with the company's security policies and procedures.

The mission

We believe that the following could constitute the generic mission for accomplishment by the client's security awareness program:

- To ensure all staff throughout the organization are aware of the importance of security, policies and practices, their obligations and responsibilities.

- To have a range of security awareness solutions in place to meet the needs of staff and enable them to fulfill their responsibilities. The obvious first step would be to induct all users through a structured security awareness program

- To work closely with all users to improve security awareness communication, cooperation, and coordination channels.

  A first step would in this process of creating security awareness is to present a series of security awareness workshops and events covering all users of information infrastructure. Details of the content and structure of this workshop is given later in this section.

The next steps

As this progresses to a certain stage, clients would like to move towards a comprehensive security awareness initiative that can meet the following objectives:

- To develop an understanding of the factors which influence security behavior and have a clear strategic road map for the security awareness function that will assist management in making security awareness decisions.

- To establish the necessary security awareness infrastructure for the ongoing management of security awareness initiatives (which includes the organization, team of security professionals, and state of art tools and techniques).

Business Benefits

The following summarizes, at a perspective level, the business benefits of implementing a comprehensive security awareness program:

- Enhanced security and business continuity awareness by increased visibility of areas of concern and client's approved information security policies, practices, procedures and responsibilities.

- Introduce desired changes in corporate security culture by developing a team-oriented, customer-focused, value-creating, knowledge-based security culture.

- Enhance security effectiveness by building relationships to obtain commitment, improve coordination and develop competencies.

- Reduce Risk by minimizing potential loss of critical information through due diligence.

- Increase stakeholder trust by enabling secure business environment.

Phases of the program

As stated in the mission statements earlier, the first part of the security awareness initiative is to create and implement a series of training modules of class room based security awareness program. Once a significant part of the users have gone through this program, executive management would like to propose a series of tests and quizzes (with varying degree of difficulty) to be taken by volunteers and their performance ranked and top performers be openly recognized and rewarded.

It will also be a good idea for the management to declare that a minimal degree of security awareness is expected of all users and the users taking an on-line test on basics of security implementation can demonstrate the reaching of such awareness. This test can be designed and administered from a secure server in client premises or through a WAN link to a third party secure server already implementing on-line tests for a couple of certification examinations.

Contents of first phase awareness program

The following are the recommended contents of the first phase of security awareness program that would be administered through a three-hour classroom based, instructor led presentation.

To make this presentation more appropriate to the users of client information system, it is suggested that the organization permit training providers to study the security policies and procedures (to the extent it does not infringe on the confidentiality of the contents). Such a study would permit the training providers to incorporate the relevant policies, procedures and guidelines into the awareness program.

- Introduction to Information Security
    - What are information resources?
    - What is information security?
    - User responsibility
    - Consequences of poor security

  - Common areas of security infraction
- Passwords
  - Passwords – the first and most used layer of defense
  - Creating the 'right' password
  - Password management – process, implementation and review
- E-Mail & Internet Usage
  - The 'dark side' of e-mails
  - Malicious attachments – recognition and management
  - Spam, hoaxes & chain letters
  - Applets and Active-X – the small bomb!
  - Surfing the net but safely
  - Appropriate use policy
- PC Security
  - PC theft – the loss of box and loss of data
  - Securing your PC
  - Access control on PC data
- Network Security
  - The basics of networked information systems
  - Implications of compromising the corporate network
  - User authentication process and security
- Data Confidentiality
  - What data is confidential
  - Keeping data secure
  - Social engineering
  - Dumpster diving
  - Data destruction – policies and processes
  - Eavesdropping
  - Should you talk?

13.1 METHODOLOGY FOR SECURITY AWARENESS PROGRAM

There are many different ways to get the information security messages across to employees. What was mentioned above is one sure starting point and the following are some of the other methods that can be actively considered for creating and implementing a good security awareness program.

- Computer Based Security Awareness application
- Security Policy based awareness program
- Awareness Services and Reminder Tools

The content for the Computer Based Awareness application or program is almost the same as the one, which is covered in instructor-led programs.

13.2 AWARENESS SERVICES AND REMINDER TOOLS

. It is important to keep security message in the minds of all users throughout the year.

There are different methods to remind users about security on continual basis. Using one or more of these messages can help organization invoke a cultural change when it comes to information security. Reminder tools should cover under mentioned security awareness topics

- Password Construction
- Password Management
- Internet Usage
- Telephone Fraud
- Physical Security
- E-mail Usage
- Privacy
- Viruses
- PC Security
- Backups
- Building Access
- Social Engineering
- Identity theft
- Mobile Devices – USB,PDA,etc

(Source: www.securityawareness.com)

13.3 REMINDER PROGRAMS

- **Security booklet**

  Security awareness booklet looks at enterprise security and focuses on objectives of information security, activities needed to ensure security, staff responsibility, and human factor in information security, social engineering, incident handling and reporting to the right people. The booklet also has information security related pictures, quotes and case studies to educate employee.

- **Security posters**

  Images have greater impact than words. Posters are the best source to convey meanings in short and descriptive format. A poster series with themes or related designs can be used to highlight specific security issues. Posters help to educate employees on the simple steps they can take to protect their PCs, environment, organization and human life. By placing posters in different

areas like break rooms, above water fountains and coffee machines, where staff normally spend a some time, employees can be efficiently and effectively educated on information security topics.

- **Computer screen savers**

  Screen savers are graphic form of communication, although they are like posters but animation and user interaction makes them more interesting. Short questions and answers, security related quotes and graphical representation of security awareness issues get more attention of the user and hence easy to educate both the novices and busy users.

- **Regular Survey Programs**

  Companies should have regular security survey conducted with a predetermined interval so that the company follows the Security Policies. This practice will give a clear picture of the status of security awareness program and encourage employees to stay up to date to perform better in the next survey.

- **Email shots**

  Important part of the security awareness program is cost effective and easy to deliver reminder message through email. Email is basic part of business and personal communication and mainly all of the people access it once a day.

- **Promotional items with security messages**

  Promotional items and gifts make people happy and users retain them for long. Adding security awareness quotes and images to promotional items and gifts should be part of organization ongoing security awareness campaign.

  Various give away items can be imprinted with a security slogan and contact information, such as security staff phone numbers or the organization's security web site address. Examples of give-away items are:

  - Pencils, pens and Erasers
  - Notepads , Frisbees

- Mouse pads and inserts
- Key chains
- Flashlights
- Cups or mugs
- TEA stands for training, education, and awareness
- Magnets, buttons, stickers
- First-aid kits
- Rulers, calculators

Summarizing, the organization should ensure that the following list of Do's and Don'ts are clearly brought to the attention of all people involved in handling any part of the information system; be they users, designers or managers of information processes and systems:

Don'ts

- Do not share your password with anyone including staff
- Do not write your password on any paper, whiteboard or post it pad
- Do not use easy to remember words as passwords e.g. Aug2001
- Do not use personal information or any word in any language spelled forwards or backwards in any dictionary
- Do not visit inappropriate web sites e.g. pornographic or hacker web sites
- Do not download unlawful or unlicensed software from the Internet
- Do not install unlicensed software onto your computer

Do's

- Do change your password regularly for your different accounts
- Do use a combination of letters, symbols and number for passwords
- Do use difficult passwords which are at least 9 characters long
- Do enable your Screen Saver Password or lock your workstation
- Do scan your computer regularly for viruses and any diskettes as well before you use them on your computer
- Do check that your virus software patches have been updated when you receive the regular update emails from Desktop Support
- Do lock away all confidential documents, files and diskettes at the end of each work day

Social Engineering

1. Be careful that your desire to be helpful in performing everyday tasks does not lead to giving away confidential details to the wrong person about your organizations business.
2. Don't fall into the trap of trusting a person until they prove to be untrustworthy.
3. Be suspicious if you get a request from someone asking you to fax or email information to them right away, but refuses to provide you a direct callback number.
4. Don't be intimidated into giving out information to an irate caller, or one who seems to know the structure of your organization.
5. Watch out for the "odd" request or when a caller asks for information that seems a bit out of the ordinary.
6. Be careful not to cut corners by writing down passwords or leaving confidential material lying around. Securely store confidential material.
7. If you are throwing confidential material away, shred it first.
8. If you print something or have something faxed to you that is sensitive, pick it up right away and store it securely.

Sharing Information

1. Verify positive identity of requestor before providing any confidential information.
2. Verify requestors need to know.
3. Never disclose Restricted Information such as your password to anyone for any reason.
4. Always be aware of how sensitive the information is that you are working with.

Electronic storage and transfer of information

1. Determine your data sensitivity.
2. Always take a "default deny" stance in providing access to information.
3. Assign security permissions to a role or group rather than to an individual.
4. Only provide the minimum level of access necessary to meet specific business requirements.
5. Remove or disable all unused access IDs and privileges on a regular basis.
6. Log and monitor access of sensitive information and notify your management and IT Security of any noticeable misuse.
7. Classify data you own according to your organizations Information Sensitivity Model.
8. Keep classified data partitioned by as many levels of technology separation as practically possible.

9. Encrypt the transmission of Confidential information when sending to an Internet address.
10. Encrypt Confidential information when stored in the DMZ or on the Internet.
11. Choose to store important and confidential information on a company network drive.
12. Backup your local hard drive on a regular basis.

Passwords

1. Do not use family names, nicknames, anniversaries, birthdays, pet names, sports teams or any such items that others would associate you with.
2. Do not use the word “password” for any of your personal password selections.
3. Select a password that is long and strong and a non-dictionary word.
4. Use a minimum of 8 characters using both upper and lower case letters, and a mix of numbers and special characters or symbols.
5. To help you remember your password use the first letter’s of each word in a phrase that means something to you. One way to do this is to create a password based on a song title, affirmation, or other phrase.
6. Never change your password to something known to anyone else, not even for a moment.
7. Keeping your password to yourself is critical to your company’s security. Never share your password with anyone – including your manager, IT Security, IT Help Desk, family, friends or co-workers.
8. Never use the same password for both your work and personal accounts.

Email

1. Always encrypt sensitive Email and attachments destined to an Internet address.
2. Always delete unrecognized Email. Never open or respond to any Email or attachment unless you positively recognize or trust the sender. This includes spam (junk Email).

Personal Computers

1. Only install software from trusted sources.
2. Keep all your PC software versions up to date with the most current patches and fixes.
3. Install Antivirus and Firewall software.
4. Never change any settings within your business computer BIOS, the operating system, or any applications (this includes personal firewalls and anti-virus utilities)

5. Never enter unfamiliar commands or run programs at the request of any person unless you can positively verify their identity as a current IT Group employee.
6. Regularly backup critical data on your local hard drives and record your critical configuration settings either to a corporate network drive or a CD-ROM on a routine basis.

Portable Computers

1. When you leave your portable computer unattended use a security cable to “tie down” your portable computer to a desk or other heavy object.
2. Consider software solutions that will cause stolen portable computers to “call home” when connected to the Internet and GPS devices that will allow you to track your portable computer’s current location.
3. Implement startup security options that will prevent your portable computer from booting into the operating system unless a pass phrase is entered or unless a specific floppy disk is in the drive.
4. Never leave your portable computer unattended, even briefly, in any public place.
5. If you leave your computer in your car, make sure to always keep your car locked and store your computer out of site under a rear pull-cover or in the trunk.
6. Avoid using any storage / carry cases that include a manufacturer’s label on the outside and scream I have a computer inside.
7. On the computer case and the portable computer itself use tamper-resistant tags or directly engrave identifying information like your company and personal name and contact information.
8. Never store associated security devices in the same location as your computer. For example, Secure ID Key-Fob / Tokens should never be stored near your desk or in your carry bag next to your computer. Always keep your security devices with you personally or store them in a secure location separate from your computer.

Telephone Voicemail

1. Do not set your voicemail password to the same number as your phone extension or any other common personal information others might think you could use.
2. It’s best to change your voicemail password often, at least every three months, especially if you think you may receive sensitive messages.
3. Follow the Password best practices listed above.

14 ENTERPRISE INCIDENT MANAGEMENT

14.1 INCIDENT ANALYSIS EVALUATION CHECKLIST

Incident Category	**Affected Party(ies)**
Potential implication Reputation Loss / Embarrassment / Confidentiality and Integrity of Correspondence / Availability to the visitors.	
Likelihood of Reoccurrence High (24/7/365 Web Presence / no analysis and countermeasure placements yet)	
Incident Occurred Date / Period	**Information Asset affected**
Incidence Response Date	**Contact Person at Affected Party(ies)**
Reason for IR Response	

ID	Items	Results / Comments	W/P Ref
Operational			
1.	Did the Webhosting provider agreed to any T&C / SLA related to activities such as cracking, hacking, defacements etc? (if yes then what are those terms)		
2.	Did the external and / or internal auditors highlight this incident as a potential risk?		
3.	Did the possibility of this incident was considered during last organizational risk assessment and risk analysis activities? Was ALE (annual loss expectancy) and SLE (single loss expectancy) calculated for risk or such incidents?		
4.	Did any financial cost occur to place countermeasures for the related information assets' protection? (if yes then did their cost/feasibility analysis covered the risk of such incidents?)		
5.	Is there any business continuity / disaster recovery / system failure / system non-reliance plan prepared in an event of such incidents? (if yes – were they invoked for the incident?)		

ID	Items	Results / Comments	W/P Ref
Technical			
6.	Examine log files for connections from odd locations or other unusual activities. Suggestions: lastlog, firewall logs, syslogs, etc. Note: unless your log files are not maintained in a real time append-only media, the integrity of logs is susceptible; otherwise, it may provide certain essential clues.		
7.	Identify setuid and setgid files: 1. find / -user root -perm -4000 -print 2. find / -group kmem -perm -2000 –print		
8.	Check to ensure integrity of your system binaries such as login, su, telnet, netstat, ifconfig, ls, find, du, df, libc, sync, etc. Also ensure integrity of any binaries referenced in /etc/intetd.conf and xinetd.conf Compare the binaries with your known good / fresh copy of same operating system version. (use md5 or sha1 hashsum algorithms for comparisons as other parameters can be duplicated as well)		
9.	Check your systems for unauthorized use of a network monitoring program, commonly called a sniffer or packet sniffer.		

ID	Items	Results / Comments	W/P Ref
	(Intruders may use a sniffer to capture user account and password information)		
10.	Examine and double check for all the files initiated by cron / at daemons.		
11.	Check for unauthorized services, initiate a full-length portscan and check all entries in /etc/inetd.conf		
12.	Examine the /etc/passwd and /etc/shadow files for unauthorized entries.		
13.	Examine the apache http logs for web application attack / injection attempts.		
14.	Review the attempted applications with their vendors for recent vulnerabilities and patches.		
15.	Review the last applied patches with the vendors of operating system and of deployed service for patch delays.		
16.	Review the procedure of Patch Management and examine any shortcomings.		

14.2 LINKS OF VARIOUS COUNTRIES LAWS

14.2.1 United States

- U.S. Federal Sentencing Guidelines

  - Lighter penalties on companies that adopt and follow an effective compliance program.
- Sarbanes-Oxley
  - Accounting reform and investor protection legislation intended to reestablish investor confidence.
  - Section 302: CEO and CFO must sign statement s verifying the completeness and accuracy of financial reports.
  - Section 404: CEOs, CFOs and auditors must report on and attest to the effectiveness of internal controls for financial reporting.
- Gramm-Leach-Bliley Act (GLBA)
  - Protect consumers' personal financial information held by financial institutions or their service providers.
  - The financial institution shall be subject to a civil penalty of not more than $100,000 for each violation;
- California SB 1386 / Notification of Risk to Personal Data Act
  - Recently submitted federal version
  - Requires disclosure of any security breach that involves personal information of a California resident, if the information is unencrypted and is reasonably believed to have been acquired by an unauthorized person.
- Health Insurance Portability and Accountability Act (HIPAA)
  - Part of a broad Congressional attempt at incremental healthcare reform.
  - Protect the security and confidentiality of electronic healthcare information.
  - Healthcare providers must provide notice of privacy policies and procedures to patients, obtain consent and authorization for use of information and tell how information is generally shared and how patients can access, inspect, copy and amend their own medical records.
  - The officers and directors of the financial institution shall be subject to, and personally liable for, a civil penalty of not more than $10,000 for each violation.
- American Express Data Security Standards
  - AE provides their data security standards for merchants to establish security programs.
  - Encrypt all stored payment data using triple DES encryption.
  - Be prepared to provide audit reports to AE or allow AE audits.
- VISA Cardholder Information Security Program (CISP)

  - Provides a standard of care and enforcement for protecting sensitive information
  - 12 basic security requirements which VISA payment system users must comply with.
  - Failure to participate may result in considerable fines starting at $50,000 imposed by VISA or exclusion from the VISA program.
- MasterCard Site Data Protection Program (SDP)
  - Providing security requirements and best practices.
  - Provide merchants with security Self-Assessment and Network Scanning Tools.

Gramm-Leach-Bliley Act	Financial
Turnbull Report: Combined Code on Internal Controls in the UK (1999)	Companies listed on London Stock Exchange
HCFA-0049-P Proposed Rule HIPAA regulations (scheduled for fall 2000)	Healthcare including both caregivers and insurance
ISO 9000, 9001, etc. (1994)	Manufacturing
Paperwork Reduction Act (44 U.S.C. Chapter 35 1995)	Federal Government
Computer Security Act (1987)	Federal Government
FFIEC SR97-16 (SPE) (May 1997)	Banking and any related service providers
FFIEC FIL-67-97; Stronger wording on client/server environment replacement for FFIEC FIL 82-96	Banking and any related service providers
Consumer Credit Protection Act (CCPA) section 2001 Title IX (1992)	Cross-Industry
FEMA FRPG 01-94 1994	Federal Government and associated contractors
Foreign Corrupt Practices Act (1977)	Cross-Industry
Comptroller of Currency BC-177 (1983, 1987) superceded by FFIEC	Banking
Inter-Agency Policy from Federal Financial Institutions Examination Council (FFIEC - 1989, revised and	Banking and any related service bureaus, includes credit unions

made stronger 1997)	
Federal Home Loan Bank Bulletin R-67 (1986) superceded by FFIEC	Banking
IRS Procedure 86-19	Cross-Industry
Fair Credit Reporting Act	Credit Reporting Agencies
Clinical Laboratory Information Act (1988)	Healthcare
JCAHO Accreditation Manual for Hospitals (1997)	Healthcare
Various State Dept. of Administrative Services Policies, e.g., Texas, (1 TAC 210.13(b)), Oregon's Dept. of Information Resources (ORS 291.038)	State Government
BS7799 Section 9	Pan European Industry
GAO/IMTEC-91-56 Financial Markets: Computer Security Controls	Financial

14.2.2 India

- IT Act 2001

14.2.3 EU Laws

http://www.europa.eu.int/eur-lex/en/lif/reg/en_register_132060.html

14.2.4 Portugal

- DL nº67/98) Personal data protection law
  http://www.cnpd.pt/Leis/lei_6798.htm
- DL n69/98) Personal data protection law for Telco's
  http://www.cnpd.pt/Leis/lei_6998.htm
- LC nº 1/2001, article 35) IT usage
  http://www.pj.pt/htm/legislacao/dr_informatica/LeiConst1_2001.htm
  http://www.pj.pt/htm/legislacao/dr_informatica/Lei109_91.htm
  http://www.pj.pt/htm/legislacao/informatica.htm

http://www.cnpd.pt

(All the given links are in Portuguese)

14.2.5 Switzerland

HTTP://WWW.ADMIN.CH/CH/D/SR/SR.HTML

14.2.6 Thailand

- Computer Crime Law
- Privacy Data Protection Law

www.impi.gob.mx/web/docs/marco_j/index_marco_j.html

www.cddhcu.gob.mx/leyinfo

http://luisrey.red-libre.org/datos/tic/Firma_Electronica.pdf

14.2.7 Singapore

- Computer Misuse Act
- E-Commerce Code for Protection of Personal Information and Communications of Consumers of Internet Commerce

14.2.8 Australia

- The Federal Privacy Act
- Commonwealth Privacy Act

14.2.9 Malaysia

- Computer Fraud and Abuse Act
- The Computer Crimes Act

14.2.10 Others

CoBIT	COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.
SAS 70	Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA)

OWASP-OWASP Guide	Open Source form which is developing guide for secure web applications
NFPA 1600	Standard on Disaster/Emergency Management and Business Continuity Programs.
Computer Security Act of 1987	The Computer Security Act requires each Federal agency to identify all Federal computer systems that contain sensitive information and implement security plans to protect these systems. The Act defines the term "sensitive information" as any unclassified information that could adversely affect the: national interest, conduct of Federal programs, or privacy to which individuals are entitled under the Privacy Act of 1974. Agencies are required to protect this information against loss, misuse, disclosure, or modification.
PIPED Act	Canadians' personal information is protected the Personal Information Protection and Electronic Documents (PIPED) Act - a law which sets out the ground rules for the collection, use and disclosure of personal information in the course of commercial activities. It balances an individual's right to privacy with an organization's needs for personal information for legitimate business purposes.
Council of Europe - Data Protection Convention (ETS no. 108)	This Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the trans-frontier flow of personal data. In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected.

Data Protection Act 1998	The UK Data Protection Act contains eight Data Protection Principles. These state that all data must be: Processed fairly and lawfully; Obtained & used only for specified and lawful purposes; Adequate, relevant and not excessive; Accurate, and where necessary, kept up to date; Kept for no longer than necessary; Processed in accordance with the individuals rights (as defined); Kept secure; Transferred only to countries that offer adequate data protection.

15 OUTSOURCING SECURITY CONCERNS

[This section is intentionally left blank]

16 BUSINESS CONTINUITY MANAGEMENT

Background

For a successful enterprise everything from its people, information and its infrastructure is an asset. The success and growth of any business is dependant on integrity, confidentiality and continuous availability of its critical assets. The Business Continuity Plan seeks to identify and weigh the potential impact of business interruption due to non-availability of key assets. It also discusses relevant controls and continuity strategies for those interruptions whose impact is high against one or more of these key assets.

Over the years, dependence upon the use of computers in the day-to-day business activities of many organizations has become the norm. Today you can find application of computers in carrying out every business function of the organization. All the branches are linked together by a sophisticated network that provides communications with central Data Center. Vital functions of the organization depend on the availability of this network of computers.

Consider for a moment the impact of a disaster that prevents the use of the critical system process. It is hard to estimate the damage to the organization that such an event might cause. One fire mishap could cause enough damage to disrupt these and other vital functions. Without adequate planning and preparation to deal with such an event, the organizations central computer systems could be unavailable for many hours or even few days.

Interruptions to business can occur from natural or human-driven disasters. Frequent interruptions often faced by businesses are equipment failures, actions by disgruntled employees, external intrusions either by professional crackers or script kiddies, etc. Disasters have many characteristics and have been best summarized in the Disaster Recovery Journal (DRJ) as “a sudden, unplanned calamitous event that brings about great damage or loss. Any event that creates an inability on the organization’s part to provide critical business functions for some undetermined period of time.”

The Business Continuity Plan (BCP) is all about Business. Business Continuity Planning and Disaster Recovery Planning have very definite roles to play in the process of managing response to any disaster or events that threaten business continuity. Clearly, the objective, scope and to some extent the methodology adopted for successful implementation of BCP and DRP are different; yet quite a few operational features have overlaps.

BCP and DRP are developed and implemented for very definite reasons, some of which include:

- Establish appropriate and immediate response to an emergency
- List procedures to be followed in emergencies identified and catalogued
- Overcome the typical confusion that normally occurs in an emergency through clear documentation, testing and training actions
- Establish criteria for declaration of a disaster and determine organizational hierarchy and authority for doing so
- Establish relationships with vendors who may need to support recovery process and establish contractual relationships with them for action in case of emergencies
- Document process to be adopted to move critical business operations to an alternate processing site when main site is damaged or is inaccessible
- Document procedures for safeguarding, storage and retrieval of information assets in case of outage

BCP and DRP needs executive management commitment if it has to succeed. First and foremost, it is executive management that has to allocate adequate resources – both fiscal and human, for the various stages of preparing, testing and maintaining the plans. More importantly a periodic show of commitment by the executive management to BCP and DRP processes will go a long way in inculcating the right kind of commitment and culture across all members of the organization.

BCP and DRP go through the following structured phases though each business entity may opt to combine two or more phases into one or may split any one of these phases into distinctly different activity set:

1. BCP/DRP planning process initiation
2. Business Impact Analysis
3. Evaluate and finalize recovery strategy

4. Design and develop BCP/DRP
5. Testing and Maintenance
6. Create awareness and train personnel

Organizations depend upon the Technological Resources for its survival and they should have a BCP in place to ensure constant availability of data. While generally it is believed that the recovery planning process should focus on recovery of information systems and data, generic disaster recovery plans take into account the recovery process of the following asst classes:

1. PEOPLE
2. Business Processes
3. Facilities and Supplies
4. Technical Processes
5. Data

In all BCP and DRP implementations, People come first. Clearly there are no questions about prioritizing anything over and above People. There are no cost-benefit analysis; no assessments and no prioritization logic when it comes to recovering people from a disaster site; people have to be evacuated to safety and without any trauma or injury - be it physical or psychological.

BCP and DRP have a lot in common but they are not the same. While DRP is focused on the processes that instantly follow a disaster and aims at recovering the five asset classes referenced above, BCP focuses on doing all that is required to be done to come back to a situation that can be referred to as “business-as-usual.” Recovering from a disaster may not always result in going to a stage that can be referred to as “business-as-usual.”

Often situations arise where the level of awareness among the different participants in the BC and DR program is significantly different. This leads to either an erroneous understanding or sometimes a gross misunderstanding of the BC and DR process which, in turn, can result in seriously impairing the efficacy of implementation of even a good plan. To overcome this, it is often suggested that at the Plan Initiation phase, a comprehensive awareness program be put in place covering all people in the organization. Success of BCP and DRP is not dependent just on the strength of the contents of the document but also on the degree of proliferation of the contents

among those who will be involved in implementing the BC and DR plans when an 'incident' occurs.

Companies should therefore document the BCP plan clearly and communicate to BCP Team and also to user management; albeit selectively if the corporate communication policy so warrants. While there are no clear consensus on what a typical BCP should necessarily contain, BCP could contain BCP Guidelines, List of Important Critical Information Assets, Priorities, Organizational Responsibility and the timing for restoration, Emergency Response Guidelines and Maintenance Plan and Testing. The BCP document may, in some cases, contain the process for Risk Assessment, Acceptance and Risk Mitigation.

16.1 INTENDED READER

Audience

BCP and DRP documents are of relevance to several groups within the administration with differing levels and types of responsibilities for business continuity, as follows:

- Senior Management
- BCP Team Leader and Alternative BCP Team Leader
- BCP Team Members
- User managers and users
- Internal and External specialists who have specific role to play in successful implementation of BCP and DRP like consultants who would be engaged for testing the BCP and DRP; those who will structure and implement awareness programs; and internal or external audit staff who are responsible for assessing the operational, control and process relevance of the plans

The BCP preparatory document is addressed particularly to the members of the BCP and DRP Team, since they have the responsibility of preparing for, responding to, and recovering from any disaster that impacts the operations of an organization.

Distribution

As a written record, this document is distributed to each member of the Business Continuity Planning Team, including members of the Support Teams. Where user managers and users have any role to play in the implementation of BCP and DRP; however small that role may be, a copy of the relevant portion of the plan document is made available to them.

This document is also distributed to members of the Steering Committee, Board of Directors and others not primarily involved but having indirect involvement in the business continuity effort.

16.2 MANAGEMENT APPROVAL

This document in its initial form is subject to review and approval process from the management which is summarized in a table like the following one:

Name of the Approving Authority	Title	Approval Date	Signature

16.3 SCOPE

The primary focus of a BCP document is to provide a plan to respond to a disaster that destroys or severely cripples the organizations infrastructure. The intent is to put in action a continuity plan till such time as the restoration operations are complete.

The Business Continuity Plan will cover:

- Identifying business processes
- Defining scope of operations covered by BCP
- Mapping key business processes and workflow required for BCP
- Identification of potential Threats to the smooth business operations
- Probability of the occurrence of the threats and Risk Ranking thereof
- Available options to address each risk (Prevention, Mitigation, Recovery)
- Selection of options
- Business Continuity Strategy
- Resumption of business operations within a stipulated time

- Description of Business Continuity Procedures
- BCP Team and description of responsibility for each member
- BCP Test Plan and Role of Internal/external auditors
- Documentation of Test Results and Enhancement of BCP
- Maintenance of BCP

16.4 BCP TEAM LEADER

The primary responsibility of the Team Leader is to provide leadership to the BCP team and coordinate support for the business continuity and recovery effort. The BCP Team Leader's role being very crucial, we have decided to ensure redundancy. With this objective the role of alternative BCP Team Leader is also created. The detailed roles and responsibilities of both BCP Team Leader and the Alternative BCP Team Leader have been furnished below.

1.	BCP Team Leader			
	Contacts	Tel:(O):	Tel:(R): –	Tel:(M):-
	Responsibilities	▪ Assumes overall responsibility for initiating business continuity plan and recovery from disaster and restoration of normal operations. (Necessary advance authorizations from top management are pre-requisites) ▪ Determines the extent and seriousness of the disaster, notifies the management immediately and keeps informed of the activities and recovery progress. ▪ Invokes the Business Continuity Plan after approval of the management. ▪ As a co-coordinator of Business Continuity project he Manages, Coordinates and directs the recovery efforts. All BCP team members will functionally report to him and all type of problem escalations will happen through him. ▪ Arranges for replacements, when needed, to fill in for any disabled or absent BC members. ▪ Keeps all members of the team informed and co-ordinates the crisis calls. ▪ Provides liaison with other members of the team for reporting the status of the recovery operations.		

	▪ Helps Insurance and Legal team members in investigating the cause of disaster. ▪ Ensures that all BC team members, Operations Head, Business Group Heads have an updated copy of Business Continuity Plan. ▪ Provides brief to Public Relations Officer (PRO).

2.

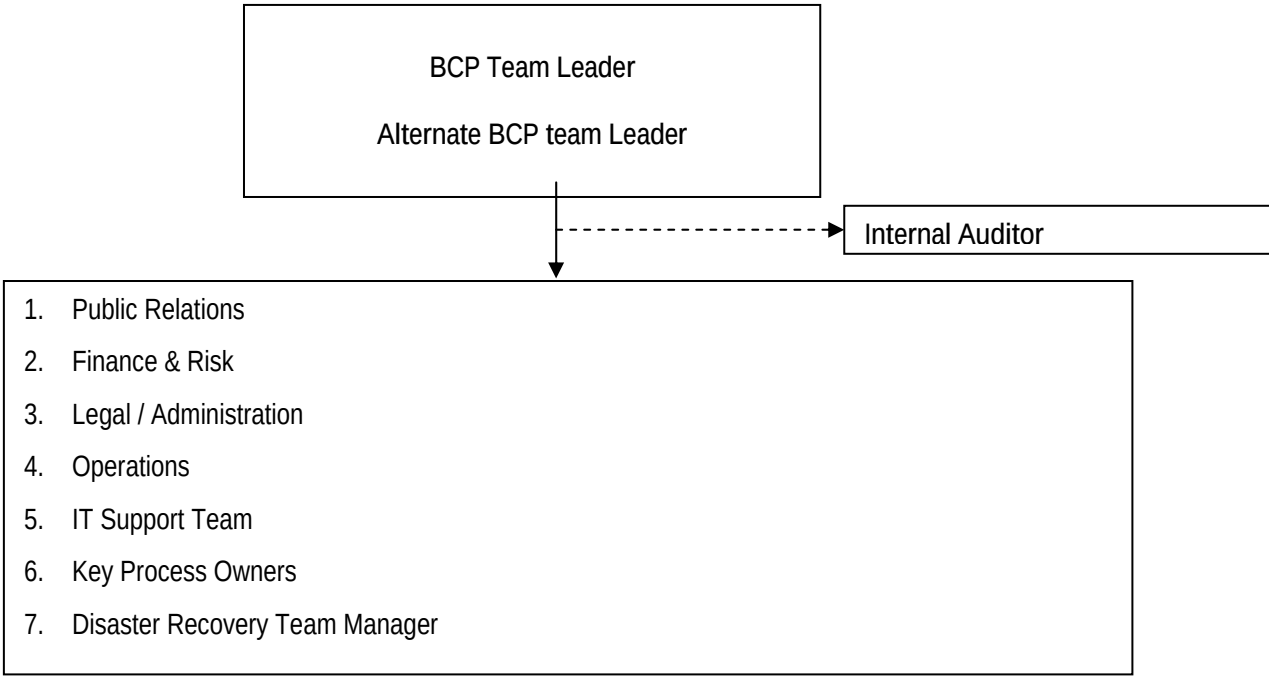
Alternate BCP Team Leader			
Contacts	Tel:(O):	Tel:(R):	Tel:(M):
Responsibilities	▪ Take over as BC Team Leader in absence of BC Leader. ▪ Assumes overall responsibility for initiating business continuity plan and recovery of normal operations. (Necessary advance authorizations from top management are pre-requisites) ▪ Determines the extent and seriousness of the disaster, notifies the management immediately and keeps informed of the activities and recovery progress. ▪ Invokes the Business Continuity Plan after approval of the management. ▪ As a co-coordinator of Business Continuity project he Manages, Coordinates and directs the recovery efforts. All BC team members will functionally report to him and all type of problem escalations will happen through him. ▪ Arranges for replacements, when needed, to fill in for any disabled or absent business continuity members. ▪ Keeps all members of the team informed and co-ordinates the crisis calls. ▪ Provides liaison with other members of the team for		

	reporting the status of the recovery operations. ▪ Helps Insurance and Legal team members in investigating the cause of disaster. ▪ Ensures that all BC team members, Operations Head, Business Group Heads have an updated copy of Business Continuity Plan. ▪ Provides brief to Public Relations Officer (PRO).

16.5 BCP TEAM

The organizational backbone of business continuity is the BC Team. In the event of a disaster affecting organization or its resources, the BC Team will respond in accordance with this Plan and will initiate specific actions for continuity. The BC Team is called into action under the authority of the BC Team Leader who has the responsibility for approving actions regarding Business Continuity Planning. The organizational structure of the BC team is depicted below.

BC TEAM ORGANISATION STRUCTURE



16.6 RESPONSIBILITIES

The roles and responsibilities of the BCP team members are listed below. Each member of the team is required to thoroughly understand his role, responsibilities, and the interdependencies. It is the duty of all the members to make themselves easily available in the event of emergencies and communicate the BCP Team Leader in advance, if they are not available due to any reason.

1.

BC Manager			
Contacts	Tel:(O):	Tel:(R):	Tel:(M):
Responsibilities	▪ Review the suitation along with Team members. ▪ Decide if BC Plan is to be invoked. ▪ Inform management of the decision. ▪ Co-ordinate the BC Plan.		

2.

Public Relations Incharge			
Contacts			
	Tel:(O):	Tel:(R):	Tel:(M):
	Tel:(O):	Tel:(R):	Tel:(M):
	Tel:(O):	Tel:(R):	Tel:(M):
	Tel:(O):	Tel:(R):	Tel:(M):
Responsibilities	• Co ordinate with the BCP Team Leader and gather facts about the suitation. • Represent appropriately the facts to the media and stake holders		

3.

Finance & Risk Incharge			
Contacts	Tel:(O):	Tel:(R):	Tel:(M):
Contacts	Tel:(O):	Tel:(R):	Tel:(M):
Responsibilities	▪ Arrange finance if required to roll out the BC Plan.		

	▪ Gather facts to assess the financial implications

4.

Legal & Administration			
Contacts	Tel:(O):	Tel:(R):	Tel:(M):
Responsibilities	▪ Gather facts to ascertain legal implications. ▪ Arrange and coordinate with administrative services required for rolling out the BC Plan.		

5.

Operations Incharge			
Contacts	Tel:(O):	Tel:(R):	Tel:(M):
Responsibilities	▪ Responsible for co-ordinating with all the support departments necessary for implementing the BC Plan. ▪ This could include depending on the business function staff like maintenance staff, engineering staff, installation staff etc. ▪ Would be responsible for rolling out the specific business process recovery as outlined in the BC Plan		

6.

IT Support Incharge			
Contacts	Tel:(O):	Tel:(R):	Tel:(M):
Responsibilities	▪ Though this team could be part of the Operations team, however acknowledging the importance of IT in today's business a special note is made. ▪ Would be responsible for rolling out the IT BC Plan		

7.	Key Process Owners			
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	▪ Co ordinate with the BCP Team leader. ▪ Co ordinate with the operations team and provide directions and guidance to roll out the specific Business process recovery procedures.		
8.	Disaster Recovery Manager			
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	▪ Co ordinates and initiates Disaster recovery procedures for different business functions once the initial BCP is put in action.		

While constituting the BCP team, one of the good principles to adhere to is that "those who plan must also be those who execute the plans." The principal advantage of this principle is that when execution takes place, it does not happen as a text book knowledge implementation but has the benefits of the person being personally committed to making it a success.

16.7 MAINTENANCE OF PLAN

Like every other plan document, BCP and DRP will also go out of date with the happening of a variety of events starting from something as trivial as settings on a set of routers having changed to something as major as a migration from one platform to another. Also, external factors could have an influence on the relevance or otherwise of the BCP and DRP. A workable procedure for maintaining the plan current needs to be developed and implemented.

The plan maintenance will be carried out after every test, on addition or withdrawal of business processes, on change or resignation of team member(s) or change in business logic / focus. Additionally, the internal / external information systems auditor will be responsible for a quarterly review and will suggest changes, if any such are applicable. Business Heads will also suggest changes in the Business Continuity Plan in the event of a new development that substantially affects the existing Business Continuity Plan. New developments can be changes in the business processes, acquisitions, mergers or spin off's of business units.

16.8 REVIEW AND APPROVAL OF PLAN

The BCP Team Leader will review the Plan after every test, on addition or withdrawal of business processes, on change or resignation of team member(s) or change in business logic / focus. In addition, it will also be reviewed in the event of any new development impacting the previous Business Continuity Plan. In such cases it will be reviewed within 30 days after such a change occurs.

16.9 BUSINESS IMPACT ASSESSMENT

Business Impact Analysis or Business Impact Assessments (BIA) is conducted for a number of purposes, the principal amongst them being:

a. To identify essential operations that needs to restart as soon as possible after the disaster has occurred
b. Establish how soon should essential or business critical operations have to restart after the disaster has occurred such that the business does not lose its strategic competitive advantage, lose customers, violate statutory or contractual obligations and minimize financial losses
c. Identify minimal resources needed to restart business critical operations and also identify the roll back point to which operations have to revert for ensuring orderly and complete restart of business critical operations
d. Evolve methodologies to assess the impact of operational discontinuity and the loss of critical business operations
e. Establish a process to assess the severity of impacts

Some key issues that need attention in the planning and conduct of BIA are:

a. An important key step before freezing the prioritization of operations for BIA purposes is to carry out interviews with operating personnel in the following departments / processes apart from information technology, manufacturing, packaging, quality, compliance etc.:

   i. physical security
   ii. health, safety and environment
   iii. building and equipment maintenance
   iv. emergency call outs – electricians, plumbing, air conditioning
   v. emergency call outs – police, medical help and fire
   vi. transport and logistics; especially if the location under consideration is dependent on organizational transport system and not well connected by public transport
   vii. mail collection and delivery

b. Interviews to collect information for BIA should be conducted in person rather than by telephone. This has the advantage that the interviewer can observe a lot of things in while in operation, which might be overlooked when interviewing over phone. In addition, the following are benefits of a personal interview:

   i. Personal interviews hold the interviewee's attention longer and he is more focused while responding to queries
   ii. The interviewer can ask supplementary questions based on the responses obtained
   iii. Can get leads that could generate additional appropriate inputs for the BIA

   There are of course situations where telephone interviews are to be used to:

   i. gather additional information from an interviewee already met
   ii. seek follow up questions or clarifications where conflicting or incompatible data has been provided by different interviewees on the same process

c. Interviews are to be fully pre-scheduled so that interviewee managers are fully aware of what to expect in the interview; this in turn gives them the time required to prepare

d. It is important to record the results of the BIA interview in a consistent manner. This is often achieved by having a structured format for recording results of the interview. It may also be worthwhile to go through a structured process of validating the data collected using statistical validation methods

e. Where more than one interviewee has referred to the same business operation as impacting operations, such operations or processes need special attention while evolving BC and DR strategies.

The primary purpose of BIA is to determine what would happen if a business process or operation were interrupted or stopped. With a view to having focus on this issue, the following practices can be considered for adoption:

a. Assess each of the operations constituting a business process cycle with a view to determining its impact on one or more of the other operations should the process under consideration fail or perform below optimal or accepted levels

b. Assess the severity of the impact of each of the processes should it fail. The impact would be determined not in absolute terms of that process failing or under-performing but in relation to its overall impact on all other related operations as well.

One of the key outcomes of a good BIA is the determination of Maximum Tolerable Downtime (MTD) in respect of each of the business operations considered for BIA. MTD, also referred to as RTO (Recovery Time Objective) or MAOT (Maximum Acceptable Outage Time) is the maximum time for which the business process or routine under consideration can continue to be unavailable without loss of strategic competitive advantage. What constitutes strategic competitive advantage is often determined by the positioning of the business entity and the business segment in which it operates.

In addition to providing clear and quantifiable value MTD for each of the key business processes, BIA interviews carried out well will also lead towards the computation of RPO (Recovery Point Objective) values which point to the best point to which

recovery should point in the event of activation of the DR Plan. The current state of back up processes and the time interval between the process and back up influences RPO values.

A typical BIA worksheet should minimally have the following information:

a. Identification and description of the business process considered
b. List of all the inputs that are required to carry out this process correctly and completely together with a list of all business processes that provide these inputs
c. Process logic that influences the completion of the process correctly
d. The extent of controls over these inputs that enter this process or influence this process. If the input comes from outside the system, what is the contractual or legal binding on the outside system that provides the input
e. Description of all the output that are delivered by this process and their criticality. If the output from this process influences the criticality of another process, that criticality will significantly influence both the RTO and RPO values of the process under consideration
f. Does this process have any interface with any statutory or contractual obligation and have such obligations been factored into RTO and RPO computations
g. Description of the impact of the process failing or performing below expected levels. The more comprehensive this description is the better for the planner
h. Criticality ranking of the operation – normally based on RTO values
i. Comment on any variables that has not been quantified for RTO and RPO computations

Ownership of Business Process

Ownership and accountability for processes helps to ensure that adequate care is taken for the maintaining the process. With this objective owners of business processes have been identified and assigned with the responsibility for the maintenance of appropriate security controls. This responsibility for implementing

security controls may be delegated but the accountability shall remain with the nominated owner of the business process.

Classification of Business Process

A business comprises of numerous processes. Not all processes are accorded with the same importance. Consequently, classification of business processes into categories is necessary to help identify a framework for evaluating the business process's relative value and the appropriate controls required to preserve its value to the organization.

For this purpose four basic classifications of information have been suggested as explained below:

Class	Description
Very Critical	The process forms the heart of the business function. If the process fails it will cause a complete disruption of business activity.
Critical	The process is critical and the failure will seriously impede the business activity
Important	The process if affected will affect the business activity but will not cause serious concerns.
Normal	It's a normal process and the failure will not affect the business activity.

To achieve this purpose, upon creation of the information (whether in a computer system, memo in a file cabinet etc.), the creator of that information (generally the information asset owner) is made responsible for immediate classification. This immediate classification assists any recipient of the information to appropriately safeguard its value to the organization against unauthorized disclosure, loss of availability, and loss of integrity. Further the owner of information asset made responsible to review the classification of information at least annually for possible reclassification.

Valuation of Business Processes

In order to identify the appropriate protection for assets, it is necessary to assess their values in terms of their importance to the business or their potential values given certain opportunities. The values have been assigned considering the cost of obtaining and maintaining the asset, and the impacts the loss of confidentiality, integrity and availability could have to the business. In order to consistently assess the asset values and to relate them appropriately, the following value scale has been applied.

Rating	Description
1	Assets having **negligible** importance to the business or their potential values given certain opportunities.
2	Assets having **low** importance to the business or their potential values given certain opportunities.
3	Assets having **medium** importance to the business or their potential values given certain opportunities.
4	Assets having **high** importance to the business or their potential values given certain opportunities.
5	Assets having **very high** importance to the business or their potential values given certain opportunities.

16.9.1 OUTCOMES & DELIVERABLES

A good BC Plan makes a good understanding of the organizations' most critical objectives , priorities of each processes and time frames for resumptions of these following unschedules interruptions.

- Agree with management on the key business processes that have to be restored in case of a disruption.
- Inform management and agree on Maximum Tolerable Outage for each business process.
- Outline dependencies that exist both internally and externally to achieve critical objectives.

16.9.2 RISK ASSESMENT REQUIREMENTS

Following ***'Requirements'*** have been considered while performing Risk assessment.

- The unique set of security risks, which could lead to significant losses in business, if they occur. This depends upon the risks associated with the business process and the level of criticality of these processes to the organizations business.
- The statutory and contractual requirements which have to be satisfied by the organization which includes government regulations, directives of trade bodies, statutory compliances, HO Directives, Intellectual Property Rights, safeguarding of organizations records and data protection and privacy.
- The requirements relating to the organization-wide principles, objectives and requirements for different processes to support its business operations.

16.9.3 IDENTIFICATION OF THREATS & VULNERABILITIES

As important as having a Business Continuity Plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. Identifying the nature of individual threats, their source and probability of occurrence is the next step considered for the risk analysis process in the context of business disruption. The unique set of threats and vulnerabilities, which could lead to, business disruption if

they occur, have been identified. Multiple threats and vulnerabilities associated with one asset are considered in the risk assessment process.

16.9.4 ASSESSMENT OF SECURITY REQUIREMENTS

For proper and objective measurement of risk it is necessary to assign a value for all identified risk requirements.

16.9.5 Assessment of Threats and Vulnerabilities

Adopt the following Rating for the assessment of Threats and Vulnerabilities

Threat Likelihood Assessment Table

Level	*Description*
1	***The threat is not likely to occur or the probability is "LOW"***
2	***Likely to occur once in ten years or the probability is "MEDIUM"***
3	***Likely to occur more often or the probability is "HIGH"***

Vulnerability Exploitation Assessment Table

Level	*Description*
1	***Highly probable or probable – it is easy to exploit the vulnerability. Protection is either absent altogether or is ineffective.***
2	***Possible – the vulnerability might be exploited, but some protection is in place.***
3	***Unlikely or impossible – it is not easy to exploit the vulnerability, good protection is in place.***

Assessment of Statutory and Contractual Requirements

Adopt the following Rating for the assessment of Statutory and Contractual Requirements

Statutory and Contractual Requirements Assessment Table

Rating	*Description*
Low	***Non-compliance of, which will not affect the business, it will be normal.***
Medium	***Non-compliance of, which can result in business losses affecting part of organizations business.***
High	***Non-compliance of, which can result in heavy business losses affecting whole organization.***

Assessment of organization-wide Principles, Objectives and Business Requirements

Adopt the following Rating for the assessment of organization-wide Principles, Objectives and Business Requirements.

Legal, Regulation and Contractual Requirements Assessment Table

Level	*Description*
Low	***Asset, which if removed / destroyed will have no impact on business.***
Medium	***Asset, which is quite useful for the business but business, will not shutdown without that asset.***
High	***Asset, without which business will come to halt.***

RECOVERY & CONTINUITY STRATEGY – DEVELOPMENT AND IMPLEMENTATION

BCP and DRP success depends on the choice of the right set of strategies and development of appropriate strategies is influenced by the results of BIA, the values for RTO and the recovery points (as determined by RPO and influenced by the back-up policies in place.

The common practice appears to be the development of three to five alternative BC and DR strategies and the business continuity management team presents it and discusses with executive management on what is appropriate. Each strategy should be a complete or near complete solution in itself and equally important is the premise

that each of the strategies should be worked assuming full disaster that will result in a total loss of information and other critical assets. While providing alternative strategies, it must be borne in mind that successful implementation of BCP and DRP also depends on the allocation of budgets. When a situation is being considered for faster recovery or a change in the criticality rating, it is essential that the additional cost be factored into the final choice of the strategy. It is better to have a working strategy that has complete budgetary allocation though it might be sub-optimal rather than have an ideal strategy that has no budgetary support and hence, when the strategy has to be implemented in the case of a disaster or business discontinuity event, it is not fully implementable.

While finalizing strategies for achieving BC and DR, the process of identifying more than one alternative for each of the following major requirements need attention:

1. Alternative premises

i. Hot site – this is considered to be a location, which is as ready as the main location is. This could either be company owned or could be hired from third party who supply such services. Hot sites provide fully configured computer facilities with power, HVAC, operational file and print servers and workstations. Applications are kept loaded on the systems in the hot site and mirror the regular production environment. Ideally, when a need arises, users should be able to walk in, pick up the latest back up data available and start processing with minimal loss of time. The principal advantage is that it has least gestation time to come to production while the greatest disadvantage is that it is very expensive to maintain.

ii. Warm Site – Though no theoretically rigorous definition exists for this form of recovery alternative, it is understood in the industry as a configuration that is less ready than the hot site. Often, warm sites have the premises with HVAC fully in place and may have the print and file servers in place but may not have applications loaded. This is often the case with vendors who offer third party warn site services that is shared by many clients who have almost similar production environment.

iii. Cold Site – Perhaps the most common form of alternative premises strategy; yet also the most ineffective form. In this case all that is

available is the premises along with HVAC. The biggest danger in this form preparedness is that, in the minds of an uninitiated manager, this can provide a false sense of security.

a. Office computers and equipments like PCs, back up data, recording media, etc.
b. Any specialist equipment like special printing machines, hologram makers and readers, etc.
c. Furniture and fixtures in case the arrangement at the alternative premises does not cover the provision of furniture and fixtures
d. Documents and Stationery – in particular any special stationery like security printed stationery, pre-numbered or pre-authenticated forms, forms with franked signatures or other forms of authentications, etc.
e. Link to communication services either through back up links or wireless services or through a forwarding service, etc.
f. Transport, logistics and delivery services covering all activities that need to be covered during operations at alternative premises

Testing the Plans

An untested BCP is no BCP at all! The strength of a BCP or a DRP is that it must be fully operational and meet the requirements of RTO and RPO completely in the event of a disaster or a business discontinuity event. Given that the BCP or DRP will be called into implementation without any notice, there is a strong need to keep it up to date and also ensure that it reflects the current set of assumptions and conditions. Also, BCP will go out of date like any other plan will and hence the need to maintain it on a regular basis to reflect the current configuration of information systems and business processes.

The most common test strategy in BCP or DRP is to start off by testing components of the plan separately and combine components progressively into a reaching a stage where a complete test would be carried out covering the whole of the BC and DR plan.

Well-planned tests give better results than those done on an ad-hoc basis. Greater the efforts put into planning BCP and DRP tests result in reduction of time and efforts

involved in testing the plans and also ensures that acceptable level of results are available in fewer tests. Testing, as a process, is never a failure since however badly a test is carried out, it still provides a number of lessons for the BC and DR team. While stating that no testing process will be a failure, it is equally important to realize that badly implemented tests can cause a disaster by themselves!

The success of testing lies in the way the team answers the question – what needs to be changed as a result of the test results obtained. Five types of testing are normally considered while planning the testing process. Each of these are graded to represent different levels of intensity of testing and provides assurance of different combination of components of the BC and DR process:

The simplest form of testing is checklist based testing. Often dubbed as armchair testing, this process has the lowest complexity in planning and implementation and a very low participation level from the participants also. In this case, checklists are prepared comprising the various activities to be carried out by each of the participant in the test process and the checklists are handed to them. Participants are requested to review the checklists and get familiar with what needs to be done. The assumption is that they would be ready to implement what needs to be done when a real disaster or a continuity-threatening event occurs. That is a very questionable assumption.

A form of testing called structured walkthrough is a good starting point for most BC and DR testing processes. In this process, all participants sit around a table, and discuss the actions that must be triggered under different scenarios that point to a disaster or a business discontinuity. The discussions usually moderated by the BCP Coordinator will usually clarify any gray areas in the implementation of the DRP and BCP. This will serve as a session where the participants proposed membership of different teams will get greater clarity on their roles in those teams. Often it takes the form of a quiz where the moderator or session chair throws out, at random, scenarios that will warrant the trigger of BCP / DRP and elicit response; evaluate the response and guide the discussion towards interpreting the response to assess its relevance to the scenario.

A third form of testing is referred to as Simulation Testing. The primary objective of this form of testing is to determine the efficacy of the human elements when they are called in to respond to a disaster. This form of testing does not test the response of

the DP systems and procedures in the recovery process; instead it presumes the availability and efficacy of DP systems and procedures involved in the disaster recovery process and checks if the relevant human elements – both at the key production departments and support services – can rise up to the occasion should a disaster occur. In this case, a 'disaster' is declared and the response process and time take to respond is tested. If the recovery support personnel are not able to facilitate the recovery within the RTO, personnel who did not meet the RTO requirements are re-visited, re-trained and re-tested for fine-tuning. In case the of processes that have not met their RTO/RPO, test professionals first and foremost determine if the failure can be attributed wholly and exclusively to a failure or non-availability of a related IPF assets and if so, that is considered at the next stage of testing after appropriate fine tuning of those systems.

The fourth form of testing is the parallel testing which does all that is done at the simulation test stage and all the IPF elements are also brought into play. In this form of testing, the declaration of a 'disaster' results in the recovery personnel and systems and processes being initiated and goes right up to the implementation of recovery strategy and parallel processing started at the alternative site if that constituted the recovery strategy. In this form of testing, excepting the fact that the principal production site is not shut down, every thing else happens as though the DR Manager or such other person who is empowered to declare a disaster, has in fact declared a disaster. While this is an expensive form of testing, it has the advantage of simultaneously testing, all components of DRP and BCP as appropriate. Another advantage of this form of testing is that, since the principal production site is operational, results of processing of information at the recovery site and at the production site can be compared. If the results are comparable and it has been achieved within the RTO, it can be reasonably concluded that the DR plan has met its objective. However, if the failure of the systems and processes point to an inherent deficiency in design or to an architectural failure, it clearly points to the need to re-visit the systems and processes in the light of recovery requirements.

The fifth and final form of test, which has to be handled with great care and caution, is the full interruption test. In this form of test, the DR manger declares a disaster and the production systems are interrupted or shut down as though a disaster really occurred and the DRP is triggered into action. The primary advantage of this form of testing is that it tests the efficacy of DRP / BCP under 'real-life' conditions of a disaster and can be a effective way of ensuring that the DRP and BCP will deliver what it is expected to deliver. In this form of testing, the recovery process is closely

monitored for determining that the RPO and RTO are fully met. It will throw out even minor bottlenecks in the implementation of the plans that could snowball into a major impediment later. Corrective action after this form of test adds significant value to the BC and DR process. However, this form of test has to be handled with adequate care since a badly planned full-interruption test could, by itself, trigger a disaster!

The test process is not complete until the test manager or the DR/BC coordinator completes a set of follow up action based on test results. Firstly, the test process owner has to communicate the test results and its interpretation to executive management. Secondly, the test process owner or BC/DR manger or the test manager will prepare a list of follow up actions required as a result of the test results. The follow-up actions very often result in one or more of the following:

- Changes to plans
- Changes to teams
- Revisit technology assumptions
- Revisit contractual arrangements
- Retrain the team members

The above list is illustrative and a wide range of follow up results is possible.
The follow up as a result of test results required executive management approval especially when it involves change to plans and / or changes to recovery strategy.

Maintenance of BCP and DRP

Like all other plans, BCP and DRP will get out of date due to a variety of conditions and circumstances. DR / BC mangers will do well to create and update a list of circumstances and conditions under which updates are required to BCP and DRP. This is in addition to ad-hoc situations and events that warrant an update to BCP and DRP which will be identified either by the BC / DR coordinator or user mangers who believe that changes in their operational domains warrant a change to BCP / DRP.

Updating and maintenance of BCP / DRP is to be regarded as a systematic process that requires a planned and consistent response. Like all other processes that is changed using a change management process, BCP / DRP changes are also subject to the same rigor of change management.

BCP / DRP requires the same degree of version control as in the case of other business critical documentation. It is often very difficult to envisage a situation where BCP / DRP will be only in soft format or available for review and download via a web interface. There are strong reasons to keep it in hard format; as written documentation. This adds to the necessity for a clear and meticulously implemented version control process. There is no need to elaborate on what would happen if there were different versions of a BCP / DRP in different locations of an organization. Such a situation is a sure recipe for disaster. A standard practice is to ask Internal Audit to check of version compatibility of all copies of BCP / DRP they come across in the course of an audit of the organization.

BCP & DRP – Awareness and Training

While testing provides a form of awareness and training on the implementation of BCP and DRP for those involved in the testing process, awareness and training of BCP and DRP has to be at all levels in the organization.

It is recommended that organizations create both awareness and training processes covering all human resources in an organization. While awareness is all about knowing the reality, training is a more proactive process of building proficiency in the participants. Successful implementation of BCP and DRP requires both awareness and training of all those who are involved in the organization's business process. A typical BCP / DRP awareness program should consider minimally covering the following:

- Why are BCP and DRP important and relevant?
- Components of BCP and DRP
- Who coordinates BCP and DRP activities?
- Where do you find more information about BCP and DRP
- When and how are BCP and DRP activated?
- How are BCP and DRP exercised?
- What can you do to make it more effective?

In addition to formal programs for awareness and training on BCP and DRP, it would be a useful practice to get executive management representatives to periodically demonstrate or reinforce their commitment to BCP and DRP in various forms – a

mention in newsletters; a reference in other corporate communications; a poster campaign with message from executive management; and the like.

When a disaster or a continuity-threatening event does occur, it is the people in the organization who have to implement the elements of BCP and DRP. It is one thing to get people to do it because they have been told to do it and it is a totally different thing to do it because they are convinced about its tremendous utility for all players in the organizational system; including themselves. This is also a reason why it is strongly advocated that those who plan must also be those who do.

17 LEGAL AND REGULATORY COMPLIANCE

17.1 INTRODUCTION

Compliance to legal and regulatory requirement is of paramount importance for enterprise. Its non compliance is not only limited to monetary impact but it also results into penalty, loss of reputation, market share and customer trust.

Legal aspects are complex and they are specific to country/state/industry. Some countries have stringent data protection rules. Some industries (e.g. financial services, government and pharmaceuticals, SEC registered clients) have particular requirements.

17.2 PRE-REQUSITES

Documents relating to requirement identification for compliance to local, regional and fedral/central laws, internal and regulatory compliance

17.3 OBJECTIVE

- To identify legal and regulatory requirements for the enterprise
- To ensure that enterprise is compliant with legal and regulatory requirement

17.4 ASSESSMENT QUESTIONNAIRE

This section contains a set of suggested evaluation check list that are expected to broadly fit the ISSAF based assessment process. Recognizing that each organization has its own unique processes, technologies and information processing architecture, it is possible that the ISSAF evaluation may need further steps to be performed. It is also possible that some of the suggested checks may need amplification. The assessor who is carrying out the ISSAF based evaluation should therefore use these check lists as guides and evolve a process that best fits the organization being reviewed.

	Evaluation Check	Yes	No	N/A	Evaluation Performed and Results
1	Compliance Department				
1.1	Is there any formally assigned/approved compliance department/officer within the enterprise who ensures legal and regulatory compliance requirement?				
	Does the said Compliance Office posess formally recognized certifications or accreditations to handle compliance? For instance is he enrolled before the bar, etc?				
1.2	Is there any procedure in place to identify legal and regulatory compliance need?				
	If such a procedure is in place, is such identificaiton done on a periodic basis or is it triggered by given set of events; both internal and external to the organization?				
	In case the procedure to re-visit legal or regulatory compliance is triggered by events, is there a list of such events available for review?				
1.3	Has the enterprise been reviewed indepenedently for compliance to legal and regulatory requirement? Is such compliance review part of a clearly definied managerial prerogative or is it mandated by any certificaiton or accreditation that the organization enjoys?				
1.4	Has the outsourcer been reviewed indepenedently for compliance to legal and regulatory requirement with respect to service provided?				
	Does the agreement with the outsourcing service provider provide for an independent audit / verificaiton of their security or is such audit / verificaiton done on a case to case request basis?				

	If the outsourcing agreement provides for regular audit of the infrastructure security, what were the major findings in the last audit and how were such findings handled to ensure appropriate security?				
1.5	Has the legal and regulatory policies and procedures been communicated to concerned people/departments?				
1.6	Does the organisation have a formal process to track and understand current and expected legal and regulatory compliance requirements? And is there any process for its continious improvement and enhancement?				
1.7	If the enterprise relies heavily on third party systems and applications, does it involve any proprietary software or solutions? If so is an escrow agreement in place covering the proprietary software and solutions.				
1.8	Are there any policy and procedure in place to collect, handle, store, maintain chain of custody of evidence in relation to posibilly law suit against a person/organization?				
1.9	Does the informaiton system log activies to be produced in court of law as evidance?				
1.10	Has the enterprise addressed concerns related to copyright, licensing, trade marke, patents and other forms of intelectual property generated or used by the organization?				
1.11	Does the organisation having a proactive process to manage software licensing?				
1.12	Is there any policy and procedure to address enterprise's need to protect its own intelectual property?				
1.13	Has the enterprise registered its internet domain names with trusted domain name provider?				
1.15	Is the role of Data Protection Officer assigned with responsibility for data protection compliance ?				
1.16	Does the DPO guide managers, users and service providers on their responsibilities?				

1.17	Has the enterprise taken steps to proactively review legal and regulatory requirements to ensure that they can be readily integrated into the organisations current working practices?				
1.18	Does internal audit department cover compliance functions when performing their reviews?				
1.19	Does the legal and regulatory policies/process support regular co-ordination with other legal and regulatory departments with respect to changes in requirements? Also does the system development and project team ensure that legal and regulatory requirements are considered?				
1.20	Is the user / owner of systems trained/ made aware of the relevant legislative requirement?				
2	Is the outsourcer reviewd/audited by an independent third party?				
3	Has there been any independent review/audit of enterprise's informaiton system? If so does previous review cover all the major domains mentioned in ISSAF?. If that's don't is the previous two years reports can be producted for review?				
3.1	Have the corrective measures been implemented following the findings of these reports?				

17.5 Assessment Questionnaire - Narrative

The following narrative supports the understanding of the contents and logic that is embedded in the assessment questionnaire. While the questionnaire is structured on the basis of possible process flow that may be found in many enterprises, the narrative is presented to aid an understanding of the concepts covered in this domain.

[coming soon]

17.6 Legal Aspects of Security Assessment Projects

Legal aspects of information technology are very complex in nature. They vary from country to country. It's a new field; many countries don't even have any legal framework for IT. Even in countries which have a legal framework, it is not mature enough. Legal frameworks are evolving based on cases. People involved in these processes have lack of knowledge.

These legal issues arise due to following reasons:
A. The lack of knowledge on the part of parties involved of legality
B. The lack of knowledge of judges about subject
C. The lack of knowledge of investigating agencies about subject

Certain aspects need to be considered before engagement in information technology Security Audit/Ethical Hacking projects:

- Pay local duty of the country under whose jurisdiction the contract is signed. This will help in taking offence in a court of law if any infringement occurs. Though to have an agreement on the letter head will be sufficient evidence for defense. For example one signs an agreement for Penetration Testing on a letter head can not sue for non payment of fees (offence) but on the other hand one can defend himself for completing scope of work as decided in the agreement
- If agreement is in electronic form these agreements should be digitally signed
- This also differs from country to country. You will find some countries like Singapore where electronic signatures are held to be valid

Domain covered

- Legal aspects of scanning
- Legal aspects of Exploit Code
- Legal aspects of Privacy

Domains yet to be covered:

- Legal aspects of Encryption
- Legal aspects of Copyright, Patent
- Legal aspects of Data Import and Export Restrictions
- Legal aspects of Trade Secrets

- Legal aspects of National Security

17.6.1 Legal aspects of scanning

Scanning is widely held to be a malicious activity. If scanning is done in the course of duty it is legal. However legal process requires a lot of time and money. In some circumstances people doing it on duty were arrested, though they were released later after complex legal processing.

To start an assignment without a legal agreement may result in a big problem. Always sign a contract.

The **US Computer Fraud and Abuse Act Section 1030(a)(5)(B)** has six elements which have to be proven by the prosecution:

A. The defendant intentionally accessed a protected computer,
B. The defendant did not have authorization to access the computer
C. As a result of the access, the defendant recklessly caused damage
D. The damage impaired the integrity or availability of data, a program, a system, or information
E. That caused a loss aggregating at least $5000 or
F. Threatened public health or safety

In November 2001, a federal US court has dealt with the issue of port scanning in the case of Moulton vs VC3.

Scot Moulton, a network security consultant was contracted to service and maintain port 911 (it's an address not TCP/UDP port) centers network. He was charged and arrested under the US computer fraud and abuse act when he port scanned the 911 center computer network.

The system network administrator noticed the port scan activity. He emailed the defendant questioning his motive for scanning the port. The defendant then quit the scanning (which according to prosecution was suspicious behavior) and emailed the system administrator back that he was doing so under the service contract.

The defendant claimed that he was performing a series of remote port scan to check security of network between the sheriff's office and the 911 center. The prosecution denied that he had access to the ports but admitted that Moulton caused no structural damage. The defendant was held not guilty since no damage was caused.

The point to be noted is that the contract for service and maintenance should grant enough scope to ensure the authority to conduct the scanning

In certain cases it can be said that port scanning creates legal liabilities. It can be proven that it was a preparation for an offence.

The scan is considered malicious when the intention is to reveal vulnerability in the target. A scan looking for a Trojan port (e.g. sub7, netbus, bo2k) would be construed as malicious.

If a scan is performed by Virus/Worm/Trojan from a system in one organization to another organization or within an organization or one system to another system, it will have to be proved that there was no malicious intention in running the Virus/Worm/Trojan by the owner of the system.

In the Indian IT act the owner of the system is responsible for the scanning (Port/Host) by a Virus/Worm/Trojan. In this case the owner of the system is guilty of not exercising due care and due diligence and lack of malicious intent has to be proven in the court.

As per the Indian IT Act 2000 whoever

- with the intent to cause or knowing that he is likely to cause
- wrongful loss or damage
- to the public or any person
- destroys or deletes or alters any information residing in a computer resource
- diminishes its value or utility
- affects it injuriously by any means

commits hacking

What would be my criminal liability, if I scan a wrong target by typo mistake or any other unintentional act?

E.g. suppose I was to scan a target 200.1.1.1 and by mistake I typed 200.1.1.2, what are the consequences?

Criminal liability is largely dependent on intention (mens rea). A bonafied mistake may not invite criminal liability, unless the mistake has resulted in a negative consequence (that is a loss in whatever manner), in which case the court may order restitution or damages to undo the loss. For example if in the scan quoted in the question results in loss of 50000 RS, you may have to pay the amount as compensation. However you are not likely to be jailed for scanning the other target. **Still you may be behind bar till the time prosecution is on and jury gives their judgment.**

Can I approach a court of law for amending an existing law for the better?
Answer is No. Making law (Legislation) is the duty of the govt. Court will entertain only a challenge to the provision of law which is against any provision of the constitution of the country or of any other valid existing law. E.g. you want to give your input in criticality of scanning the court will not entertain it. However suppose certifying authority has power to reject your application for digital signature certificate without hearing you, you could challenge this provision as arbitrary and unconstitutional.

What is the difference between Penalties and Offences?
Penalty for damage to target (Computer/Network) is levied irrespective of the intention. It is computed in terms of money to be paid for crossing the forbidden line. Offences which relates to hacking invites jail term as well. However in the later case the intention of the hacker plays a major role. This involves jail or penalty or both. The intention involved in crossing the forbidden line plays a big role in deciding the quantum of jail term as well as damages.

17.6.2 Legal aspects of Writing/Publishing Exploit Code

[This section is intentionally left blank]

17.6.3 Legal aspects of Privacy

[This section is intentionally left blank]

ANNEXURE - KNOWLEDGE BASE

[This page is intentionally left blank]

1 TEMPLATES AND OTHERS

1.1 IT INFORMATION GATHERING – SAMPLE QUESTIONNAIRE - I

1.1.1 Overview

Client Organization						
Assessor Organization						
Nature of Business						
Group/Division/Sub Division/Entities						
Engagement Reference						
Client's Turn Over	Overall			Group		
IT Budget	Overall			Group		
IT Security Budget	Overall			Group		
No. of staff	Overall		IT		IT Security	
No. if Internal Audit Staff	IT			Non IT		

1.1.2 Engagement Information

Engagement Director	Client Organization							Assessor Organization	
Engagement Manager	Client Organization							Assessor Organization	
Engagement Duration	d	d	m	m	y	y	Engagement Duration		

1.1.3 Understand Business

Organization business, how they function, organizational structure, revenue stream etc…

1.1.4 Understand IT Environment

Sr. No.	Evaluation check	Evaluation performed and results
	1.1.4.1 GENERAL INFORMATION	
	Does the organization outsource some functions e.g. IT operations, systems development, web development, hosting, Internal Audit etc…	
	What are the hardware platforms is in use? Include Centralized and Decentralized IT and e-commerce.	
	What are the types of operating systems is in use?	
	What are the types of database	

	systems is in use?			
	What are the applications is in use that supports key business processes? Industry standard like HP open view, oracle e-business suite and organization specific e.g. in banking environment Banksys, Swift, in-house developed applications etc…			
	Name	Supplier/In-house	Key business process	Date – Developed/Implemented

1.1.4.2 Understand Network Environment

	Evaluation check	Evaluation performed and results
	Network architecture design: LAN/WAN network diagram, their connectivity etc…	
	Does the organization having server level operating system standard?	
	What other server/mainframe level Operating Systems available?	
	What types of network protocol(s) are implemented?	
	Does the organization having desktop level standard?	
	What type of WAN is implemented and how many sites participate in this WAN?	
	What types of network elements (NEs) might be found?	
	What protects remote connectivity?	

1.1.4.3 Understand information security state

2.1	Does the organization have formal and documented security policies, procedures and plans? And are they available for review?	
2.2	Does the organization have formal information security organization?	
2.3	Does the organization have formal plan for business continuity and disaster recovery?	
2.4	Does the organization implemented firewalls and if so it's of which kind?	
	Does the organization implemented intrusion detection system (IDS) and if so it's of which kind?	
2.5	Does the organization intrusion prevention system (IPS) and if so it's of which kind?	
2.5	Is the basic physical controls (guards, barriers, PACS, CCTV, badges, etc…) are in place?	

1.1.4.4 UNDERSTAND COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENT		
	What are the legal and regulatory compliance applicable to organization? e.g. Sarbnes-Oxley, HIPAA, GLBA, FMA etc…	

1.2 IT INFORMATION GATHERING – SAMPLE QUESTIONNAIRE - II

1.2.1 Background Information

a. How many employees are there in the organization?

   i. What was the average growth in employees over the company's history?
   ii. What was the growth rate for the last financial year?
   iii. Which function has the most employees?
   iv. Which function has the least number of employees?
   v. How many employees currently use information systems?

b. How many customers does the company have?

   i. How many transactions with customers per day on average?
   ii. What is the ratio of cash to credit transactions?
   iii. What is the ratio of regular to one-time/non-regular customers?
   iv. How is the credit approval process managed by the organization currently?
   v. How are cash receipts managed by the organization currently?
   vi. How is the collection scheduling process setup internally? What is the current A/R cycle?
   vii. Who is responsible for invoicing the customers? How do they do this right now?
   viii. What is the average sales per year in local currency?
   ix. What is the history of bad debts over the recent history?
   x. Is e-Business being conducted with any customers at present?

c. How many vendors does the company have?

   i. How many payments to vendors and consultants per month?
   ii. Is e-business conducted with vendors?
   iii. Average payment to vendors?

d. How many Geographic locations does the company operate from at the moment?

   i. How many of these locations are currently connected by a network?
      1. How many of these locations have their own systems for data processing?

2. How many of these locations depend on outsourced services for data processing?
3. Which of these locations carry out business critical functions. What do they do?

ii. What are the roles of the other locations not covered by the network?

e. Materiality related information from the last audited financial statements and current records

i. Balance sheet accounts
   1. Current assets
   2. Total assets
   3. Current Liabilities
   4. Long term liabilities

ii. Income statement
   1. Revenues
   2. Cost of sales
   3. Gen and Admin exp
   4. Operating Income/Loss

iii. Cash flow
   1. Net cash flow

1.2.2 Pre-fieldwork meeting with the IT management and/or team

1. IT employees
   i. Who is responsible for managing IT? What are their responsibilities?
   ii. Has the IT manager turnover been high in the history of the organization? Reasons?
   iii. Are there separate systems, applications, and help desk departments? Any other depts.?
   iv. How many IT employees?
   v. How experienced are the IT staff members? What training have they received in the company?
   vi. How much turnover were there in employees over the last few years?
   vii. What is the hardware in place (very brief descriptions only, more detail only if audit is required).
   viii. The software (very brief description, more detail later if required).
      - Any in-house development?
      - Any contract / outsourced development?
      - Any consultant contributions?
   ix. Internet and Website (very brief descriptions, more detail later if required).
      - Any in-house development?
      - Contract web site development with consultants?
   x. E-Business?
      - Hosted in-house or web hosting company?
      - Transaction processing hosted on website?
      - Credit card processing processed on systems or outsourced?
   xi. Who manages the network?
      - Design
      - Development/Systems Integration
      - Deployment

- Maintenance
- Upgrades
- Troubleshooting
- Security Administration

xii. Business applications

- Any in-house development?
- Any contracted development?
- Any consultants?
- What is the history of business applications within the organization?

xiii. EDI

- Who is the VAN provider?
- Any in-house development?
- Any third party software components (brief descriptions only)?
- Any contracted development?
- Any consultants?
- What is the volume of transactions handled on a monthly basis?
- What are the type of transactions currently being handled?
- What are the reports that are used to monitor EDI transactions?
- Who is responsible for handling data transfer to/from EDI to applications?
- What are the applications and/or software that send data to/from EDI?

2. Gain a familiarity with internal controls (for larger organizations only)
   a. Review prior year internal audit general control work papers if available.
      i. Are there any significant unresolved items?
   b. Review any new interim management reports since last year's audit
      i. Note any significant unresolved items.

3. Client Personnel

A. IT Managers

- Executive(s) responsible for IT
- Manager(s) responsible for IT
- Systems Administrator(s)
- Network Administrator(s)
- Other(s)

B. Financial Managers

- Chief Financial Officer
- Controller(s)
- Accountant(s)

C. HR Management

- Manager
- Administrator
- Payroll controller(s)

D. Other Department(s) (Fill this section out for each of the other departments)

- Manager
- Supervisor(s) / Administrator(s)
- Line Function (s)

1.2.3 Fieldwork

I - Systems specification

a. Overview
Illustrate using a flow diagram the initiation of key financial transactions from workstation, through the network, to the application server, the application, and how it is processed to the final presentation in the financial statements.

b. Hardware

i. What is the vendor, make, and model number of the system(s) used for recording, processing, and reporting financial information?
ii. What is the current physical capacity of the system?
    1. Memory _____, Hard drive _____, Network ____, Backup drive _____
iii. What is the most current baseline reading for the system? What is the baseline period?
    1. CPU _____, Hard drive _____, Network _____, Memory _____
    2. Other (please describe)
    _____
iv. Where is this systems physically located? What are the physical safeguards for this system?
v. What are the audit features available on this system?
    1. What are the User activities that can be logged? Which ones are enabled?
    2. Is the system logging network activities? Which ones are enabled?
    3. Is the system logging database activities? Which ones are enabled?
    4. Is the system logging application events. Which ones are enabled?
    5. Is the system logging security events. Which ones are enabled?
    6. What are the other logging features available. Describe. Which ones are enabled?
    7. What is the policy for log retention? What is the practice for each type of log?
    8. What is the policy for log backup?
vi. How many workstations are currently logging into this system
vii. Where these workstations are physically located?

c. Financial applications

i. What is the name of the system, the name of the vendor, the name of the local support agency and version of the business application used for processing financial transactions?
ii. What are the business transactions handled by this system?
iii. How long has it been in operation?
iv. How long did it's implementation take?
v. Who managed the acquisition of this system?

vi. Who was responsible for deploying this system?
vii. Who is responsible for supporting the users of this application?
viii. Who manages the vendor updates to this system?
ix. Who is responsible for managing the customization of the system generated reports?
x. Who is responsible for customizing the system to meet changes in business requirements?
xi. Who is responsible for personalizing the system to meet changes in user requirements?
xii. Who is responsible for setting up and managing user accounts for this application?
xiii. How many users are currently setups to use this application?
xiv. Who handles the security for the application?
xv. What is the name and version of the computer operating system on the system? What are the patches that have been applied to this operating system? What are the hardening procedures that have been used to secure this system? What are the current known security vulnerabilities on this system? What are the intrusion detection features that have been setup on this system?

d. Network system

i. What is the name and version of the network operating system used to control access to financial applications? On which system does this network access control reside?
ii. What is its vendor, make and model number? What is it's current utilization for CPU, Network, RAM and hard drive?

e. Is there a WAN (Wide Area Network) used within the organization?
i. What is the operating system used for the WAN?
ii. What is the network protocol(s) used for the WAN?
iii. How many LANs are connected by this WAN?
iv. What are the make of the devices used to interconnect the LAN to the WAN?
v. What is the bandwidth of the circuits used on the WAN?
vi. What is the cost of the total bandwidth used by the WAN?
vii. Where the WAN devices are physically located?
viii. Do any of the LANs connect to any non organizational network and/or the internet?
1. Where is this LAN located?
ix. Is the WAN connected to any other external network and/or the internet?
1. Where is this connection located?
2. How is this connection being protected against unauthorized access?

f. Is there an Intranet being used by the organization currently?

g. Intranet Hardware platform
(1) In-house?
(a) If so, OS and version
(b) If so, which type web server software and version (IIS, Apache, iPLanet, Websphere, etc.)?

h. How many Windows servers are there?
    i. What version of Windows?
    ii. Service pack level?
    iii. What are the patches and/or hardening procedures that have been applied to these systems?
    iv. How many of the known/published vulnerabilities have been addressed to date?
    v. Have the systems been tested against any security threats? Please describe

i. How many UNIX servers are there?
    i. What version of UNIX?
    ii. What are the patches and/or hardening procedures that have been applied to these systems?
    iii. What are the known/published vulnerabilities that have been addressed to date?
    iv. Have the system(s) been tested against any particular security threats? Please describe

Note: Check if any other operating platforms are being used. If so, repeat the above four questions for each platform.

j. What is/are the e-mail system(s) being used by the organization?
k. How many web servers are there?
What is/are the web server software used internally by the organization?
l. What is/are the Database software used internally by the organization?
m. What is/are the firewall(s) in use within the client organization?
n. Is Dialup services available to remote users? What are the solutions implemented for this?
o. Is remote control software available to remote users? Which solutions are in use for this?
p. Is remote file sharing configured for external / remote users? Which solutions?
q. Additional internal control implications
    i. Hardware, operating, and network system
    a. has there been significant changes to hardware, operating, or network software in the last 12 months?
    (1) If so, describe.
    (2) If so, what are the internal control implications of these changes?

    b. has there been any significant changes to the system environment such as out-sourcing, down-sizing, or key staff turnover or re-assignments in the last 12 months?
    (1) If so, describe.
    ii. If so, what are the internal control implications of these changes?

II - Application software

a. What are the financial and financial related records that reside on the system? What are the names (and version) of the applications used to capture, store, process and report these records.

b. Has there been initiation of significant application development or purchase of new packaged software for recording, processing, or reporting financial and related information?

c. If packaged software is used has there been a significant version upgrade of the application?

d. Has there been implementation of other significant applications which may affect the financial software applications?

e. Have there been changes in the user environment?

f. If the answer to any of b. - d. is yes then describe.

g. Did the systems specification section identify any opportunities to improve control?

(1) If so, document how internal control would be improved by these specifications.

h. Did the systems specification section identify any threats to achieving the control objectives?

(1) If so:

(a) Document the threat.

(b) Does the client have a control activity to reduce the risk of the threat?

[I] If so describe the control.

[II] If not, make a recommendation of a control activity to reduce the risk of the threat to an acceptable level.

(c) If not, is the threat and lack of control a reportable condition?

[I] If the lack of control is a reportable condition contact the engagement manager immediately upon that determination.

IV. Consideration of Internal Control in Planning the Audit

A. Control Environment

1. Management style

a. Describe management's philosophy and operating style as it relates to the IT control environment.

b. Describe management's commitment to developing and maintaining a good general control environment.

c. Describe available evidence of senior management involvement in IT and related activities.

d. Is senior management knowledgeable enough to ask the right questions about IT alignment to business?

e. Does senior management hold meetings with IT and financial managers to ensure resolution of serious IT problems?

2. Board of Directors / Committees (For Publicly traded companies / Government organizations etc)

a. Audit committee

(1) Rate the Audit Committee's participation in IT issues. (High, low)

(2) Does the audit committee take an interest in IT general controls?

b. IT Steering committee

(1) Is there an IT steering committee?

(2) Is there a Board member on the IT steering committee?

c. Does the Board or one of its committees spend adequate time developing and reviewing long and short-term IT plans?

d. Does the Board or one of its committees review and approve IT policies and procedures before implementation?

e. Is a report on security violations made to the IT steering or audit committee?

3. Organizational Structure and Delegation of Authority and Responsibility

a. Obtain the organizational chart.

(1) Review the organizational structure.

(2) Does the organizational structure indicate any weaknesses in communication and control?

(3) Are there clearly defined lines of authority and responsibility?

b. Are there written job descriptions for IT managers and staff?

(1) Interview and observe selected IT employees and determine what their job duties are.

(2) Do key IT managers have the experience, training, and education necessary to carry out their responsibilities?

(3) Do IT managers regularly attend IT training and conferences to continually update their skills?

(a) Do IT managers and staff attend IT security training and conferences?

4. Monitoring

a. Who monitors general controls over IT?

(1) How frequently?
(2) Who gets interim general control monitoring reports?
(3) Are there unresolved IT findings reported in previously issued monitoring reports?

5. Personnel Policies

a. Are vacations mandatory for employees in sensitive and IT positions?
b. Is there cross training of employees for key IT positions? Please describe
c. Is there mandatory rotation of job duties for key IT positions? Please describe

6. Integrity and Ethical Values
a. Rate the integrity and ethical values of IT management. (High, low)

7. Conclusion on Control Environment

a. Consider the substance of controls rather than form. Is the control environment taken as a whole as described in 1. to 7. above conducive to a good control environment?
(1) If not ,why not?

B. Management's Risk Assessment

1. Has management prepared a formal risk assessment for general controls considering:

a. objectives?

b. risks?

c. control activities?

2. If so, evaluate management's risk assessment for general controls.

a. Does the risk assessment address general control objectives

(1) If not, which objectives does it not address?

(2) If not, how does the lack of management's risk assessment addressing an objective of internal control over financial information impact our audit?

C. Interviews

1. IT Manager

a. Inquire about long-term and short-term plans to upgrade hardware and software to meet changing technology and growth needs.

b. Inquire about known IT security and control problems and weaknesses.

c. Inquire about areas the IT manager would like to see the auditor address.

d. Inquire about known problems with hardware and software.

e. Inquire with IT manager if in his opinion:

(1) IT personnel are adequately trained?

(2) There is adequate maintenance of IT equipment?

(3) There is obsolete hardware or software that causes problems?

(4) The quality of the work done by:

(a) inside programmers?

(b) outside programmers?

f. Is there a formal process for testing application software upgrades, modifications, and maintenance?

g. Do contracts with outside programmers specify documentation of their work?

h. What percentage of time were system(s) down in the 12 months preceding the audit?

i. What percentage of time was the network down in the 12 months preceding the audit?

j. What percentage of the time was the web site down in the 12 months preceding the audit?

k. What percentage of time was the intranet down in the last 12 months?

l. Does the client have the most current version of the operating system for the platform on which financial information is entered, stored, processed, and reported?

m. Does the client have the most current version of the network operating system?

n. Does the client have the most current version of server software and patch levels?

o. Does the client have the most current version of the application software?

p. What is the financial stability of the application software vendor?

q. What is the quality of technical support for the application software?

r. Have there been any significant employee problems?

s. Is there a history of processing incidents attributable to specific individuals?

t. Does the client have a copy of vendor owned application source code?

(1) If not, is there a copy in escrow?

u. Do in-house programmers, vendors, and contract programmers have access to live production data?

v. How many IT employees have full administrator rights on the system?

w. How many IT employees have full administrator rights on the network servers?

x. Is notification required before vendors make changes via modem?

y. How does IT stay informed of the latest Internet, server, and e-mail vulnerabilities?

z. Does anyone at IT subscribe to e-mail lists from:

(1) CERT?

(2) SANS?

(3) Others (Please provide names)

aa. Is there an up-to-date IT asset inventory list that includes for routers, switches, servers, and
firewalls:

(1) Hostname

(2) IP address

(3) Purpose

(4) Operating system and version

(5) Database type (DB2, SQL, Oracle, Ascii, none)

(6) Name of administrator

(7) Physical location

bb. Is there an up-to-date network diagram?

D. Control Activities

1. Strategic information technology plan

a. Does the organization have an entity wide strategic information technology plan?

b. Has the organization established specific written objectives for use and control of information technology?

2. Information technology organization and relationships

a. Is there a senior level management committee that meets regularly to assess information technology risks and controls?

(1) Do IT and applications managers report to the committee?

(2) How does the committee identify and resolve general control weaknesses?

(3) How does the committee report to the Board on information technology issues?

b. How does management communicate to personnel their roles and responsibility for general controls over information technology?

c. Who performs quality assurance in regard to the general controls over information technology used for recording and reporting financial information?

d. Segregation of duties

(1) Who performs or is responsible for the following functions:

(a) application system(s)

[I] data migration and/or corrections to application records?

[II] system administration?

[III] system development and maintenance?

[IV] change management?

[V] security administration?

[VI] security audit?

[VII] Does one person performs all or several of the above (a), or is responsible for all or several of the above (a)? If so, is there improper segregation of duties? Describe

(b) network and servers

[I] computer operations?

[II] system administration?

[III] system development and maintenance?

[IV] change management?

[V] security administration?

[VI] security audit?

[VII] Does one person performs all or several of the above (a), or is responsible for all or several of the above (a)? If so, is there improper segregation of duties? Describe

(c) intranet

[I] computer operations?

[II] system administration?

[III] system development and maintenance?

[IV] change management?

[V] security administration?

[VI] security audit?

[VII] Does one person performs all or several of the above (a), or is responsible for all or several of the above (a)? If so, is there improper segregation of duties? Describe

(d) web site

[I] computer operations?

[II] system administration?

[III] system development and maintenance?

[IV] change management?

[V] security administration?

[VI] security audit?

[VII] Does one person performs all or several of the above (a), or is responsible for all or several of the above (a)? If so, is there improper segregation of duties? Describe

e. Are there written procedures for controlling the activities of consultants and other contract personnel to assure the protection of financial records?

3. Communication of Information Technology Policy

a. Has management assumed responsibility for formulating, developing, documenting, and communicating information technology policies?

(1) If so, does management regularly review the policies for changes in information technology and new threats?

b. How does management communicate information technology policy to employees?

c. How does management monitor the implementation of information technology policy?

d. How does management know that information technology policies are understood and complied with by employees?

e. Is there a written definition of penalties and disciplinary actions associated with failing to comply with information technology policy?

(1) Are the penalties and disciplinary action for non-compliance with information technology policy communicated to employees?

f. Does the information security policy address intellectual property rights(illegal software, music, dvds,)?

4. Human resources

a. Are personnel responsible for information technology required to take training courses on a regular basis?

b. How does management verify that personnel responsible for information technology are qualified and taking training courses on a regular basis?

c. Are employees provided with information technology orientation upon hiring and periodic updates?

d. Are employees sufficiently cross-trained in case of key employee turnover in positions responsible for information technology?

e. Are employees in sensitive information technology security positions required to take uninterrupted vacations of sufficient length to exercise the organization's ability to cope with unexpected turnover and to detect fraudulent activity?

f. Are employees considered for sensitive information technology positions subjected to background checks before they are hired, transferred, or promoted?

g. What and when are actions taken regarding job changes and terminations regarding security access to information assets?

5. Compliance with external and legal requirements

a. How does the organization maintain awareness of existing and new legal requirements for information assets?

(1) privacy of customer information?

(2) Confidential records (such as medical records, customer credit information etc)?

(3) Data retention?

b. How does management ensure compliance with existing laws, rules, and regulations regarding financial information?

c. How does management ensure compliance with intellectual property laws?

d. Are there formal contracts in place establishing requirements for information exchanged electronically via dial-up, Internet, or ftp with outside parties?

(1) How does management ensure that contract requirements for data exchange are complied with?

(2) Do contracts specify management's security requirements for data exchange?

e. Have insurance policies been reviewed for provisions regarding management's responsibilities in regard to information technology assets?

6. Risk assessment

a. How often are risk assessments made?

b. Has there been a risk assessment made of the threats to IT and financial information assets?

c. Does the risk assessment:

(1) identify all IT and financial information assets to be protected?

(2) the threats to IT and information assets?

(3) the vulnerabilities of IT and financial information assets?

(4) the safeguards over IT and financial information assets?

(5) the consequences and likelihood of the threats?

d. Is there a risk action plan to mitigate exposure?

e. For areas where risk is accepted is it offset by adequate insurance?

f. Is risk assessment documented and signed off by senior financial management?

g. Is acceptance of risk documented and signed off by both IT and senior business management?

7. Project management

a. Has the organization adopted a software development life cycle (SDLC) standard?

b. Is each new project or change assigned a unique tracking number?

c. Are standard forms used for new project requests and changes?

d. Is there a log of new project and change requests?

e. Is the cost vs. benefits of considered and documented before projects are approved?

f. What ensures that new information technology projects for financial information are designed to adhere to the organization's IT security objectives and policies?

g. Are changes to systems and programs documented whether the changes are made internally or by third party consultants?

h. Are there minimum documentation standards?

i. Are new information technology projects tested to see if they meet IT objectives and policies before implementation?

(1) If so, are there written minimum testing standards?

(2) Is there written criteria for when parallel or pilot testing will be applicable?

(3) If so, is there a written work plan for the tests?

(4) If so, is the testing documented and retained?

j. Is testing conducted in a separate test environment?

k. Are test environments representative of the future operational environment i.e. security, internal controls, workload.

l. Do users or application owners validate the operation of new systems before they are placed into the production environment?

m. Is there formal signoff by users, IT management, and business managers before new information technology projects are released into production?

n. Is there post implementation evaluation of new information technology projects to ensure that controls are effective and operating as planned?

o. Is there defined written procedures to control the handover of new systems from the test environment to production?

p. Is change management software utilized?

q. Are back-out or contingency plans required for new systems should testing fail or implementation be delayed?

8. Quality control

a. Are periodic reviews of general controls over information technology used for financial information conducted independent of the MIS department?

b. Is periodic inquiry made by management independent of MIS of owners, managers, and users of information technology for financial information as to concerns, issues, and known problems?

c. Are owners, managers, and users of financial information encouraged to report security concerns, issues, and known incidents directly to senior management on a timely basis?

9. Application development

a. When new applications or modifications to existing applications are considered:

(1) Are written operational requirements for data security specified?

(2) Are there written criteria for audit trail requirements?

(3) Are there documentation requirements?

(4) Are there data dictionary rules?

b. What measures are taken to prevent disclosure of sensitive information during testing?

c. Are new applications and modifications required to have:

(1) Authorization and authentication procedures for processing of financial information?

(2) Transaction journals?

(3) Field edit, validity, and reasonableness checks?

(4) Hash or control totals?

(5) Procedures to ensure completeness and accuracy of updating?

(6) Means of restoration or rollback in the event of procedure program aborts?

10. Acquisition and Maintenance of Application Software

a. Is there documentation of application software including a description of:

(1) The main executable program?

(2) The key tables?

(a) Record layouts

[I] data fields

[II] Key fields

[III] Field descriptions

(3) Table relationships?

(4) Which table's forms are linked to?

(5) Which tables or forms reports are linked to?

(6) Menu structure?

11. Maintenance of hardware and software

a. Is there scheduled maintenance of the air filtration system where the system units are located?

b. What control procedure ensures that system upgrades and patches do not jeopardize financial data stored on the system?

c. Are all system software changes documented?

12. Operation procedures

a. Is there a written operations procedures manual?

b. When was the last time the operations manual was updated?

c. Are there written training procedures for new operations employees, promotions, and reassignments?

d. Is there a regular training plan for operations personnel?

13. User procedures

a. Are there written user procedure manuals?

b. When was the last time the user procedure manuals were updated?

c. Are there written training procedures for new application users?

d. Is there a regular training plan for user personnel?

14. Change management

a. Is there a formal procedure to document system and application change requests?

b. Is there written procedures to evaluate change requests in regard to:

(1) Cost vs. benefit?

(2) Security implications?

(3) Impact on operations?

c. How are access rights controlled to avoid risk of unauthorized access to financial data by programmers?

d. How are programmers working on program changes and maintenance monitored to detect unauthorized access attempts?

e. Are there formal sign-off procedure for changes placed into production?

f. How is an audit trail of system and application changes generated and protected?

15. Continuity planning

a. Does the organization have a written information technology business continuity plan in the event of an unrecoverable incident or disaster which renders the system inoperable?

(1) If so, does the plan include:

(a) Communication procedures with employees, key information trading partners, owners, management, the media, and government agencies?

(b) Minimum requirements for personnel, facilities, hardware, software, equipment, forms, supplies, and furniture necessary to restore minimum levels of service.

(c) Procedures to keep the plan up-to-date?

(d) Testing?

(e) Training for staff for procedures to follow in the event of an incident or disaster?

(f) Procedures to safeguard the plan document from release to unauthorized parties?

(g) Alternative procedures in user departments to use until information services are restored?

(h) Identification of minimum key application systems, data files, and time frames needed for recovery?

(i) A formal contract if a back-up hot site is utilized?

16. Access controls

a. Have Access controls been reviewed in depth for applications applications, systems, and networks?

17. Inventory

a. Is there an up-to-date inventory identifying all IT hardware and software?

18. Unauthorized software

a. How is unauthorized software prevented from being introduced and detected on personal computers?

19. Problem and Incident management

a. Does IT management keep a audit log of operational problems, incidents, and errors?

(1) If so, does the log trace the incident from underlying cause to resolution?

b. Is there an escalation policy defining what conditions should be reported to higher levels of management?

20. Data retention periods

a. Does the organization have defined retention periods for data and programs?

21. Magnetic and Optical Media Library

a. Is there an inventory of magnetic and optical media?

(1) If so, is a physical inventory ever taken to disclose discrepancies?

b. Are there written standards and procedures for external marking of magnetic and optical media?

c. Are there written logs for accountability of storage and movement of magnetic and optical media?

d. Is the responsibility for magnetic and optical media assigned to a specific employee?

22. Backup and retention

a. Describe the backup plan.

(1) What data and programs are backed up?

b. Are the backup procedures documented?

c. How often are the backups verified to determine that they are usable?

(1) How do the tests of the backup system ensure that key systems can be restored with minimal disruption?

d. Where are the backups and related written backup and restore procedures stored?

e. How is physical access to the backup storage site controlled?

f. How is logical access to the backups in storage controlled?

23. Protection of transmitted data

a. What procedures ensure integrity of transmitted data?

b. What procedures ensure confidentiality of transmitted data?

c. What procedures ensure non-repudiation of transmitted data?

24. Authorization of transmitted data

a. How is data received from outside parties authenticated as to source?

b. How is confidential data transmitted to outside parties authorized?

(1) Is the authorization documented?

c. How is the security of confidential data transmitted to outside parties controlled?

25. Integrity of stored data

a. Are key financial files checked periodically for unusual changes and unauthorized access attempts?

(1) If so, how?

26. Facilities Management

a. How is physical access to the servers/systems protected?

b. Who has access to the systems room?

c. Are there any water pipes within 50 feet of the server room?

d. Are the servers on the floor, is there a raised floor, or raised above the floor on racks?

e. Are there halon or waterless fire extinguishers in the server room?

(1) If not, what kind of fire protection system is there?

f. Is the location of the servers kept in a low profile?

g. How are dust, heat, and humidity in the server room controlled?
(1) Are there alarm devices and monitors to automatically notify management if excessive heat or humidity conditions exist in the server room?

h. Is there an uninterruptible power supply?

(1) If so, how long can the system and servers operate on the UPS?

(2) Are there orderly shut down procedures in the event of a power failure?

27. Operations Management

a. Is there a processing operations manual?

b. Are start-up procedures documented?

c. How are job schedules authorized?

d. How are unauthorized jobs identified and investigated?

e. Is there a formal handover of operator shift changes?

f. Are there job logs of operations?

(1) If so, who reviews them for unusual activity?

(2) If so, are the reviews retained?

(3) Are unusual conditions defined in writing?

(4) Are there written procedures in the event the job logs indicate unauthorized or suspicious activity?

g. Can operators logon remotely and operate the system?

(1) If so, how are remote operator logons authenticated?

(2) If so, is a dialback routine utilized?

H. Monitoring Controls (Describe the controls in place to monitor systems, applications, backups etc)

1. Identity who monitors controls on an ongoing basis.

2. Describe how controls are monitored.

3. Are separate as opposed to ongoing evaluations of controls made?

a. If so, who makes the separate evaluations?

4. How often are controls monitored?

I. Audit logging

1. Does the system have built-in audit logging features?

a. If so, is it utilized?
b. Are audit logs of access and changes to security and system settings produced?
c. How is continuity of the logs controlled?
d. How is the integrity of the logs controlled?
e. Are the logs retained?
    (1) How long?
f. Who reviews the audit logs?

2. Are the network operating system logs enabled?
    If so:
    (1) Has anyone independent of IT inspected the audit settings?
    (2) Are the logs retained?
        (a) How long?
    (3) How is continuity of the logs controlled?
    (4) How is the integrity of the logs controlled?
    (5) Who reviews the audit logs?

3. Are the server audit logs enabled?
    If so:
    (1) Has anyone independent of IT inspected the audit settings?
    (2) Are the logs retained?
        (a) How long?
    (3) How is continuity of the logs controlled?
    (4) How is the integrity of the logs controlled?
    (5) Who reviews the audit logs?

4. Are the router logs enabled?
    If so:
    (1) Has anyone independent of IT inspected the audit settings?
    (2) Are the logs retained?
        (a) How long?
    (3) How is continuity of the logs controlled?
    (4) How is the integrity of the logs controlled?
    (5) Who reviews the audit logs?

5. Is there an intrusion detection and/or prevention system?
    If so:
    (1) Has anyone independent of IT inspected the audit settings?
    (2) Are the logs retained?
        (a) How long?
    (3) How is continuity of the logs controlled?
    (4) How is the integrity of the logs controlled?

(5) Who reviews the audit logs?

6. Is there a firewall?
If so:
(1) Has anyone independent of IT inspected the firewall rule set?
(2) Are the logs retained?
(a) How long?
(3) How is continuity of the logs controlled?
(4) How is the integrity of the logs controlled?
(5) Who reviews the audit logs?

7. What is the procedure when logs indicate suspicious activity?
a. Is the procedure documented?
b. Are incidents documented?
c. Who in the organization is notified of a suspected breach and resolution?

J. Additional Procedures

1. Are there any other procedures not included in this audit program that need to be performed in order to conclude on general controls?

a. If so, discuss additional procedures with the audit partner.

K. Assessment of General Controls

A. Identification of Internal Control Weaknesses
Based on I - IV above identify internal control weaknesses that may prevent the achievement of objectives of general controls over information technology used for financial information.

B. Document Weaknesses and Risks
Prepare proposed management letter comments on any identified weaknesses and risk including recommendations to control the risk.

VI. Reportable Conditions and Fraud

A. Did any of the preceding audit steps identify any reportable conditions, indicators of fraud, or unresolved material control weaknesses?

1. If so, document your findings and inform the engagement senior immediately.

VII. Conclusion

A. Are the general controls adequate? Are there appropriate policies and procedures that cover the development of new programs and systems, changes to existing programs, systems, and computer operations.

(Note: access to programs and data will be reviewed in a separate audit program for Information Technology Security.)

B. What is the risk of the general controls not achieving the control objectives of confidentiality, integrity, and availability (High, low)?

VIII. Index, Cross Reference and Sign-off

A. Index, cross-reference, sign-off, and date all of the work papers.

This work program has been completed in accordance with corporate policies in effect.

_____	_____
Done by <Name> <Title>	Date
_____	_____
Reviewed by	Date

1.3 TEMPLATE - NON DISCLOSURE AGREEMENT (NDA)

Private and Confidential
[Client Name and Address]
[Date]
[Salutation]

Confidentiality Undertaking

We acknowledge that during the course of [nature of work/transaction] we shall have access to and be entrusted with Confidential Information. In this letter, the phrase "Confidential Information" shall mean information (whether of a commercial, technical, scientific, operational, administrative, financial, marketing, business, or intellectual property nature or otherwise), whether oral or written, relating to [name of client/group] and its business that is provided to us pursuant to this Agreement.

In consideration of you making Confidential Information available to us, we agree to the terms set out below:

1. We shall treat all Confidential Information as strictly private and confidential and take all steps necessary (including but not limited to those required by this Agreement) to preserve such confidentiality.
2. We shall use the Confidential Information solely for the preparation of [nature of work/transaction] and not for any other purpose.
3. We shall not disclose any Confidential Information to any other person or firm, other than as permitted by item 5 below.
4. We shall not disclose or divulge any of the Confidential Information directly or indirectly to any other client of <Assessment Company Name>.
5. This Agreement shall not prohibit disclosure of Confidential Information:
   5.1. To our partners/directors and employees who need to know such Confidential Information to assist with the [nature of work being carried out]
   5.2. With your prior written consent, such consent not to be unreasonably withheld
   5.3. To the extent that such disclosure is required by law

5.4. To the extent that such disclosure is required by any rule or requirement of any regulatory authority with which we are bound to comply

5.5. On terms that as to confidentiality are to the same effect as those contained in this Agreement, to our professional advisers for the purposes of our seeking advice.

6. Upon your request we shall arrange delivery to you of all Confidential Information, and copies thereof, that is in documentary or other tangible form, except:

6.1. For the purpose of a disclosure permitted by items 5.3 and 5.4 above

6.2. To the extent that we reasonably require to retain sufficient documentation that is necessary to support any advice, reports, or opinions that we may provide.

7. Access is restricted to directors/employees/advisers of counterparties.

8. We shall inform each partner/director or employee who receives Confidential Information in accordance with items 5.2 and 5.3 above of this agreement.

9. This Agreement shall not apply to Confidential Information that:

9.1. Is in the public domain at the time it is acquired by us

9.2. Enters the public domain after that, otherwise than as a result of unauthorized disclosure by us

9.3. Is already in our possession prior to its disclosure to us

9.4. Is independently developed by us.

10. This Agreement shall continue for two years from the date of this Agreement unless and to the extent that you may release it in writing.

11. We acknowledge that the Confidential Information will not form the basis of any contract between you and us.

12. We warrant that we are acting as principal in this matter and not as agent or broker for any person, company, or firm.

13. We acknowledge that no failure or delay by you in exercising any right, power, or privilege under this Agreement shall operate as a waiver thereof, nor shall any single or partial exercise thereof or the exercise of any other right, power, or privilege.

14. This Agreement shall be governed by and construed in accordance with [applicable law] and any dispute arising from it shall be subject to the exclusive jurisdiction of the <Court Name> of the <Country Name>.

Yours truly,

1.4 TEMPLATE - SECURITY ASSESSMENT CONTRACT

This agreement made on <Date> by and between <Assessor Firm / Organization Name> hereinafter called the Assessor and <the name of the client company>, hereinafter called the Owner.

The Owner is the owner of an Information Systems Network spanning work areas and functionalities detailed in Annexure A to this Agreement;

And the Owner desires to have the Internal and External Susceptibilities and Vulnerabilities of the Security of the network tested by an Independent Network Security Assessment professional/ team of professionals with a view to obtain a reasonable assurance about the effectiveness and resilience of the Security System;

And the Assessor, who is professionally qualified and wee versed in Information Systems Security Aspects, has agreed to conduct a thorough test of the Security Systems of the network;

And both the Owner and the Assessor have agreed to the following conditions in respect of the said assignment;

Scope of work

The Assessors will carry out tests on Domains listed in Annexure B of this Agreement.
The Owner will provide the Assessors with an encrypted list of all the IP addresses/ Network / Sub Network / domains that it wishes to be tested for security vulnerabilities . It will also provide the list of the IP addresses Network / Sub Network / domains which the Assessors will not assess or access under any circumstance (hereafter referred as “Out of bound ports”).

Immediately on signing of this agreement and on receipt of the information referred above, the Assessor will commence the Assessment work.

The Assessment work shall comprise inter-alia of Site visits for Assessment of Physical Security of the Information Assets and Security Assessment from a remote location;

Limitations

1. The Assessor shall not exploit any weakness detected during the Assessment to his benefit;
2. The Assessor shall not take any advantage of the Social Engineering of the Information Organization of the Owner;
3. The Assessor shall not access/ attempt to access Out of Bound Ports and where in his professional judgment it becomes necessary to access/ assess such Ports, he shall do so with the prior consent of the Owner after apprising him of the need to do so;

Location Coverage

The locations covered include the Owner premises listed below

1
2
3
4

Liability for any downtime/DAMAGES

The Assessor will execute all tests according to the best practice in the industry and all measures will be taken to avoid damaging the network, the systems and the data contained within such network and systems;

If prejudice has been caused to the network or the data stored on the systems due to negligence while performing the tests, the Assessor will be held responsible and will compensate the Owner for all damages directly or indirectly caused. However such damages shall not exceed the fees charged for this project.

However, if downtime or damages caused by the Assessor were not due to any negligence, were unforeseeable and unavoidable, the Assessor will not be held responsible for the damages or any of its consequences.

Time of Completion of project and indication of any delay

The entire work shall be completed in <state time agreed>. In case of any delay on account of reasons beyond the control of the Assessor the same shall be explained by the Assessor to the owner. In case of any unexplainable delay the Owner shall be entitled to make deductions from the agreed Fees as Under:

<Here state the agreed penalty for delay in completing the assignment without any reasonable cause>

The contract price, any additional charges

The fees for the entire assignment shall be $ which shall be < inclusive/ exclusive> of out of pocket expenses. Where in the course of the work the Assessor feels that he has to perform work not envisaged originally he shall explain the same to the Owner and also indicate the Additional Charges for the same.

Payments

The fees agreed shall be paid by the Owner to the Assessor as Under:
< Schedule of Fee Payment>

Date and Time of assessment

The Assessor will commence the Assessment work immediately on receipt of the Advance indicated in Clause 1.7 above.

All site visits shall be made during office hours and the Assessor will inform the Owner of his Schedule of on-site visits at least <number of days> days in advance to enable the Owner to make necessary arrangements.

All remote tests on the network shall be performed outside office hours more specifically from midnight until 6 am, and only on dates preauthorized by the owner.

Remote Penetration test

The Assessor will notify the Owner the Source IP Address from the machines from where the Assessor will make remote penetration tests on the Network and Systems.

A mechanism for dealing with false positive to avoid unnecessary law enforcement

The Assessor will put in place an appropriate mechanism of correlating information to deal with false positives and ensure that the False Positives are kept at minimal levels.

For delay/non payment

If the Owner delays the payment of the agreed fees as per the agreed Schedule, the Assessor will be at freedom to withhold his report and also to enforce payment by the Owner. The Assessor, however, shall not compromise the integrity of the network &/or do any malicious activity on the Information Systems of the Owner, in case of non-payment of fees.

For additional Labor

Claims of the Assessor for extra works over that envisaged originally shall be with the prior approval of the Owner.

Contact Person(s)

Both the Owner and the Assessor will provide each other Phone, Mobile Phone Numbers and Email addresses of the Contact Persons in their respective Organisations, also indicating the area of operations and level of authority of such persons.

Confidentiality

The Assessor will maintain complete confidentiality about the information accessed by him in the course of this assignment and will execute a comprehensive Non-Disclosure Agreement in this regard.

Date_____

_____ _____

Name of Owner Name of Contractor

_____ _____

Designation (e.g. CIO) Designation (e.g. CIO)

_____ _____

Phone: Cell: Phone: Cell:

_____ _____

Fax: Fax:

_____ _____

Signature Signature

c.c.
1.
2.
3.

1.5 REQUEST FOR PROPOSAL TEMPLATE

<Company Name and specific depart name > invites you to quote for Information System Security Assessment of the < Division/Location name >

Please provide a costed response broken down by task to:

Contact Person Name
Adress
Phone
Fax
Email
Web

1.5.1 Timescales and Dependencies

- Please indicate followings:
    - Expected time to complete each task
    - Serial and Parallel tasks
    - Dependencies between tasks

1.5.2 Overview of Infrastructure

The infrastructure is located in various locations, it's huge and it makes more sense to perform assessment based on sampling. We request you to assess it based on sampling not over the complete infrastructure.

We request that a representative sample of devices shall be assessed from each identified access point, and this quote has been drawn up on this basis. Due to the huge size of network, it is also not advisable to assess vulnerabilities from every point to every other point. Assessment shall carry out per VLAN basis, however in conjunction with firewall rule-set assessment; this shall provide adequate initial coverage.

1.5.3 Domains which needs to be assessed

- Task 1: Public Information Gathering
- Task 2: Network Mapping
- Task 3: Router Security Assessment
- Task 4: Switch Security Assessment
- Task 5: Firewall Security Assessment
- Task 6: Standard build Server Security Assessment
- Task 7: Customer Isolation Security Assessment
- Task 8: Denial of Service (DoS) Assessment

1.6 REPORTING

1.6.1 Executive Summary

The objectives of carrying out the assessment were to determine the vulnerabilities present within the existing security implementation and to mitigate them. A pre-emptive assessment will help the organisation identify & mitigate information security threats before these are exploited by hackers which might result in financial loss or a loss of reputation. This assessment addresses shortcomings in the organisations security controls that include certain technology controls as well as modifications to existing security processes for a more effective security implementation on <Date> <OISSG, Tiger Team,CA> performed an assessment of the information systems security of <ABC Organization Ltd >. This report highlights several deficiencies found in the IS Security & recommends appropriate mitigation controls & strategies to overcome those.

The overall security of the systems under review was deemed rather insecure. Your organizations network is completely vulnerable. It is imperative that you take immediate actions in fixing the security stance of your organizations network.

1.6.1.1 SCOPE OF WORK

The scope of the assessment performed for <ABC Organization's Ltd, Canada> includes the following domains.

Domains	Effort (Man HRS)
• Network- and telecommunication, system, application and Database Security (Internal and External)	160
• Social Engineering	16
• Physical Security	16
• Information System Process Security	96

Location Coverage

The locations covered include the Owner premises listed below

1 IT Department, ABC Organization's, Vancouver, Canada

2 IT Department, ABC Organization's, Frankfurt, Germany

3 IT Department, ABC Organization's, London, UK

4 IT Department, ABC Organization's, New Delhi, India

1.6.1.2 OUT OF SCOPE WORK

Denials of service attacks were not carried out on the production environment (only performed on provided test infrastructure based on standard configuration documents of ABC Organization's), as these would have hampered the normal business operations. However systems vulnerable to DoS attacks have been highlighted in this report.

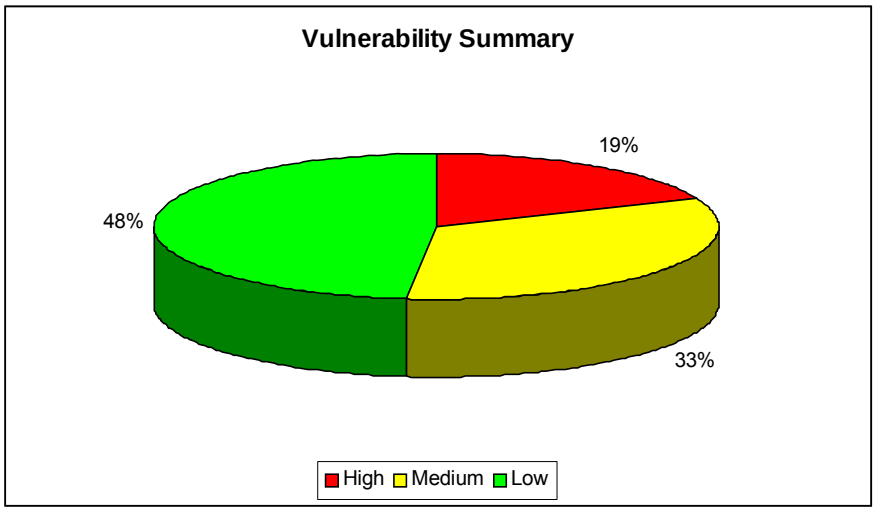
1.6.1.3 METHODOLOGY USED

The information systems were assessed using the 11 steps methodology of ISSAF which is explained in brief below.

- Information Gathering
- Network Mapping
- Vulnerability Identification
- Penetration
- Gaining Access & Privilege Escalation
- Enumerate Further
- Compromise Remove Users/Sites
- Maintaining Access
- Covering The Tracks
- Audit
- Reporting
- Clean up and Destroy Artifacts

1.6.1.4 SUMMARY OF THE ASSESSMENT RESULTS

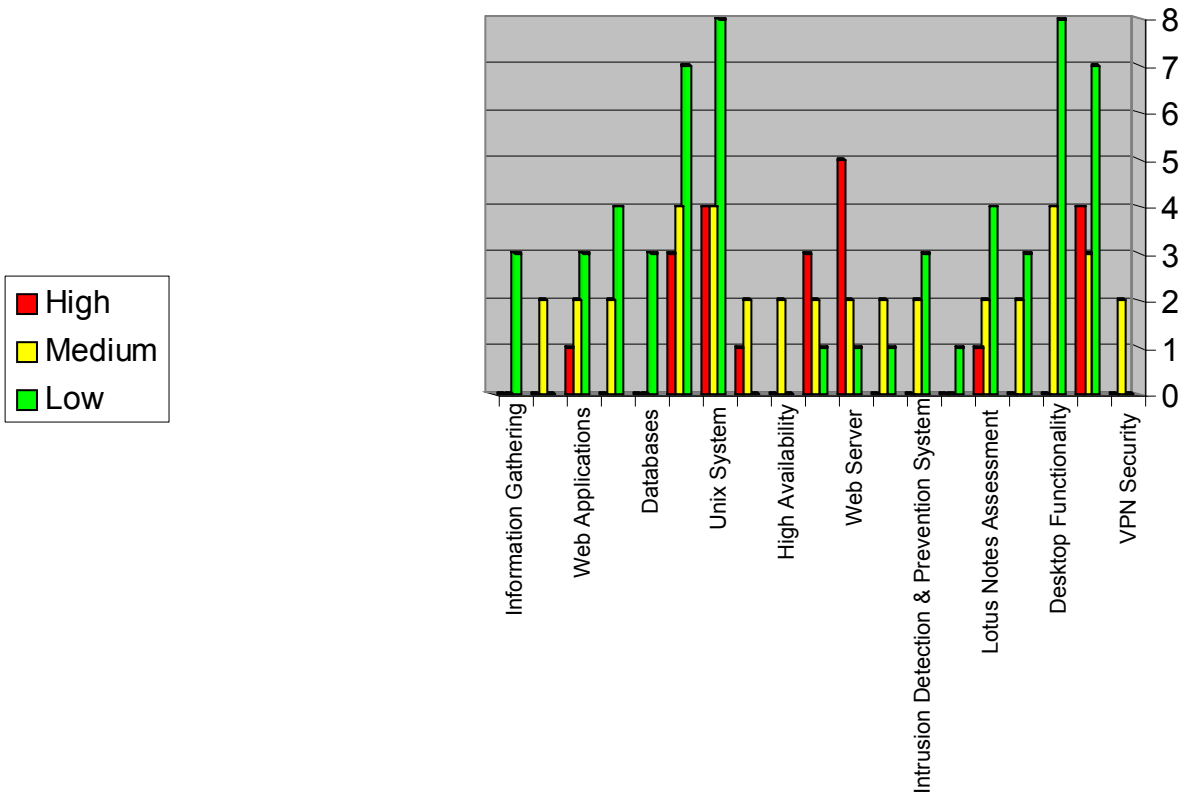
The assessment was performed on total 780 hosts, out of those 450 hosts was found to be live. In this assessment your network had 28 high-risk, 50 medium-risk and 73 low-risk vulnerabilities.



Domains Tested	Number of Vulnerabilities		
	High	Medium	Low
Network and Telecommunication, System, Application, Database Security	22	39	57
Information Gathering			3
Network Mapping		2	
Web Applications	1	2	3
Router and Routing Protocol		2	4
Databases			3
Windows System	3	4	7
Unix System	4	4	8
Password Testing	1	2	
High Availability		2	
Switch and Layer2	3	2	1
Web Server	5	2	1
Firewall Security		2	1

Intrusion Detection & Prevention System Assessment		2	3
Antivirus Assessment			1
Lotus Notes Assessment	1	2	4
Load Balancer		2	3
Desktop Functionality		4	8
Wireless Security	4	3	7
VPN Security		2	
Social Engineering	1	3	2
Physical Security	2	3	5
Process Security	3	5	9
Total	28	50	73

Number of Vulnerabilities found in each domain assessed.



Breakdown of the number of vulnerabilities under the Network and Telecommunication, System, Application, Database Security Domain

1.7 MINUTES OF MEETING - <PROJECT/TOPIC NAME>

Note:
If you are not able to participate or you will arrive late, please inform X person in advance at Tel. yyyyyy or email zzz@oissg.org

General	
ORGANIZATION AND DEPARTMENT	
DATE AND TIME OF MEETING: (MM/DD/YYYY)	DATE, STARTING TIME – FINISHING TIME (+TIME ZONE)
MINUTES PREPARED BY:	
VENUE	
GOAL	REASON FOR/GOAL OF THE MEETING
PREPARATION	PREPARATION INSTRUCTIONS (OPTIONAL)

Purpose of Meeting

Attendees of Meeting				
NAME	DEPARTMENT/DIVISION	E-MAIL	PHONE	PRESENT
				START-END
				START-END
				START-END
				START-END

Meeting not attend by

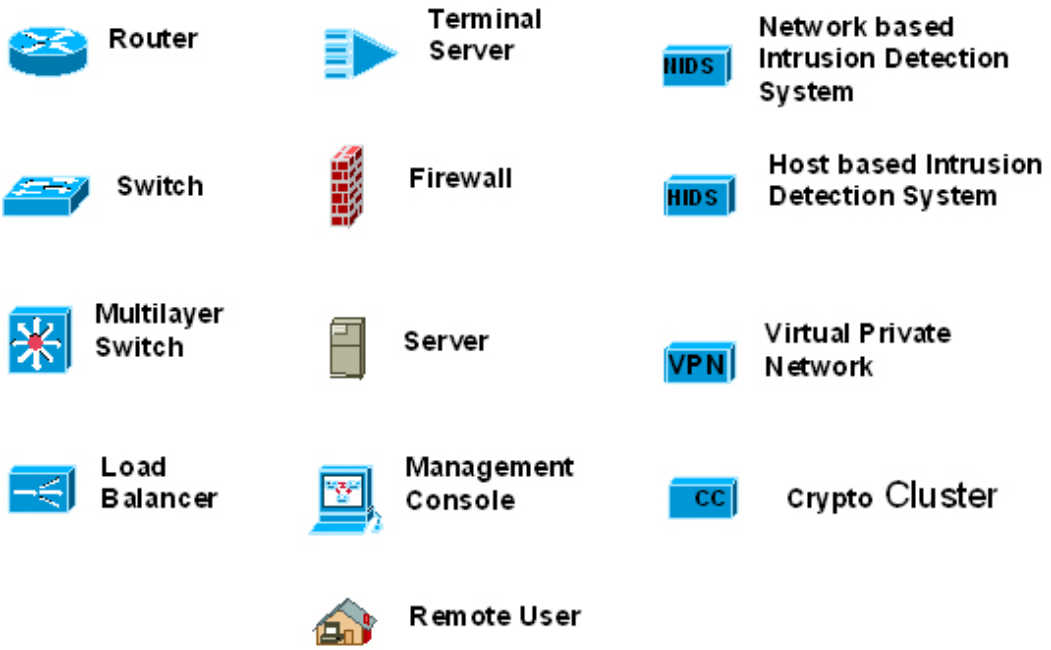
Highlights of Meeting (Discussion, Issues, Notes)

1.
2.
3.
4.

Action Item			
Action	*Assigned to*	*Due Date*	*Status*

Next Meeting		
Date: (MM/DD/YYYY)	*Time:*	*Location:*
Agenda:		

1.8 DIAGRAM LEGENDS



2 BUILD FOUNDATION

2.1 DOS ATTACKS: INSTIGATION AND MITIGATION

Author: Jeremy Martin CISSP, ISSAP, CCNA, Network+, A+
info@infosecprofessionals.com

During the release of a new software product specialized to track spam, ACME Software Inc notice that there was not as much traffic as they hoped to receive. During further investigation, they found that they could not view their own website. At that moment, the VP of sales received a call from the company's broker stating that ACME Software Inc stock fell 4 point due to lack of confidence. Several states away, spammers didn't like the idea of lower profit margins do to an easy to install spam blocking software so they thought they would fight back. Earlier that day, they took control of hundreds of compromised computers and used them as DoS zombies to attack ACME Software Inc's Internet servers in a vicious act of cyber assault. During an emergency press conference the next morning, ACME Software Inc's CIO announced his resignation as a result of a several million dollar corporate loss.

Scenarios like the one above happen a more then people think and are more costly then most will admit. Denial of Service (DoS) attacks are designed to deplete the resources of a target computer system in an attempt to take a node off line by crashing or overloading it. Distributed Denial of Service (DDoS) is a DoS attack that is engaged by many different locations. The most common DDoS attacks are instigated through viruses or zombie machines. There are many reasons that DoS attacks are executed, and most of them are out of malicious intent. DoS attacks are almost impossible to prevent if you are singled out as a target. It's difficult to distinguish the difference between a legitimate packet and one used for a DoS attack.

The purpose of this article is to give the reader with basic network knowledge a better understanding of the challenges presented by *Denial of Service* attacks, how they work, and ways to protect systems and networks from them.

The attendee should have a basic knowledge of computers systems, networking, and familiarity with the Microsoft Windows platforms. Programming knowledge is helpful.

Instigation

Spoofing – Falsifying an Internet address (know as spoofing) is the method an attacker uses to fake an IP address. This is used to reroute traffic to a target network node or used to deceive a server into identifying the attacker as a legitimate node. When most of us think of this approach of hacking, we think of someone in another city essentially becoming you. The way TCP/IP is designed, the only way a criminal hacker or cracker can take over your Internet identity in this fashion is to blind spoof. This means that the impostor knows exactly what responses to send to a port, but will not get the corresponding response since the traffic is routed to the original system. If the spoofing is designed around a DoS attack, the internal address becomes the victim. Spoofing is used in most of the well-known DoS attacks. Many attackers will start a DoS attack to drop a node from the network so they can take over the IP address of that device. IP Hijacking is the main method used when attacking a secured network or attempting other attacks like the *Man in the Middle* attack.

SYN Flood - Attackers send a series of SYN requests to a target (victim). The target sends a SYN ACK in response and waits for an ACK to come back to complete the session set up. Instead of responding with an ACK, the attacker responds with another SYN to open up a new connection. This causes the connection queues and memory buffer to fill up, thereby denying service to legitimate TCP users. At this time, the attacker can hijack the system's IP address if that is the end goal. Spoofing the “source“ IP address when sending a SYN flood will not only cover the offender's tracks, but is also a method of attack in itself. SYN Floods are the most commonly used DoS in viruses and are easy to write. See
http://www.infosecprofessionals.com/code/synflood.c.txt

Smurf Attack- Smurf and Fraggle attacks are the easiest to prevent. A perpetrator sends a large number of ICMP echo (ping) traffic at IP broadcast addresses, using a fake source address. The “source” or spoofed address will be flooded with simultaneous replies (See CERT Advisory: CA-1998-01). This can be prevented by simply blocking broadcast traffic from remote network sources using access control lists.

Fraggle Attack – This types of attack is the same as a Smurf attack except using UDP instead if TCP. By sending an UDP echo (ping) traffic to IP broadcast addresses, the systems on the network will all respond to the spoofed address and

affect the target system. This is a simple rewrite of the Smurf code. This can be prevented by simply blocking broadcast traffic from remote IP address.

Ping of Death - An attacker sends illegitimate ICMP (ping) packets larger than 65,536 bytes to a system with the intention of crashing it. These attacks have been outdated since the days of NT4 and Win95.

Teardrop - Otherwise known as an IP fragmentation attack, this DoS attack targets systems that are running Windows NT 4.0, Win95 , Linux up to 2.0.32. Like the Ping of Death, the Teardrop is no longer effective.

Application Attack **-** These are DoS attacks that involve exploiting an application vulnerability causing the target program to crash or restart the system.

Kazaa and Morpheus have a known flaw that will allow an attacker to consume all available bandwidth without being logged.
See http://www.infosecprofessionals.com/code/kazaa.pl.txt

Microsoft's IIS 5 SSL also has an easy way to exploit vulnerability. Most exploits like these are easy to find on the Internet and can be copied and pasted as working code. There are thousands of exploits that can be used to DoS a target system/application.
See http://www.infosecprofessionals.com/code/IIS5SSL.c.txt

Viruses, Worms, and Antivirus **–** Yes, Antivirus. Too many cases where the antivirus configuration is wrong or the wrong edition is installed. This lack of foresight causes an unintentional DDoS attack on the network by taking up valuable CPU resources and bandwidth. Viruses and worms also cause DDoS attacks by the nature of how they spread. Some purposefully attack an individual target after a system has been infected. The Blaster worm that exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135 is a great example of this. The Blaster targeted Microsoft's windows update site by initiating a SYN FLOOD. Because of this, Microsoft decided to no longer resolve the DNS for 'windowsupdate.com'.

DoS attacks are impossible to stop. However, there are things you can do to mitigate potential damages they may cause to your environment. The main thing to remember is that you always need to keep up-to-date on the newest threats.

Mitigation

Antivirus software – Installing an antivirus software with the latest virus definitions will help prevent your system from becoming a DoS zombie. Now, more then ever, this is an important feature that you must have. With lawsuits so prevalent, not having the proper protection can leave you open for downstream liability.

Software updates **-** Keep your software up to date at all times. This includes antivirus, email clients, and network servers. You also need to keep all network Operating Systems installed with the latest security patches. Microsoft has done a great job with making these patches available for their Windows distributions. Linux has been said to be more secure, but the patches are far more scarce. RedHat is planning on incorporating the NSA's SE Linux kernel into future releases. This will give Mandatory Access Control (MAC) capabilities to the Linux community.

Network protection - Using a combination of firewalls and Intrusion Detection Systems (IDS) can cut down on suspicious traffic and can make the difference between logged annoyance and your job. Firewalls should be set to deny all traffic that is not specifically designed to pass through. Integrating IDS will warn you when strange traffic is present on your network. This will assist you in finding and stopping attacks.

Network device configuration – Configuring perimeter devices like routers can detect and in some cases prevent DoS attacks. Cisco routers can be configured to actively prevent SYN attacks starting in Cisco IOS 11.3 and higher using the TCP intercept command in global configuration mode *access-list number {deny | permit} tcp any destination destination-wildcard ip tcp intercept list access-list-number ip tcp intercept ? (*Will give you a good list of other options?)

Cisco routers can prevent Smurf and Fraggle attacks by blocking broadcast traffic. Since Cisco IOS 12.0, this is the default configuration. ACLs or access control lists should also be configured on all interfaces.

no ip directed-broadcast

The Cisco router can also be used to prevent IP spoofing.

ip access-group list in interface
access-list number deny icmp any any redirect
access-list number deny ip 127.0.0.0 0.255.255.255 any
access-list number deny ip 224.0.0.0 31.255.255.255 any
access-list number deny ip host 0.0.0.0 any
See Improving Security on Cisco Routers - www.cisco.com/warp/public/707/21.html

Old Cisco IOS versions are vulnerable to several DoS attacks. The "*Black Angels*" wrote a program called *Cisco Global Exploiter*. This is a great software to use when testing the security of your Cisco router version and configuration and can be found at http://www.blackangels.it/Projects/cge.htm

Security is not as mystical as people believe. DoS attacks come in many different types and can be devastating if you don't take the proper precautions. Keep up to date and take steps to secure network nodes. Keeping security in mind can minimize damages, downtime, and save your career.

Resources
Black Angels: http://www.blackangels.it/
Cisco: http://www.cisco.com
Microsoft: http://www.microsoft.com/technet/security/current.aspx
Forum of Incident Response and Security Teams: http://www.first.org/
SANS Institute: http://www.sans.org/resources/

2.2 VIRUS & WORMS

Author: Jeremy Martin CISSP, ISSAP, CCNA, Network+, A+
info@infosecprofessionals.com

Virus damage estimated at $55 billion in 2003. "SINGAPORE - Trend Micro Inc, the world's third-largest anti-virus software maker, said Friday that computer virus attacks cost global businesses an estimated $55 billion in damages in 2003, a sum that would rise this year. Companies lost roughly $20 billion to $30 billion in 2002 from the virus attacks, up from about $13 billion in 2001, according to various industry estimates." This was the story across thousands of news agencies desk January 2004. Out of $55 billion, how much did it cost your company? How much did it cost someone you know?

The purpose of this class is to inform the attendee about how malicious code works, how they spread, and how to protect yourself from infection. The most well know viruses will be covered in the first part of the presentations along with the most recent. The attendee will also learn several methods (while used in combination) that will minimize both risk of infection and potential damages caused by them.

The attendee should have a basic knowledge of computers and be familiar with the Microsoft Windows platform (Win9x, WinNT, Win2k, WinXP, Windows 2003 server).

***I. The Why

There is an average of 10-20 viruses released every day. Very few of these viruses actually make “Wild” stage. Viruses are designed to take advantage of security flaws in software or operating systems. These flaws can be as blatant as Microsoft Windows NetBIOS shares to exploits using buffer overflows. Buffer overflows happen when an attacker sends responses to a program longer then what is expected. If the victim software is not designed well, then the attacker can overwrite the memory allocated to the software and execute malicious code.

People make viruses for various reasons. These reasons range from political to financial to notoriety to hacking tools to plain malicious intent.

Political: Mydoom is a good example of a virus that was spread with a political agenda. The two targets of this virus were Microsoft and The SCO Group. The SCO Group claims that they own a large portion of the Linux source code threatened to sue everyone using Linux operating systems (with “stolen” programming source). The virus was very effective knocking down SCO’s website. However, Microsoft had enough time to prepare for the second attack and efficiently sidestepped disaster.

Financial: Some virus writers are hired by other parties to either leach financial data from a competitor or make the competitor look bad in the public

eye. Industrial espionage is a high risk/high payout field that can land a person in prison for life.

Notoriety: There are some that write viruses for the sole purpose of getting their name out. This is great when the virus writers are script kiddies because this helps the authorities track them down. There are several famous viruses that have the author's email in the source code or open script

Hacking Hackers sometimes write controlled viruses to assist in the access of a remote computer. They will add a payload to the virus such as a Trojan horse to allow easy access into the victims system.

Malious: These are the people that are the most dangerous. These are the blackhat hackers that code viruses for the sole intention of destroying networks and systems without prejudice. They get high on seeing the utter destruction of their creation, and are very rarely script kiddies.

Many of the viruses that are written and released are viruses altered by script kiddies. These viruses are known as generations of the original virus and are very rarely altered enough to be noticeable from the original. This stems back to the fact that script kiddies do not understand what the original code does and only alters what they recognize (file extension or victim's website). This lack of knowledge makes script kiddies very dangerous.

II. The How

Malicious code has been plaguing computer systems since before computers became a common household appliance. Viruses and worms are examples of malicious code designed to spread and cause a system to perform a function that it was not originally designed to do.

Viruses are programs that need to be activated or run before they are dangerous or spread. The computer system only becomes infected once the program is run and the payload has bee deployed. This is why Hackers and Crackers try to crash or restart a computer system once they copy a virus onto it.

There are four ways a virus can spread:

1.) Email

2.) Network

3.) Downloading or installing software

4.) Inserting infected media

Spreading through Email

Many emails spread when a user receives an infected email. When the user opens this email or previews it, the virus is now active and starts to immediately spread.

Spreading through Network

Many viruses are network aware. This means that they look for unsecured systems on the network and copy themselves to that system. This behavior destroys network performance and causes viruses to spread across your system like wildfire. Hackers and Crackers also use Internet and network connections to infect systems. They not only scan for unprotected systems, but they also target systems that have known software vulnerabilities. This is why keeping systems up to date is so important.

Spreading through manual installation

Installing software from downloads or disks increase the risk of infection. Only install trusted and scanned software that is known to be safe. Stay away from freeware and shareware products. These programs are known to contain Spyware, Adware, and viruses. It is also good policy to deny all Internet software that attempts to install itself unless explicitly needed.

Spreading through boot sectors

Some viruses corrupt the boot sector of disks. This means that if another disks scans the infected disk, the infection spreads. Boot sector viruses are automatically run immediately after the disk is inserted or hard drive connected.

Research Project

Below are three famous programs. Research these programs using the Internet and write down how the spread, what damage they caused, if you feel you are vulnerable to a similar threat, and why.

Melissa:

Code Red:

Blaster:

Notes:

III.

Minimizing the effect of viruses and worms

We have all heard stories about the virus that destroyed mission critical company data, which cost companies months to recover and thousands of dollars and man-hours restoring the information. In the end, there are still many hours, costs, and would be profits that remain unaccounted. Some companies never recover fully from a devastating attack. Taking simple precautions can save your business

Anti-virus Software

Another step is to run an antivirus program on the local computer. Many antivirus programs offer live update software and automatically download the newest virus definitions minutes after they are released (Very important that you verify these updates weekly if not daily). Be careful of which antivirus program you chose.

Installing a PC antivirus on a network can be more destructive on performance than a virus at work. Norton makes an effective corporate edition specifically designed for Windows NT Server and network environments. When using antivirus software on a network, configure it to ignore network drives and partitions. Only scan the local system and turn off the auto protection feature. The auto-protect constantly scans your network traffic and causes detrimental network issues. Corporate editions usually have this disabled by default. PC editions do not.

Email Clients

Do not open emails from unknown sources. If you have a website for e-commerce transactions or to act as a virtual business card, make sure that the emails come up with a preset subject. If the emails are being sent through server side design instead of the users email client, specify whom it is coming from so you know what emails to trust. Use common sense when looking at your email. If you see a strange email with an attachment, do not open it until you verify whom it came from. This is how most MM worms spread.

Disable preview panes in email clients. Email clients such as Outlook and Outlook Express have a feature that will allow you to preview the message when the email is highlighted. This is a *Major* security flaw and will instantly unleash a virus if the email is infected.

It is also a good idea to turn off the feature that enables the client to view HTML formatted emails. Most of these viruses and worms pass by using the html function “<iframe src>” and run the attached file within the email header.

We will take a quick look at an email with the subject header of “You're now infected” that will open a file called readme.exe.

Subject: You're now infected
MIME-Version: 1.0
Content-Type: multipart/related;
type="multipart/alternative";
boundary="====_ABC1234567890DEF_===="
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1

To: undisclosed-recipients:;

--====_ABC1234567890DEF_====
Content-Type: multipart/alternative;
boundary="====_ABC0987654321DEF_====" ***** (This calls the iframe)**

--====_ABC0987654321DEF_====
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>
<iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0> ***** (This calls readme.exe)**
</iframe></BODY></HTML>

--====_ABC0987654321DEF_====--

--====_ABC1234567890DEF_====
Content-Type: audio/x-wav;
name="readme.exe" ***** (This is the virus/worm)**
Content-Transfer-Encoding: base64
Content-ID: <EA4DMGBP9p> ***** (Notice the <iframe src=…>)**

```
PCFET0NUWVBFIEhUTUwgUFVCTElDICItLy9XM0MvL0RURCBIVE1MIDQuMCBUcmFuc2l0aW9u
YWwvL0VOIj4NIDxodG1sPg08aGVhZD4NPHRpdGxlPldobydzIHRoZSBiZXN0LS0tLS0tPyAt
IHd3dy5lemJvYXJkLmNvbTwvdGl0bGU+DQ0NDTxzY3JpcHQgbGFuZ3VhZ2U9amF2YXNjcmlw
dCBzcmM9aHR0cDovL3d3dzEuZXpib2FyZC5jb20vc3BjaC5qcz9jdXN0b21lcmlkPTExNDc0
NTgwODI+PC9zY3JpcHQ+DTxzY3JpcHQgbGFuZ3VhZ2U9ImphdmFzY3JpcHQiPg08IS0tDWZ1
bmN0aW9uIE1NX29wZW5CcldpbmRvdyh0aGVVUkwsd2luTmFtZSxmZWF0dXJlcykgeyAvL3Yy

*** Broken to protect the innocent.  (Worm is encoded in Base64)

aHJlZj1odHRwOi8vY2l0YWRlbDMuZXpib2FyZC5jb20vZmNhbGhpc3BvcnRzZnJtMT5Gb290
YmFsbDwvYT4NIA08Zm9udCBjb2xvcj0jRkYwMDAwPiAtIDwvZm9udD4NDTxicj48YnI+PGJy
Pjxicj5Qb3dlcmVkIEJ5IDxhIGhyZWY9aHR0cDovL3d3dy5lemJvYXJkLmNvbS8+ZXpib2Fy
ZK48L2E+IFZlci4gNi43LjE8YnI+Q29weXJpZ2h0IKkxOTk5LTIwMDEgZXpib2FyZCwgSW5j
Lg08L2NlbnRlcj4NPC9ib2R5Pg08L2h0bWw+DQ0NDQoNCj==

--====_ABC1234567890DEF_====--
```

Email Servers

The first step to minimizing the effect of viruses is to use an email server that filters incoming emails using antivirus software. If the server is kept up to date, it will catch the majority of Mass Mailer (MM) worms. Ask your Internet Service Provider (ISP) if they offer antivirus protection and spam filtering on their email servers. This service is invaluable and should always be included as the first line of defense.

Many companies house an internal email server that downloads all of the email from several external email accounts and then runs an internal virus filter. Combining an internal email server with the ISP protection is a perfect for a company with an IT staff. This option adds an extra layer of control, but also adds more administration time.

Sample specs for an internal email server are:

Setup #1

Linux:	OS
Sendmail:	Email serverd
Fetchmail:	Grabs email from external email addresses
F-prot:	Antivirus
SpamAssassin:	Spam Filter

Setup #2

Win 2003 Server:	OS
Exchange:	Email server
Symantec	antivirus: Antivirus
Exchange Intelligent Message Filter:	Spam Filter

Software Updates

Keep you software up to date. Some worms and viruses replicate through vulnerabilities in services and software on the target system. Code red is a classic example. In august 2001, the worm used a known buffer overflow vulnerability in Microsoft's IIS 4.0 and 5.0 contained in the Idq.dll file. This would allow an attacker to run any program they wanted to on the affected system. Another famous worm called Slammer targeted Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000.

When updating your software, make sure to disable features and services that are not needed. Some versions of WinNT had a web server called IIS installed by default. If you do not need the service, make sure it is turned off (Code red is a perfect example). By only enabling services you need, you decrease the risk of attack.

Telecommunications Security

Install a firewall on the network. A firewall is a device or software that blocks unwanted traffic from going to or from the internal network. This gives you control of the traffic coming in and going out of your network. At minimum, block ports 135,137,139,445. This stops most network aware viruses and worms from spreading from the Internet. However, it is good practice to block all traffic unless specifically needed.

Security Policies

Implementing security policies that cover items such as acceptable use, email retention, and remote access can go a long way to protecting your information infrastructure. With the addition of annual training, employees will be informed enough to help keep the data reliable instead of hinder it. Every individual that has access to your network or data needs to follow these rules. It only takes one incident to compromise the system. Only install proven and scanned software on the system. The most damaging viruses come from installing or even inserting a contaminated disk. Boot sector viruses can be some of the hardest malware to defeat. Simply inserting a floppy disk with a boot sector virus can immediately transfer the virus to the hard drive.

When surfing the Internet, do not download untrusted files. Many websites will install Spyware, Adware, Parasites, or Trojans in the name of “Marketing” on unsuspecting victims computers. Many prey on users that do not read popup windows or download freeware or shareware software. Some sites even use code to take advantage of vulnerability in Internet explorer to automatically download and run unauthorized software without giving you a choice.

Do not install or use P2P programs like Kazaa, Morpheus, or Limewire. These programs install server software on your system; essentially back dooring your system. There are also thousands of infected files floating on those networks that will activate when downloaded.

Backups & Disaster Recovery Planning

Keep daily backups offsite. These can be in the form of tape, CD-R, DVD-R, removable hard drives, or even secure file transfers. If data becomes damaged, you would be able to restore from the last known good backup. The most important step while following a backup procedure is to verify that the backup was a success. Too many people just assume that the backup is working only to find out that the drive or media was bad six months earlier when they were infected by a virus or lost a hard drive. If the data that you are trying to archive is less then five gig, DVD-R drives are a great solution. Both the drives and disks have come down in price and are now a viable option. This is also one of the fastest backup methods to process and verify. For larger backups, tape drives and removable hard drives are the best option. If you choose this method, you will need to rotate the backup with five or seven different media (tapes, CD/DVD, removable drives) to get the most out of the process. It is

also suggested to take a “master” backup out of the rotation on a scheduled basis and archive offsite in a fireproof safe. This protects the data from fire, flood, and theft.

In the Internet age, understanding that you have to maintain these processes will help you become successful when preventing damage and minimizes the time, costs, and liabilities involved during the disaster recovery phase if you are affected.

Resources

Virus Resources

F-PROT: http://www.f-prot.com/virusinfo/

McAfee: http://vil.nai.com/vil/default.asp

Symantec Norton: http://www.symantec.com/avcenter/

Trend Micro: http://www.trendmicro.com/vinfo/

NIST GOV: http://csrc.nist.gov/virus/

Free software

AVG Anti-Virus - http://free.grisoft.com Free

F-Prot - http://www.f-prot.com Free for home users

Free online Virus scan

BitDefender - http://www.bitdefender.com/scan

HouseCall - http://housecall.trendmicro.com

McAffe - http://us.mcafee.com/root/mfs

Panda ActiveScan - http://www.pandasoftware.es/activescan/activescan-com.asp

RAV Antivirus - http://www.ravantivirus.com/scan

Free online Trojan scan

TrojanScan - http://www.windowsecurity.com/trojanscan/

Free online Security scan

Symantec Security Check - http://security.symantec.com/sscv6

Test my Firewall - http://www.testmyfirewall.com/

More Security Resources

Forum of Incident Response and Security Teams: http://www.first.org/

Microsoft: http://www.microsoft.com/technet/security/current.aspx
SANS Institute: http://www.sans.org/resources/
Webopedia: http://www.pcwebopedia.com/

Definitions

Adware: **A form of spyware that collects information about the user in order to display advertisements in the Web browser based on the information it collects from the user's browsing patterns.*

Software that is given to the user with advertisements already embedded in the application

***Malware: ****Short for malicious software, software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.*

Script Kiddie: **A person, normally someone who is not technologically sophisticated, who randomly seeks out a specific weakness over the Internet in order to gain root access to a system without really understanding what it is s/he is exploiting because the weakness was discovered by someone else. A script kiddie is not looking to target specific information or a specific company but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability.*

Spyware: **Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.*

Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising/marketing purposes or sell the information to another party.

Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers.

***Trojan:** *A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.*

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

***Virus**: *A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.*

Since 1987, when a virus infected ARPANET, a large network used by the Defense Department and many universities, many antivirus programs have become available. These programs periodically check your computer system for the best-known types of viruses.

Some people distinguish between general viruses and worms. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

Worm**:** **A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.*

* Definitions provided by Webopedia

A special thanks goes out to the CISSP community, various Chief Information Security Officer (CISO)s, and to those in the Risk assessment specialty of Information Systems Security for their help in proof reading and suggestions.

2.3 CRYPTOGRAPHY

Author: Jeremy Martin CISSP, ISSAP, CCNA, Network+, A+
info@infosecprofessionals.com

While Janet was sitting in a cyber cafe sending emails to friends and surfing the web, there was a person sitting three tables away reading each email she sent before they ever get to the email server. During this period of time, the thief is able to gain access to her bank account, steal passwords to several business websites, and "archive" her credit card numbers. This scenario is not far from reality and is the main reason that using cryptography is so important in today's technological world.

Most people think that cryptography is an island in the magical land of make believe. However, cryptography is very real and not as complex as most would believe. If you use the Internet, you are likely to use applied cryptography in your day-to-day functions. This can be accessing you bank account to retrieve your monthly balance to purchasing the newest season of your favorite TV show from an online shopping mall. Companies use cryptography to make sure sensitive data stays confidential between the intended parties and the data stays intact. Cryptography is the art of converting messages into a secret code or cipher to protect it from prying eyes. This process alters a plaintext message using an algorithm to create a ciphertext/encrypted message.

History of Ciphers

Cryptography has been in use for thousands of years. In fact, it was in use before 2000 B.C. Egypt in the form of hieroglyphs. The Greeks even used encryption referred to as the Scytale cipher. The Scytale was a long strip of leather with writing on it and was worn as a belt by couriers. This leather strip would be wrapped around a specific sized staff to decrypt the ciphertext. Another popular cryptographic algorithm used by Julius Caesar. This for of encryption shifts the alphabet three spaces to the right and is also referred to as ROT-3.

Applied Cryptography

Ok, but how do I use it and why does it affect me? The basic uses of cryptography are to provide confidentially (secrecy of the data), integrity (protection from intentional or unintentional alteration), and authentication (prove you are who you say you are). Some forms even allow for Nonrepudiation services that prove that the message was written, sent, or received. We will briefly discuss the most commonly used cryptographic schemes that you may use every day while leaving the trivial details out.

You will hear the terms X.509 and digital certificates (used in digital signatures) throughout this paper. The most well know companies that sell these certificates are:

1. Verisign - http://www.verisign.com/

Thawte – http://www.thawte.com/ (Offers free personal email digital certificates)**File access**

Stenography: Stenography is the art of concealing files or messages in other media such as a .JPG image or .MPG video. You can add this data in the unused bits of the file that can be seen by using a common hex editor. Stenography is the easiest way to hide a message, but is by far the least secure. Security by obscurity is only intended to keep the honest, honest.

PGP: Pretty Good Privacy was created by Philip Zimmerman in 1991 and was the first widely accepted public key system. PGP is suite of encryption tools used for encrypting various types of data and traffic. PGP can be used for S/MIME and digitally signing a message. They use a web of trust that allows the community to trust a certificate rather than a hierarchy Certification Authority (CA) to verify the user's identification.

Personal/Freeware: This can be downloaded from MIT for free.

- Diffie-Hellman key exchange
- CAST 128 bit encryption
- SHA-1 hashing function

Commercial: PGP® Software Developer Kit (SDK) 3.0.3 has received Federal Information Processing Standards (FIPS) 140-2 Level 1

validation by the National Institute of Standards and Technology (NIST).

- RSA key exchange
- IDEA encryption
- MD5 hashing function

Internet traffic

HTTPS: Hypertext Transfer Protocol over Secured Socket Layer. Do not mistake HTTPS with SSL. This is a common misnomer that is spread by those that do not understand SSL. HTTPS uses SSL to create an encrypted tunnel between a client and a server. This tunnel lasts the entire connection and is the most common website security feature on the Internet. This form of encryption is established by the use of a server side X.509 certificate that digitally signs the message.

S/MIME: Secure Multipurpose Internet Mail Exchange. S/MIME uses two X.509 certificates (also called digital signature) and both signs and encrypts the email. The author digitally signs the email with their private key. Once this happens, the message is encrypted with the recipient's public key. When the message reaches the recipient the message is decrypted with the recipient's private key, and then verified using the author's public key. Email clients like Netscape Communicator and Microsoft Outlook can use S/MIME with little setup required.

S-HTTP: Secured HTTP. The benefit of S-HTTP over HTTPS is the fact that each message is encrypted rather then using a tunnel that is vulnerable to both a man-in-the-middle and a session hijack attack. Another advantage of S-HTTP is that it allows for two-way client/server authentication.

Tunneling encryption

IPSec: IP Security Protocol is the most commonly used network encryption for the corporate world. When most people in the computer industry think about Virtual Private Networks (VPN)s, they immediately think of

IPSec. Companies that use IPSec need an encrypted tunnel that allows all network traffic to flow through. Unlike SSL, IPSec is not limited to a port. Once the IPSec tunnel has been established, the system should have the same network access that it would have at the physical location. This offers far more power, but also requires far more overhead. Another issue is security. The more open the network, the more vulnerable it is. This is another reason why VPNs are usually on the outside of a firewall. Vulnerabilities to IPSec include session hijacking, and replay attacks.

SSH: Secure Shell provides a terminal like tunnel that protects the data crossing the network and should replace clear text protocols like Telnet and FTP. One of the most popular windows SSH clients is Putty.

SSL: Secured Socket Layer can be used to create a single port/socket Virtual Private Network (VPN) using a server side X.509 certificate. The most common use of SSL is webpage traffic over HTTP or HTTPS. SSL is vulnerable to man-in-the-middle attacks. Anyone can create a CA to distribute certificates, but keep in mind that a digital certificate is only as trustworthy as the CA that controls the certificate.

WEP: Wired Equivalent Privacy. This algorithm uses either a 40-bit key or a 128-bit (24 of the bits is used for the initialization vector) key. Most devices also allow for a wireless access point to filter MAC addresses to increase access controls onto the device. WEP is vulnerable and has been exploited by criminal hackers (crackers) while wardriving since WEP has hit the market. Some of the more popular tools used for wardriving are:

- Airsnort - a WEP encryption key recovery tool
- Kismet - an 802.11 layer2 wireless network detector

Netstumbler - an 802.11 layer2 wireless network detectorWPA: Wi-Fi Protected Access is a new standard that may overtake the old WEP technology in the near future. WPA uses a Pre-Shared Key (PSK) for SOHO networks, and Extensible Authentication Protocol for other wired/wireless networks for authentication. Some cryptoanalysts claim PSK is a weakness due to the fact that a cracker can access the

key and brute force the key until it is known. The encryption scheme that is used is Temporal Key Integrity Protocol (TKIP). TKIP ensures more confidentiality and integrity of the data by using a temporal key instead of the traditional static key. Most people welcome this technology over the less secure WEP.

Each encryption model is vulnerable to one attack or another. Below is a list of attack techniques that are used by cryptoanalysts to break the keys used to protect the messages

Ciphertext-Only: This is the easiest to instigate, but hardest to succeed. The attacker retrieves the ciphertext data through listening to the network traffic. Once the key is has been salvaged, the cracker can attempt to brute force the message until it resembles something legible.

Known-Plaintext: This covers the scenario of the cracker having both the plaintext and corresponding ciphertext of one or more messages. In WWII, the Japanese relied on cryptography, but had a weakness of sending formal messages. These messages were able to be broken because the ciphertext started and ended with the same message. Part of the plaintext was known and cryptoanalysts were able to decipher the message using the known-plaintext method.

Chosen-Plaintext: Similar to the know-plaintext attack, but the attacker can choose the plaintext to be encrypted. An attacker can assume someone else identity and send a message to target that needs to be encrypted. Since the plaintext is chosen and the target sends the encrypted message, the chosen-plaintext attack is successful.

Chosen-Ciphertext: The cryptoanalyst is chooses the ciphertext and has access to the decrypted plaintext.

Birthday Paradox: This attack is successful when a hash value of a plaintext matches the hash value of a completely different plaintext. This anomaly is proven mathematically among 23 people, there are 23*22/2 = 253 pairs, each of which being a potential candidate for a match.

Brute-Force: This form of attack is implemented by passing through every possible solution or combination until the answer is found. This is the most resource and time intensive method of attack

Dictionary: The attacker compares the target hash values with hash values of commonly used passwords. Dictionary files can be downloaded from hundreds of Internet sites.

Man-in-the-Middle: The attacker intercepts messages between two parties without either target knowing that the link between them has been compromised. This allows the attacker to modify the message at will.

Replay: Replay attacks are simply the replay of captured data in an attempt to trick the target into allowing the unauthorized access.

Back at the cyber café, if Janet connected to a secured web server using SSL to do her online banking and used S/MIME to send private email, the cyber thief would never had a chance of seeing her unmentionables.

3 WINDOWS (DESKTOP) SECURITY CHECKLIST

Overview

Windows 95 which is a commonly used platform does not allow for easy application or administration of security standards. As the Windows 95 password security system serves only to provide a means of authentication to the local machine, it can easily be bypassed by the cancellation of or escape out of the login process and was cached in a relatively easily cracked .pwl file

Therefore it is **recommended that Windows 2000 Professional be used on the desktop**. It is easier to configure than the O/S it replaced (Windows NT Workstation) & offers increased stability and security (compared to both Win95 and WinNT) by use of NTLM and/or NTLMv2 password encryption (as opposed to the LanMan Hash used by Win95). It also provides file system security with NTFS.

Check-List

Listed below are a few security settings that can be done on the Windows 2000 Professional desktop to make it resistant to network & physical break-in attempts.

Action	Need	Check
Provide Physical Security for the machine	Preferred	
Enable BIOS password	Mandatory	
Disable the Guest Account	Mandatory	
Limit the number of unnecessary accounts	Optional	
Create 2 accounts for Administrators	Optional	
Rename the Administrator Account	Preferred	
Consider creating a dummy Administrator account		
Replace the "Everyone" Group with "Authenticated Users" on file shares	Mandatory	
Password Security	Mandatory	
Password protect the screensaver	Mandatory	
Use NTFS on all partitions	Mandatory	
Always run Anti-Virus software	Mandatory	
Secure your Backup tapes	Mandatory	
Shut down unnecessary services	Preferred	

Enable Auditing	Optional	
Check Microsoft's web site for the latest hotfixes	Preferred	
Disable the ability to boot from a floppy or CD ROM on physically unsecured systems.	Optional	
Use NTFS file system	Mandatory	

Description

Provide Physical Security for the machine

Most security breaches occur from the inside. It is possible to break into the system when a console access is available unless there are other access control methods deployed.

Enable BIOS password

Enabling the bios/boot password would help to prevent unauthorized users from accessing the system. The only possible way to access data from this system with the bios password would be to open it & reset the bios password. This password must be deposited with the users superiors.

Disable the Guest Account

Disable the guest account from user manager. This will help prevent users from accessing folders that were shared accidentally to the "Everyone" Group users in Win2K.

Limit the number of unnecessary accounts

Eliminate any duplicate user accounts, test accounts, shared accounts, general department accounts, etc., Use group policies to assign permissions as needed, and audit your accounts regularly.

Create 2 accounts for Administrators

Having 2 accounts with administrative access help easy retrieval of data incase password for one of the system administrator accounts was forgotten/ misplaced.

Rename the Administrator Account

Renaming the administrator account will help in securing the system as hacking attempts for the user administrator will not be valid & it will be that much more difficult for the hacker to find the administrative system account & break it. If you rename the account, try not to use the word 'Admin" in it's name. Pick something that won't sound like it has rights to anything.

Consider creating a dummy Administrator account

Another strategy is to create a local account named "Administrator", then giving that account no privileges and impossible to guess +10 digit complex password. If you create a dummy Administrative account, enabled auditing so you'll know when it is being tampered with.

Replace the "Everyone" Group with "Authenticated Users" on file shares

"Everyone" in the context of Windows 2000 security, means anyone who gains access to your network can access the data. Never assign the "Everyone" Group to have access to a file share on your network, use "Authenticated Users" instead.

Password Security

Do not share passwords with other users including administrators. Passwords should be at least 6 characters (recommended 10 characters) with a combination of alpha numeric characters. Change passwords at least every 60 days & do not recycle at least 3 previously used passwords.

Password protect the screensaver

Once again this is a basic security step that is often circumvented by users. Make sure all of your workstations and servers have this feature enabled to prevent an internal threat from taking advantage of an unlocked console. For best results, choose the blank screensaver or logon screensaver. Avoid the OpenGL and graphic intensive programs that eat CPU cycles and memory. Choose 5 minutes or less as the screen saver activation time.

Use NTFS on all partitions

FAT and FAT32 File systems don't support file level security and give hackers a big wide open door to your system. Make sure all of your system partitions are formatted using NTFS. Using dos bootable floppys a user can boot inito the system & access data. Having NTFS can make it difficult to access the data.

Always run Anti-Virus software

Make sure that the Norton anti-virus software is running on the system & the updates to the software are at least 1 week old.

Secure your Backup tapes

Its a good idea to have all floppy disks, CDROM's & other media with backup data to be placed under lock & key. Please also remember to delete files not required from the media before sharing the data on the media with other users.

Shut down unnecessary services

Windows 2000 comes with Terminal Services, IIS, and RAS that can open holes into your operating system. It's often convenient to enable Terminal Services to allow remote control functions for the help desk or administering servers, but you have to make sure it's configured correctly. There are also several malicious programs that can run quietly as services without anyone knowing. Be aware of all the services that all run on your servers and audit them periodically. These are the basic services that need to be running.

Computer Browser
Netlogon
NTLM SSP
RPC Locator
RPC Service
TCP/IP NetBIOS Helper
Spooler
Server
WINS
Workstation
Event Log

The other services like IIS admin service WWW publishing service etc should be disabled. This in addition to securing your desktop also improves the system performance as it uses less resources.

Enable Auditing

The most basic form of Intrusion Detection for Windows 2000 is to enable auditing. This will alert you to changes in account policies, attempted password hacks, unauthorized file access, etc., Most users are unaware of the types of doors they have unknowingly left open on their local workstation, and these risks are often discovered only after a serious security breach has occurred. At the very minimum, consider auditing the following events:

Event Level of Auditing

Account logon events Success, failure
Account management Success, failure
Logon events Success, failure
Object access Success
Policy change Success, failure
Privilege use Success, failure
System events Success, failure

Periodically Check Microsoft's web site for the latest hotfixes

There are a lot of service packs that are released by microsoft for patching up the vulnerabilities in the software. You can go to the url
http://windowsupdate.microsoft.com/

This will analyze your system & ask you to download & install all service packs that are required to be installed on your system.

Disable the ability to boot from a floppy or CD ROM on physically unsecured systems.

There are a number of 3rd party utilities that enable a number of security holes is used via a boot disk (including resetting the local administrator password.) If your security needs are more extreme, consider removing the floppy and CD drives entirely. As an alternative, store the CPU in a locked external case.

Use NTFS file system

The default used filesystem is FAT32 or FAT 16. This can be accessed easily by booting from a floppy. It is advisable to convert this filesystem to NTFS as this has filesystem level security for users.

4 LINUX SECURITY CHECKLIST

4.1 AUDITING MODULE

Perform audit before and after the security of system.

4.2 CHECK FOR UNNEEDED SERVICES

Check /etc/inet/inetd.conf, /etc/xinetd.conf for all the unnecessary services. Best would be to backup existing and start from scratch with web/mail/ftp and telnet whichever is required (copy the lines needed from backup).
Check /etc/rcS.d, /etc/rc2.d and /etc/rc3.d for services starting from there.
Use chkconfig and ntsysv to verify the running services. Minimum for chkconfig would be like:
syslog
network
sshd
crond
xinetd

Sendmail should be disabled completely or at least remove the "–bd" flag to stop sendmail from listening on port 25 if the server is not a smtp server, if smtp server or the service is listening try to disable EXPN and VRFY options in Sendmail.cf.

4.3 CHECK FOR UNWANTED USERS AND LOCK DEFAULT USERS.

Check for all pwck errors, check for unnecessary users. Verify the shell to be "/bin/false" for users which are not allowed to log on to the server.

Bin
Daemon
Adm
Sync

Shutdown

Halt

nobody

4.4 VERIFY THE FILE PERMISSIONS FOR (AT LEAST) THE FOLLOWING FILES:

File	Permission
/etc/ftpusers	640
/etc/inetd.conf	440
/etc/xinetd.conf	440
/etc/inetd.d	440
/etc/at.deny	600
/etc/hosts.allow	644
/etc/hosts.deny	644
/etc/cron.allow	600
/etc/cron.deny	600
/etc/crontab	644

4.5 VERIFY PASSWORD SETTINGS IN /ETC/LOGIN.DEFS.

Inactive should be 40 in /etc/default/useradd/etc/login.defs

PASS_MAX_DAYS 40

PASS_MIN_DAYS 5

PASS_MIN_LEN 9

PASS_WARN_AGE 6

4.6 CHECK IF IP FORWARDING IS DISABLED OR NOT?

4.7 CREATE SEPARATE PARTITIONS FOR LOG/TMP FOLDERS AND SMTP QUEUE.

4.8 VERIFY THE LEGAL NOTICE

Verify if the following files exist:

/etc/motd

/etc/issue

Verify the content of these files as well.

4.9 VERIFY CRON & FTP RESTRICTIONS

Verify the following files:

/etc/cron.d/at.deny

/etc/cron.d/cron.deny

/etc/ftpusers

4.10 CHECK FOR WORLD WRITABLE DIRECTORIES AND FILES

4.11 CHECK FOR NONUSER AND NOGROUP FILES

- Check for suid and sgid files and remove suid/sgid permissions from unwanted files
- Check for local modem.
- Check the default run-level
- The default run-level should be set to 3 for networked systems.
- The boot loader should be password protected

Verify that lilo or grub have a password configured (can be performed by either checking /etc/lilo.conf, /etc/grub/grub.conf or rebooting)

- The root user should be restricted to console
- nosuid should be set for floppy and cdrom mount options in /etc/fstab
- Check /etc/shells for invalid shell files

5 SOLARIS SECURITY CHECKLIST

5.1 INTRODUCTION

Standard Operating Systems Hardening

A secure (Hardened) operating system has the following characteristics:

1. Only the required programs and services run
2. All vendor recommended patches are installed – this needs constant attention
3. Only required user accounts exist, with secure passwords and set privileges
4. Only required ports are open
5. Cleartext protocols like telnet and ftp protocols are replaced with more secure encrypted access product such as SSH
6. Routing is disabled for all servers that are not routers
7. No root ftp is allowed
8. r commands (eg rhosts) are disabled
9. Sendmail is disabled unless required (if sendmail is required it must be made as secure as possible.)
10. Failed login attempts limited and logged
11. List of “cron” and “at” schedules created and checked regularly – investigate any additional tasks
12. SNMP is disabled

5.1.1 Process for Hardening Solaris

- Install all recommended Sun Patches
- Determine required programs, services, ports and user accounts for the specific server.
- Remove or disable all non essential programs, ports and user accounts
- Tighten the security for required services.
- Use hardening packages such as YASSP if required.

5.1.1.1 MESSAGING SERVER

Sendmail must not be disabled. Perform sendmail hardening instead (see sendmail service in the table below for the minimum requirements: disabling vrfy/expn and version display.) The sendmail service has historically been prone to security breaches, and the securing of this program is beyond the scope of this document.

5.1.1.2 WEB APPLICATION AND/OR DATABASE SERVER

Sendmail should be disabled if not needed. FTP and SSH access is required usually for development and/or publishing. Remember to replace telnet with ssh!

5.1.2 Minimum Hardening recommendations from SANS

Service Recommendations

Service	Recommendation	Comments
TCP Services Enabled	SSH	Run as few TCP services as possible. TCP services that are run should encrypt authentication data (i.e. user name / password pairs)
UDP Services Enabled	syslog	Run as few UDP services as possible. UDP services that are run should encrypt where possible
Filter services	TCP Wrappers	Disable connections from unauthorized hosts. Firewall utilites have similar functionality
OS Version revealed	disabled	Version information can be used by intruders
TCP Banners	enabled	All services should display a banner (legal note) displaying use and monitoring policy
Multicast	disabled	Not needed at most sites
Daemon Unmask	022	Network daemons should not create world or group readable files

FTP system accounts	disabled	Administrative users should never use cleartext protocols
Sendmail vrfy/expn	disabled	Sendmail should not give out account information
Sendmail version displayed	disabled	Version information is useful to intruders
Rhosts-style auth	disabled	"r" commands have inherent weakness in the protocol
DHCP	disabled	Prevent roge DHCP servers from giving faulty information
Snmpd	disabled	SNMP may give information out to intruders: May need to be enabled for development/ testing

Kernel Parameter Recommendations

Parameter	Recommendation	Comments
Stack Protection	enabled	Stack protection thwarts some types of buffer overflows
NFS port monitor	enabled	
Disable core dumps	enabled	Core dumps may give out confidential information. Should be enabled only on non production machines

Network parameter recommendations

Parameter	Recommendation	Comments
Act as router	disabled	Secure hosts should not route packets
Arp_cleanup_interval	60000	ARP hold time for unsolicited information (in millisecounds)
Ip_ire_flush_interval	60000	
Ip_forward_src_routed	0	Direct broadcast messages may be used in smurf-type attacks
Ip_forwarding	0	Workstation should not route packets (this is equivalent to touching (etc/notrouter)
Ip_ignore_redirect	1	Hosts with a single default router need not accept redirects
Ip_send_redirects	0	Only routers need redirect errors
Ip_strict_dst_multihoming	1	Prevents packet spoofing on non forwarding multi homed systems

Tcp_extra_priv_ports_add	2049	Increase the reserved TCP port range – most notable for NFS
Tcp_conn_req_max_q	10240	Protect against SYN flood by increasing queue size
Udp_extra_priv_ports_add	2049	Increases the reserved UDP port range.
Strong TCP Sequence Numbers	2	RFC 1948 strong sequence numbers to prevent IP spoofing attacks.

File Permissions and User Default Recommendations

Permission	Recommendation	Comments
Fix-modes	enabled	Fix-modes tightens file permissions and updates the pkginfo Database
User default mask	022	New user files should only be readable by owner

System Logging Recommendations

Log	Recommendation	Comments
Authentication	Auth.info	Authentication information logged to disk
Failed login	/var/log/login	Logs multiple failed login attempts

Miscellaneous Recommendations – for every solaris installation

Description	Recommendation	Comments
CDE	disabled	CDE and other X servers have a long history of security problems
Set EEPROM security	command	Password is required to boot except of default media
NFS	disabled	NFS has history of security problems
AutoFS	disabled	AutoFS is an extension of NFS
Patches	Recommended cluster	Install ALL vendor recommended patches
Packet Filtering	Default Deny	All services should be filtered to ensure that only legitimate connections are accepted

5.2 LEADING TOOLS FOR HARDENING SOLARIS

Titan: is a collection of programs, each of which either fixes or tightens one or more potential security problems with a particular aspect of a unix system. Titan is available free of charge from www.fish.com/titan

YASSP: Yet Another Secure Solaris Package. The default behavior of the YASSP package is to harden the system with a configuration that's suitable for an external (exposed) server like a Firewall, a web server or an ftp server where you should limit your security exposure. The configuration should also be adequate for an internal "back-room" server -- e.g. a database engine. The package establishes several security settings: network services are disabled, file ownership and protection weakness are resolved, system logging is enabled, the network stack is tuned and several system parameters are set. The resulting configuration is the consenus of a large working group. However, if you need a different configuration you can control most of the settings from a single configuration file (/etc/yassp.conf). The result is a coherent ***default*** environment where you ***know*** what to expect and where. The product is available free of charge at http://www.yassp.org/

SSH: Secure Shell is the replacement for rsh, rlogin, rcp, telnet, rexec, rcp and ftp. It encrypts all traffic, and provides various levels of authentication depending on your needs. Main features of Secure Shell include secure remote logins, file copying, and tunneling TCP and X11 traffic. A non commercial version can be downloaded from www.ssh.org/download.html and commercial licences from www.ssh.com .

SUDO: sudo is a utility that permits superuser-like access controls, it installs in /usr/local. The sudoers file is installed in /usr/local/etc. It is available free of charge from http://sunfreeware.com/

Sun Enterprise Authentication Mechanism™ (SEAM) - for secure network services, this product is based on **Kerberos**, called. **Kerberos** is a centralized network security architecture that uses a ticket mechanism to provide strong authentication. The SEAM product also uses strong encryption.

JumpStart Architecture and Security Scripts ("JASS" Toolkit): The JumpStart Architecture and Security Scripts ("JASS" Toolkit) is a tool designed to assist in creation and deployment of secured Solaris Operating Environment systems. The Toolkit is comprised of a set of scripts and directories implementing the

recommendations made in the Sun BluePrints OnLine program. (http://www.sun.com/software/solutions/blueprints/tools/index.html;$sessionid$MTINZJAAAAFPNAMTA1LU4GQ)

5.3 SOLARIS SECURITY CONCEPTS

This section outlines the key concepts, programs and settings that should be considered when securing an exposed server.

5.3.1 File System and Local Security

5.3.1.1 INITIAL INSTALLATION

The initial installation should be minimized to include only the required services and programs for the purpose to which the server will be put. All SUN recommended patches should be applied. The file partitions must include enough space for all requirements to prevent Denial of service attacks, for example mail servers need a separate var/mail partition for mail files, this needs to be monitored to ensure adequate space.

5.3.1.2 CONSOLE SECURITY

The console security eeprom should be set to full, the password changed and password guessing monitored.

5.3.1.3 FILE SYSTEM

File permissions should be strengthened, removing group write ability. Set user ID and Set Group ID bits allow executables to operate with files as though they own them, this is necessary for many programs, but can be used in security breaches – especially if poorly written. It is important to remove all unnecessary programs with suid and guid bits. The command: **# find / -type f \(-perm -u+s -o -perm -g+s \) –ls** will identify all such files.

Important areas should be mounted with read only access using the nosuid option (for example the /usr partition.) It is not possible to mount the root (/) file system with the nosuid option.

5.3.1.4 ACCOUNTS

Unnecesary system accounts such as uucp should be identified and disabled (eg #passwd –1 uucp disables the uucp account.)

“cron” and “at” access should be restricted to only the user account that require it using the cron.deny and cron.allow files. At list of all scheduled tasks should be compiled and checked regualarly, unexpected additions should be investigated.

5.3.1.5 THE INIT SYSTEM

The init system manages system services, some are not needed and should be disabled, those remaining need to be strengthened. The simplest way to disable a service is to rename it. Sun recommends putting an underscore in front of the name as this makes it easy to identify and restart services if they are needed again.

The system default Umask is initially set to 000 which allows new files created by system daemons have read / write access by all users by default. The value should be changed to 022.

5.3.1.6 KERNAL ADJUSTMENTS

Several kernal adjustments can be made to increase Solaris security, extreme care needs to be taken as mistakes can prevent the system from booting.

The Solaris Network File Service should be modified to only accept client requests from privileged system ports.

The system stack should be made non executable to help prevents that attack a priveliged program stack to take control of it. This requires the addition of two lines to the etc/system file, the first block execution of the stack while the second logs unsuccessful attempts:

```
set noexec_user_stack = 1
set noexec_user_stack_log = 1
```

Core files may contain sensitive information and can be very large, these should be disabled unless needed for debugging. If core files are needed for debugging they should be regularly cleaned up.

5.3.1.7 LOG FILES

It is important to ensure there is sufficient disk space for both system and application log files as full partitions can lead to denial of service problems. All log files should be checked regularly for problems.

5.3.1.8 MISCELLANEOUS

The contents of the etc/issue file are displayed for all telnet logins, it should contain a message outlining the companies monitoring policies and contain warnings about inappropriate or unauthorized use.

The Pluggable Authentication Module (PAM) should be altered to replace the use of the unsecured rlogin and rsh with an ssh protocol system.

5.3.2 Network Security Service

5.3.2.1 TELNET

Telnet allows users to log in and access a remote system on the network, it is not a secure system. Authentication is by user name and password only, neither of which

is encrypted while in transit making it vulnerable to attack. Sun's SEAM product provides a replacement telnet
command that uses strong authentication and encryption as does SSH.

If telnet daemon without encryption must be used, then One Time Passwords and TCPWrappers should be used to secure the connections

5.3.2.2 REMOTE ACCESS SERVICES (RSH RLOGIN RCP)

Remote Access commands to not provide for system authentication or information accountability, as they are generally used within a 'zone of trust' where each computer is trusted, by default the only authentication is the IP address. IP addresses are easily stolen and misused, so Secure Shell ssh, kerbos or SEAM protocols should be used instead.

5.3.2.3 REMOTE EXECUTION SERVICE (REXEC)

Rexec provides for remote execution using cleartext username password authentication and so is not secure exposing the system to the same threats as telnet. It should be disabled.

5.3.2.4 FTP

ftp provides for remote file transfer using cleartext username password authentication and so is not secure exposing the system to the same threats as telnet. Alternatives such as SSH or kerbized ftp should be used.

5.3.2.5 INETD MANAGED SERVICES

inetd manages the majority of minor network services available on a system, A secured server should neither have an /etc/inetd.conf (inetd configuration file) nor run inetd. If some of its services are needed ensure that the others are disabled.

Services managed by inetd are: telnet, ftp, tftp, intnamed, in.uucp, systat, netstat, time, echo, discard, chargen.

Note the Web application server will require a system time function to produce error logs, for security the xntp daemon should be used instead of time.

5.3.2.6 RPC SERVICES

Remote Procedure Call (RPC) services are used in many UNIX services including: NFS, NIS, NIS+, and Kerberos., and many applications such as: Solstice Disk Suit software and SunCluster software.

Security issues arise mainly with some of the services that use RPC that do not use encrypted authentication. Many aspects of RPC can be disabled in most instances and where possible applications using these services should be configured to use strong authentication.

5.3.2.7 NFS SERVER

From a security perspective it is better to neither provide or accept NFS services. If NFS services are required the following precautions should be taken:

- Explicitly list hosts allowed access to NFS server directories. Do not open access to all systems.
- Export only the lowest directory necessary.
- Export read-only whenever possible.
- Use strong authentication methods such as AUTH_DES or AUTH_KERB whenever possible.

5.3.2.8 SENDMAIL

Sendmail is used to both forward and receive mail, it has been historically vulnerable to attack. Unless it is required sendmail should be disabled. Where sendmail is required it should be configured to make it as secure as possible, this is an involved task and special references for it need to be followed.

5.3.2.9 NAME SERVICE CACHING (NSCD)

The nscd provides a cache for the most common name services requests, password, group and host databases. Unless needed this service should be disabled completely. If it is required (for example to run NFS) it should be configured to cache only the minimum required information – not passwords or groups.

5.3.3 Print services

Unless required the print services should be disabled by removing the printer line of the inedt.conf file.

5.3.4 IP Forwarding

IP forwarding should be disabled unless the server is required to be a router.

5.3.5 Multicast Routing

Muticast routing should be disabled unless specifically required.

5.3.6 Reducing inetscv

Many sections of this file should be commented out, as they will not be needed, generally this includes DHCP support, named startup support, multicast support.

5.3.7 Network Service Banners

Banners include information about the operating system version and can be of use to intruders. They should be removed from ftp and telnet logins and a new message substituted (see telnet above.) The banner message attached by sendmail to outgoing mail should also be changed to remove reference to the operating system.

These measures provide only a small increase in security, as there are many other techniques to determine the operating system.

5.4 EXAMPLE (GENERAL) HARDENING SCRIPT

This procedure is not all inclusive, and additional hardening steps should be taken time permitting.Information, and automated scripts to accomplish this, are available at http://www.yassp.org/.

- Install ssh. Source is available from ftp.ssh.org. SSH should be installed as the primary remote access mechanism for all production servers. The telnet service should be disabled.
- Deny root telnet login. Make sure the to enable the "CONSOLE" line in /etc/default/login.
- Disable /etc/inetd.conf services that are unnecessary.
- Install sudo. Package is available from http://sunfreeware.com/. Sudo should be configured and the root password secured. Users requiring administrative access should use sudo instead of su. Be sure to enable sudo logging in syslog by editing /etc/syslog.conf to make the /var/adm/messages line look like the following:
  .err;kern.debug;daemon.notice;mail.crit;.notice /var/adm/messages
- No root FTP. To disable use of ftp by root, add "root" to /etc/ftpusers.
- Remove, lock, or comment out unnecessary accounts, including "sys", "uucp", "nuucp", and "listen". The cleanest way to shut them down is to put "*LK*" in the password field of the /etc/shadow file. Also consider using the noshell program to log attempts to use secured accounts.
- Lockdown /etc No file in /etc needs to be group writeable. Remove group write permission via the command chmod –R g-w /etc .
- Disable NFS export NFS exports are controlled by the /etc/dfs/dfstab file. Remove this file. To disable the NFS server daemon, rename /etc/rc3.d/S15nfs.server.
- Log all cron activity Review all the cron jobs by reading the cron file of every system account in /var/spool/cron/crontabs. Consider logging all cron activities by setting "CRONLOG=yes" in /etc/default/cron.

- Disable RPC: rpcbind is the program that allows rpc callers and rpc service provides to find each other. Unfortunately, standard rpc is unsecure. It uses "AUTH_UNIX" authentication, which means it depends on the remote system's IP address and the remote user's UID for identification. Both of these forms of identification can be easily forged or changed. General-purpose systems usually need rpc running to keep users happy. Special purpose systems (web servers, ftp servers, mail servers, etc) can usually have rpc disabled. Be sure to test all the facilities that you depend on to be sure they aren't affected if you turn off rpc. To disable rpc, rename /etc/rc2.d/S71RPC to s71RPC.
  NOTE: Lipposhop's Netbackup solution relies on RPC, so it cannot be disabled without disrupting backup service. Make sure that the firewall is not configured to pass RPC traffic.
- Remove setuid bit from non-critical binaries: Many of the setuid and setgid programs on Solaris are used only by root, or by the user or group-id to which they are set. They can have setuid and setgid removed without diminishing user's abilities to get their work done. Consider each of these programs individually as to their use on your system. Execute *sudo find / -perm -4000 –print* to get a list of setuid files on the system. Create a master list of the remaining setuid/setgid programs on your system and check that the list remains static over time. If this list changes, beware!
- Enable enhanced login logging by creating the "loginlog" file: touch /var/adm/loginlog hmod 600 /var/adm/loginlog chgrp sys /var/adm/loginlog
- Check patchlevel & install patches as necessary Use showrev -p to list patches installed on the system. Check Sun's patch list (www.sun.com) for current security-related patches for the version you are running. Download and install all pertinent security patches. Recheck the patch list frequently. Not all security patches need be installed on every machine. But protect machines, or those with public access, should be kept up-to-date. The patchdiag program that is available on the SunSolve CD and at the SunSolve web site will automatically compare the patch level of a host against the current Sun recommended patch set, and display any differences.
- Create telnetd banners: The banner displayed during a terminal or console login comes from /etc/motd. The default telnet banner can be changed by creating /etc/default/telnetd and adding the "BANNER" variable, as in: BANNER="\n\n This is a secured system. Unauthorized access prohibited. All activity is logged.\n\n" The default ftp banner can be changed via a similar line

in /etc/default/ftpd. The default banner is undesirable because it gives away the OS type of the host system.

5.5 ENABLE HARD TCP SEQUENCE:

In /etc/default/inetinit, modify the variable setting "TCP_STRONG_ISS=2".Firewall Hardening Script

A firewall is only as secure as the operating system it resides upon. At the end of this section is a link to a script that automate most of the armoring process, to include implementing TCP Wrappers, this is recommended for new installations only.

5.5.1 Installation

The best place to start armoring a system is during OS installation. For a firewall, previous installations should not be trusted. The system should be placed in an isolated network not connect an active network nor the Internet, which exposes the system to a possible compromise. To get critical files and patches later, you should use a second box that acts as a go between. The Core installation should be loaded, because this is the absolute minimum installation, and create a more secure operating system, however to use a GUI the 'End User' installation may be needed. Anything above the End User package, such as Developer, is adding useless but potentially exploitable software. Be sure to add the "On-Line Manual Pages" during the install process. For more information on building a minimal installation, refer to Solaris Minimization for Security (http://www.sun.com/blueprints/1299/minimization.pdf .)

During the installation process, you will be asked to partition your system, several partitions are needed to protect the root drive. If the root partition was filled with data, such as logging or email, we would cause a denial of service, potentially crashing the system.

Once the system has rebooted after the installation, install the recommended patch cluster from Sun. Be sure to use your go between box to get the patches, the firewall box should always remain on an isolated network. Patches are CRITICAL to maintaining a secure firewall and should be updated at least once a week

5.5.2 Eliminating services

Armoring consists mainly of turning off services, adding logging, and TCP Wrappers.

By default, Solaris is a powerful operating system that executes many useful services. However, most of these services are unneeded and pose a potential security risk for a firewall. The first place to start is /etc/inetd.conf. This file specifies which services the /usr/sbin/inetd daemon will listen for. By default, /etc/inetd.conf is configured for 35 services, you only need two, ftp and telnet, eliminate the remaining unnecessary services by commenting them out. This is critical, as many of the services run by inetd pose serious security threats, such as rexd. Confirm what you have commented out with the following command:
#grep -v "^#" /etc/inetd.conf (this will show you all the services that were left uncommented)

Next look at /etc/rc2.d and /etc/rc3.d. Here you will find startup scripts launched by the init process. Many of these are not needed. To stop a script from starting during the boot process, place an underscore (_) infront of the name. That way you can easily start the script again just by removing the underscore. The following scripts are not needed and pose serious security threats to your system.

/etc/rc2.d

S73nfs.client	used for NFS mounting a system. A firewall should never mount another file system
S74autofs	used for automounting, once again, a firewall should never mount another file system
S80lp	used for printing, your firewall should never need to print.
S88sendmail	listens for incoming email. Your system can still send mail (such as alerts) with this disabled.
S71rpc	portmapper daemon, a highly insecure service (required if you are running CDE).

S99dtlogin	CDE daemon, starts CDE by default

/etc/rc3.d	
S15nfs.server	used to share file systems, a bad idea for firewalls
S76snmpdx	snmp daemon

Running any GUI (CDE or OpenWindows) is not a good idea. Only run a GUI when it is absolutely required. You can disable CDE, the default GUI in Solaris 2.6, with the S99dtlogin startup script (replace the capital S with a small s).

To determine how many ports and services CDE requires, type the following command when it is running. ps -aef | wc - l

Once you are done with the installation and have turned off S99dtlogin and S71rpc (required to run CDE), type the command again and compare how the number of services have decreased. If only the Core installation was followed, this is not an issue, as the GUI is not installed.

5.5.3 Logging and Tweaking

Once all unnecessary services are deactivated, the next step is to enable logging. Most system logging occurs in /var/adm. We want to add two additional log files there, sulog and loginlog. /var/adm/sulog logs all su attempts, both successful and failed. This allows you to monitor who is attempting to gain root access on your system. /var/adm/loginlog logs consecutive failed login attempts. When a user attempts to login 5 times, and all 5 attempts fail, this is logged. To enable the files, just touch the files /var/adm/loginlog and /var/adm/sulog. Ensure both files are chmod 640, as they contain sensitive information.

Next create the file /etc/issue. This file is an ASCII text banner that appears for all telnet logins. This legal warning will appear whenever someone attempts to login to your system.

We also want to create the file /etc/ftpusers. Any account listed in this file cannot ftp to the system. This restricts common system accounts, such as root or bin, from attempting ftp sessions. The easiest way to create this file is the command: cat /etc/passwd | cut -f1 -d: > /etc/ftpusers

Ensure that any accounts that need to ftp to the firewall are NOT in the file /etc/ftpusers.
Also, ensure that root cannot telnet to the system. This forces users to login to the system as themselves and then su to root. This is a system default, but always confirm this in the file /etc/default/login, where console is left uncommented.

5.5.4 Connecting to Firewall

It is critical that you develop a secured, controlled way to connect to the firewall. Often, you need remote access to your firewall for administration or the uploading of files, these communications need to be secured. Two options are mentioned here, ssh and TCP Wrappers.
Ssh encrypts all communication between you and the firewall. TCP Wrappers will NOT protect your network traffic from sniffing. Users can still capture all of your keystrokes (including passwords) on the network. To prevent users capturing communications to your firewall, replace telnet/ftp with ssh. ssh will encrypt all communications to your firewall, allowing you both to upload files and administer the firewall in a secure manner. ssh is similar to TCP wrappers in that it has its own layer of logging, and can limit what systems can connect to it.

TCP Wrappers, while it does not encrypt, it does log and control who can access your system. It is a binary that wraps itself around inetd services, such as telnet or ftp. With TCP Wrappers, the system launches the wrapper for inetd connections, logs all attempts and then verifies the attempt against a access control list. If the connection is permitted, TCP Wrappers hands the connection to the proper binary, such as telnet. If the connection is rejected by the access control list, then the

connection is dropped. TCP Wrappers are useful even though the firewall does all that for you, to protect against firewall misconfigurations and crashes.

Implementing TCP Wrappers involves editing several files (these examples are based on the advance configuration). First, once compiled, the tcpd binary will be installed in the /usr/local/bin directory. Second, the file /etc/inetd.conf must be configured for which services are to be wrapped. Third, /etc/syslog.conf must be edited for logging tcpd, be sure to touch the file /var/adm/tcpdlog . Last, the access control lists must be created, /etc/hosts.allow and /etc/hosts.deny.

Once all the proper files have been edited and are in place, restart /usr/bin/inetd with kill -HUP. This will restart the daemon with TCP Wrappers in place. Be sure to verify both your ACLs and logging before finishing.

5.5.5 Other important measures

5.5.5.1 WHEEL GROUP

A wheel group is a group of select individuals that can execute powerful commands, such as /usr/bin/su. By limiting the people the can access these commands, you enhance the system security. To create the group, vi the file /etc/group, create the group wheel, and add the system admins to the group. Then identify critical system binaries, such as /usr/bin/su. Change the group ownership to wheel, and the permissions to owner and group executable only (be sure to maintain the suid or guid bit for specific binaries). For /usr/bin/su, the commands would be:
/usr/bin/chgrp wheel /usr/bin/su
/usr/bin/chmod 4750 /usr/bin/su

13. Note: (*Don't forget, for su there is actually another binary in /sbin. Don't forget to change this file also*).

5.5.5.2 LOCK DOWN RHOSTS

Lock down the files .rhosts, .netrc, and /etc/hosts.equiv. The r commands use these files to access systems.To lock them down, touch the files, then change the

permissions to zero, locking them down. This way no one can create or alter the files. For example,

/usr/bin/touch /.rhosts /.netrc /etc/hosts.equiv

/usr/bin/chmod 0 /.rhosts /.netrc /etc/hosts.equiv

5.5.5.3 SET TCP INITIAL SEQUENCE NUMBER GENERATION

Set the TCP initial sequence number generation parameters. By truly randomizing the initial sequence number of all TCP connections, we protect the system against session hijacking and ip spoofing. This is done by setting TCP_STRONG_ISS=2 in the file /etc/default/inetinit. By default, the system installs with a setting of 1, which is not as secure.

5.5.5.4 PROTECT AGAINST BUFFER OVERFLOW

To protect against possible buffer overflow (or stack smashing) attacks, add the following to lines to /etc/system.

set noexec_user_stack=1

set noexec_user_stack_log=1

5.5.5.5 MODIFY IP MODULE

Add these commands to one of your start up scripts. For detailed information on ndd and tuneing ip modules for security, see the Sun blueprint Network Settings for Security.

Set kernel parameters for /dev/ip

ndd -set /dev/ip ip_respond_to_echo_broadcast 0

ndd -set /dev/ip ip_forward_directed_broadcasts 0

ndd -set /dev/ip ip_respond_to_timestamp 0

ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0

ndd -set /dev/ip ip_forward_src_routed 0

ndd -set /dev/ip ip_ignore_redirect 1

5.5.5.6 ELIMINATE UNNECESSARY SUID ROOT BINARIES

suid root binaries pose a high risk, as vulnerable versions can be used to gain root. Since this is a dedicated system with few accounts, most of the suid binaries can be disabled or removed. To find all suid root binaries, run the following command on your system.
find / -type f -perm -4000 -exec ls -lL {} \; | tee -a /var/tmp/suid.txt
Once you have identifed all of the suid root binaries, you can remove most of them by changing the permissions to '555', or deleting the binaries entirely.

5.6 ADDITIONAL STEPS

There are many additional steps that can be taken, such as sudo (allows a system administrator to give limited root privileges to user and log their activities), tripwire (monitor changes in system binaries), and swatch (automated log monitoring and alerts).

The script file below will go through your Solaris system and make all the above changes, first backing up any changed files. The script will also implement TCP wrappers for you. This script detects what processor you are using (Sparc or x86) and what version (2.5.1, 2.6, 2.7, and 2.8) and makes the proper changes. It is recommended for new installs only. Download armor-1.3.1.tar.Z (http://www.enteract.com/~lspitz/armor-1.3.1.tar.Z)
References:

Required Solaris patches: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access

Solaris operating environment minimization for security: http://www.sun.com/blueprints/1299/minimization.pdf

Solaris[tm] Operating Environment Network Settings for Security: *Updated for Solaris 8 Operating Environment: http://www.sun.com/software/solutions/blueprints/1200/network-updt1.pdf*

Solaris Operating Environment Security:

http://www.sun.com/software/solutions/blueprints/0100/security.pdf

6 LINKS

6.1 WEB-SITES

6.1.1 Cryptoraphy

www.bouncycastle.org

Legion of the Bouncy Castle has created a crypto API in Java. This piece of work could benefit one that is in need of implementing some crypto algorithms into own applications. Check the specifications on the site to see what is supported.

ssh.fi crypto-page

SSH.fi has wrapped up a page where it tries to explain cryptography to the reader. It begins with introduction, digs in to algorithms and protocols, and has a reference list + other online resources. Might be very interesting read.

anujseth.com crypto-page

This page is an effort to provide a one-stop-shop for all your cryptography/security related queries. This site has lots of detailed information on topics ranging from the history of cryptography to the latest of crypto algorithms and products to hit the market. Might be interesting read if you're into crypto.

www.pki-page.org

This site digs into Public Key Infrastructure and does it well. Loads of information, not just about PKI, but also on SSL, PGP, crypto articles, RFC's, and much more. A crypto overload..

handbook of applied cryptography

A recommended crypto-book is available for download as e-book, for free! This is a must-read book and I recommend you get it. Perhaps now I finally get to read it :) Paper-back would be much nicer, thought. This book is intended as a reference for professional cryptographers, presenting the techniques and algorithms of greatest

interest to the current practitioner, along with the supporting motivation and background material. It also provides a comprehensive source from which to learn cryptography, serving both students and instructors. (2001 edition)

basic cryptanalysis

This manual is intended as practice material for basic cryptanalysis, originally developed for the army, but apparently it has been available to the public for some time already. This is old material, but should give you some insights about cryptanalysis.

www.ciphersbyritter.com

This site has crypto-resources that help one get some idea what crypto is about. It also hosts a nice 'technical crypto terminology' that tries to tell what some of those neat words mean. And it has lots of resources.

6.1.2 Hacking

astalavista.box.sk

Astalavista is a search engine for exploits and cracks. Especially the exploit part is good for security/pentesters. However, a word of warning, as with Packetstorm, beware of trojanized code. Same warning goes with cracks, those can contain virii so keep your virus definitions updated before running any code provided by these sites.

www.anticrack.de

Anti-Crack is mainly focused on reverse engineering, coding & cracking software. If you are a programmer, this site can wield lots of interesting information. I'm not a coder, so I can't really tell if the information here is good or not.

adm.freelsd.net

This is the page of FreeLSD, a member of ADM hacking group. I listed this page mainly because it had some resources about programming that could be of interest to some people. It contains other stuff too, but it appears FreeLSD promotes safe

programming, that is of course something that is important to security. The site also has links to ADM released hacking tools.

www.lsd-pl.net

LSD-Planet is a group of polish hackers that are well known in the security/hacking community. These guys are very good in what they do and spend a lot of time researching server & network security. They provide exploit code and some tools and have written some good papers about several issues.

www.phenoelit.de

Phenoelit is an experienced group of hackers that based on the site are more focused on network security (hardware, protocols). They have published some papers and tools that can be used to assess networks & protocols + they have done some advisories. They also host the darklab.org mailinglist that is worth checking out.

gb0x.net

This site publishes information about exploits & proof of concept material. They also post some papers on the site that are more related to hacking than securing stuff. The site has a forum available where exploits are discussed. Might be an interesting site for some people.

thehackerschoice.com

This is a german hacking group that research security vulnerabilities and create exploits. They have a nice collection of tools available that you can use to assess some stuff. They also publish papers, thought some of them are written in german.

www.w00w00.org

w00w00 is a global non-profit security team with over 30 participants. They do security-research, make proof-of-concept exploits and release advisories with a tint of humour included.

www.areyoufearless.com

This site focuses on trojans and other malware related stuff. It has also a forum, but only for registered users. I bet there is discussions about the things already mentioned. It could give insights to this part of security / hacking.

www.ccc.de

This is the site for the famous german hacking group called the Chaos Computer Club. It has lots of members but unfortunately the pages are mostly in german. There is a notice on the site that promises there will be more english content at some point.

www.collusion.org

This is a hacking group that mainly share information and write articles, their mission being to learn more information about everything. The area of subject is wide, ranging from playing around with TV to phreaking.

www.i-hacked.com

This site is dedicated to Hardware Hacking. It does not support "Cracking" or "Hacking" into someones email/website/computer. This might be interesting read for those hardware-enthusiasts, and this is also a form of hacking.

www.phrack.com

Phrack is an online zine that allows downloading issues to your own machine for offline reading. Security-enthusiasts and hackers put effort to the articles and release stuff for the community every now and then. Lots of interesting read, I think I have to start from the beginning as I haven't been into security THAT long :) Phrack is considered being one of the best out there.

www.legions.org

Keen Veracity is an online zine that works about the same way as Phrack but apparently has a much smaller contributor base. The information on these zines tend to be a bit humorous and not written that seriously.

6.1.3 Security

www.securityrisk.org

This sites main goal is to provide security information to help the average user to patch operating system flaws. Based on the amount of forum messages, it is a relatively new one. (a friends site)

www.toolcrypt.org

Toolcrypt is a site that focuses on tools for windows and linux (unix) platforms. Pretty impressive ideas and just wondering what the non-crippled versions really are capable of.

www.secureroot.com

SecureRoot is a security-portal with lots of pointers to different resources, like hacking sites, security sites and so on. Quite clean site, and appears well structured. The site also has a forum, but it was down when reviewing the site.

www.windowsecurity.com

WindowsSecurity is a site dedicated to security-related issues with Microsoft server-products, containing articles and tutorials, software categories and a nice whitepaper section.

www.infosyssec.org

This site has loads of links to different sites and resources. It also lists usual mailinglists, vulnerability databases, search engines, antivirus- and OS/software-vendors with links to their patch-pages.

www.sans.org

SANS offers lots of seminars and training-sessions. It also has certification paths that one could follow. It has nice resources available that students/security persons have written, and it has the TOP-20 vulnerabilities listed that most likely are the common reasons for security- breaches if services are publicly available.

www.cert.org - www.cert.fi

CERT is a computer security incident response "team", having local sites around the world. This site reports world-wide if there is any major vulnerabilities spotted that should be fixed. It also has information how to deal with incidents and how to follow best practices to avoid unnecessary compromise.

www.securityfocus.com

This has been an excellent site and hopefully it stays that way and offers free service to the community. Symantec bought Securityfocus and is selling alert-information a few days ahead to companies with fixing information before the information gets released to the public. Hmmm, do I smell something rotten in this? Oh well, if the free services stay, this is overally a nice site. You can search for vulnerabilities, participate in many mailinglists & learn more about several areas (some of them being incident response, forensics, penetration testing and so on). It also has lots of articles/papers published.

www.tietoturva.org

This is a site for Finnish Information Security Association, one of its purposes being to promote it's members educational status in the security-field. They have some basic resources available. This probably mainly interests finns, because the site is in finnish.

www.net-security.org

This site collects some interesting tidbits into their page, news from the world. They also have lots of book-reviews so that might be a place to look for when considering buying a book, it might have a review done on this site. It also lists some vulnerabilities and newly released security-related tools.

www.nmrc.org

Nomad Mobile Research Centre, this group concentrates on security research. They have some interesting papers and projects going on, good FAQs about hacking

several things and provide some tools. The quality is good, and they include welcome humour into the pieces of information they provide.

www.securiteam.com

SecuriTeam is formed by a small group of people from Beyond Security. It is a security-portal that has quite recent and interesting information posted about vulnerabilities, news, tools & papers. One thing that makes this a good site is that they give their expertise in commenting on the information they post. Something that many sites lack.

www.packetstormsecurity.nl

This is a huge site mirrored around the world. It contains lots of papers & publications, and this is one of of the places to come to when you need to find an exploit or specific tool. They also provide links to other sites that could be useful to you.

www.security-protocols.com

This is a semi-interactive portal that concentrates on security. It posts some of the latest happenings in the security-field and contains some sections for tools, tutorials and documents. It also has links to other security-sites and so on.

www.cgisecurity.org

The site focuses mainly on web-security and lists vulnerabilities found on web-servers and technologies like PHP, and so on. It gives good pointers to certain web-servers and applications from the security point of view.

www.blackhat.com

This is the homepage for the Blackhat Briefings. They have a lot of resources on the pages in form of presentations. Of course this material acts only as presentation material, but should give clues where to look for more information on a specific topic.

razor.bindview.com

RAZOR is a team of security researchers around the world. The site has lots of nice tools available and there are also lots of papers, presentations & advisories the group has made. Overally a clean, nice site.

www.ebcvg.com

This is a security-site containing lots of different articles and tutorials regarding security, virii, cryptography and hacking. The site also has own editorials/articles posted and a "security"-shop.

www.infosecwriters.com

A site dedicated for papers and articles written by security-minded people. It also has some other resources, like honeynet-related stuff and forensics. It also has a nice library of documents.

www.security-forums.com

Security-Forums contains many forums with specific topics. If you are interested in swapping security viewpoints with other people around the world via your web-browser, this is one of those places

6.2 TOOLS

6.2.1 Web Applications

web audit library (wal)

It is a python module that provides a powerful and easy API for writing web applications assessment tools, similar to what Libwhisker does for Perl. Wal provides for example send/receive/analyze HTTP 0.9/1.0/1.1, decoders/encoders and more.

lilith

It works as an ordinary webspider and analyses any grabbed webpages. It dissects forms and if requested, inject special characters that have a special meaning to any underlying platform.

httprint

HTTPrint is a tool that does identification of web servers despite the banner string and any other obfuscation. httprint can successfully identify the underlying web servers when their headers are mangled by either patching the binary, by modules such as mod_security.c or by commercial products such as ServerMask.

whisker

Whisker is a tool developed by Rain Forest Puppy. The tool is mainly used to find default files & possible flaws from web-server implementations that one could attack further. It also supports some IDS-evasion techniques, but in assessment tasks that might not be necessary.

stunnel

Stunnel is a program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer) available on both Unix and Windows. Stunnel can allow you to secure non-SSL aware daemons and protocols (like POP, IMAP, LDAP, etc) by having Stunnel provide the encryption, requiring no changes to the daemon's code.

achilles proxy

Achilles is an intercepting HTTP/HTTPS proxy that can be used for hacking/pentesting web-applications. This tool is for Windows-platform and is simple and usable.

form scalpel

The tool automatically extracts forms from a given web page and automatically splits out all fields for editing and manipulation - making it a simple task to formulate detailed GET and POST requests. The application supports HTTP and HTTPS connections and will function over proxy servers. This tool is for Windows.

nikto

Nikto is a web server scanner which performs comprehensive tests against web servers for multiple items, including over 2000 potentially dangerous files/CGIs, versions on over 130 servers, and problems on over 200 servers. This software uses RFP's LibWhisker as a base for all network funtionality (no sense reinventing the wheel), and creates an easy to use scanner.

httpush

HTTPush aims at providing an easy way to audit HTTP and HTTPS application/server security. It supports on-the-fly request modification, automated decision making and vulnerability detection through the use of plugins and full reporting capabilities.

spike

SPIKE Proxy is a similar tool to Achilles and can intercept traffic and let you edit it. You can also get a fuzzer that is trying to attack parameters and make the server in the other end to react in unwanted ways.

httrack

It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.

mieliekoek

Mieliekoek.pl is a SQL insertion crawler which tests all forms on a web site for possible SQL insertion problems. This script takes the output of a web mirroring tools as input, inspecting every file and determine if there is a form in the file.

exodus

Exodus is an intercepting HTTP/HTTPS proxy made purely in Java, and it is self-contained. It works and has some nice features, but lacks the _simplicity_ of editing requests.

paros

This is a java-based intercepting local proxy, a bit like Exodus. It is like a mix between Exodus and Achilles. Testing performed so far gives thumbs up for this proxy, except the logging features seems to be bad. I recommend testing it if you are into web-application pentesting

6.2.2 Wireless

toolcrypt wireless toolkit

This toolkit is built for Windows platform and contains for example WEP key extraction, decryption tools, client and AP analysis tools and other goodies. Might be a nice addition to a Windows WLAN auditing laptop.

airsnort

AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. This exploits the weaknesses in the Wired Equivalent Protocol (WEP).

ap tools

This tool is for identifying wireless access points & what hardware these are using. Might be good for a pentester to spot possible access points into a clients network.

kismet

Kismet is an 802.11 wireless network sniffer - this is different from a normal network sniffer (such as Ethereal or tcpdump) because it separates and identifies different wireless networks in the area. Kismet works with any 802.11b wireless card which is capable of reporting raw packets (rfmon support).

prismstumbler

Prismstumbler is a wireless LAN (WLAN) which scans for beaconframes from accesspoints. Prismstumbler operates by constantly switching channels an monitors any frames recived on the currently selected channel. Prismstumbler will also find

private networks. Since the method used in prismstumbler is receive only it can also find networks with weaker signal and you will discover more networks..

fake ap

Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points. Hide in plain sight amongst Fake AP's cacophony of beacon frames. As part of a honeypot or as an instrument of your site security plan, Fake AP confuses Wardrivers, NetStumblers, Script Kiddies, and other undesirables.

bsd airtools

BSD-airtools is a package that provides a toolset for wireless 802.11b auditing. Namely, it currently contains a bsd-based wep cracking application, called weputils (as well as kernel patches for NetBSD, OpenBSD, and FreeBSD). It also contains a curses based ap detection application similar to netstumbler (dstumbler) that can be used to detect wireless access points and connected nodes

6.2.3 Network

dhcping

DHCPing is a lightweight and featureful security tool written in PERL and designed to test the security of various flavors of DHCP implementations around. Many options allow DHCPing users to craft malicious DHCP/BOOTP packets "a la HPING"

ettercap

Ettercap NG is a network sniffer/interceptor/logger for switched LANs. It uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts. Features character injection in an established connection.

4g8

4G8 is a sniffer for switched networks. It utilizes ARP cache poisoning, packet capture and packet reconstruction techniques, 4G8 works with nearly all TCP, ICMP and UDP IPv4 traffic flows.

arptoxin

ARPToxin is a windows-based arp-poisoning tool, useful for sniffing traffic on a switched network and so on. There are not many tools for windows that perform this kind of functionality.

snort ids

Snort is a open-source intrusion detection system that is developed actively. It is free and could compete with some of the commercial products. Maintaining snort is a bit harder, but it does what it is supposed to do.

www.whitehats.com

Whitehats has alternative snort-signatures available on their site. Check them out if you happen to like them. This site has also other information & resources available so its anyways worth checking out.

firewalk

Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device will pass. Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway. To get the correct IP TTL that will result in expired packets one beyond the gateway we need to ramp up hop-counts. We do this in the same manner that traceroute works. Once we have the gateway hopcount (at that point the scan is said to be `bound`) we can begin our scan.

hping3

hping is a command-line oriented TCP/IP packet assembler/analyzer. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

fragroute

Fragroute is an IDS stress testing tool and verification tool. It has a rulebase it acts on and sends "attacks" against specified hosts. IDSes should pick these up and generate alerts and so on.

snot

Triggers snort alerts taking a snort rules file as input. Use to decoy your IDS. This version now allows for non-randomised payloads, to inflict more damage on the dumber IDS'. Decoy & stress-testing tool.

nmap port scanner

Here you can find Fyodor's NMAP-tool that you can use to portscan targets. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

ethereal

Ethereal is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. This tool can analyze tcpdump-compatible logs.

hunt

Hunt is a TCP/IP protocol vulnerability exploiter & packet injector. This could be used to evaluate firewalls, routers and so on. I haven't personally tested this, but is definitely one that I'm going to look at.

nemesis

Nemesis is a packet injection suite that supports protocols ARP, DNS, ETHERNET, ICMP, IGMP, IP, OSPF, RIP, TCP and UDP. This might be a good tool for enumerating a network consisting of firewalls, routers and so on.

domtools

Domtools suite can be used to enumerate DNS-servers. In the context of security, this could be an efficient tool for checking if the servers allow zone transfers of private addresses and so on.

phenoelit router tools

Phenoelit has lots of router specific enumeration and exploitation tools available that can be used to assess network specific stuff. They also have some brute-forcers for telnet, ldap & http.

dsniff

Dsniff is a collection of tools for network auditing and penetration testing. Passively monitor a network for interesting data (passwords, e-mail, files, etc.). Facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2

switching). Implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

netcat - unix , win32

Netcat is a multipurpose tool that you can utilize for many things. I recommend this tool warmly, as in my opinion, its good :)

Alternatives:
SoCat
CryptCat

6.2.4 Miscellaneous

patchfinder 2

PatchFinder2 is a W2K-utility for detecting W2K-based rootkits that work via DLL-injection or kernel-level attacks. Might be very useful if you suspect a break-in.

the coroners toolkit

The Coroner's Toolkit is a toolkit for forensics analysts. Notable TCT components are the grave-robber tool that captures information, the ils and mactime tools that display access patterns of files dead or alive, the unrm and lazarus tools that recover deleted files, and the findkey tool that recovers cryptographic keys from a running process or from files.

chkrootkit

Chkrootkit is a rootkit discovery tool. It can at the moment detect 44 rootkits, worms & LKMs. If you suspect you have been hacked and someone is using your system, check this tool out. This tool works on several unix platforms.

www.foundstone.com

Foundstone has released a variety of free tools to the community. The tools include forensics-tools, assessment-tools, intrusion detection tools, scanning tools & stress testing tools. You might find something useful in here.

[@stake tools]

@stake also provides some freely downloadable tools. The tools range from Information Gathering to Recovery & Restoration, both for unix & windows. Check it out, you might find something useful.

[sql security scripts]

SQLSecurity has collected some useful MS-SQL scripts & tools on their page that can be used to enumerate MS SQL servers and check security of the databases. Might come handy.

[tscrack]

TScrack is a wordlist-based terminal server login-cracker, developed by gridrun. This tool basically hits a terminal server by using a wordlist. If you need to enumerate passwords and terminal services is enabled, this is one way to go.

[john the ripper]

John the Ripper is a password-cracking tool that can use wordlists and brute-force. The tool is available for unix, dos & windows. It also has plugins for other schemes, like cracking NTLM hashes.

[its 4]

Cigital has released a C/C++ source-code analyser that scans for possible vulnerabilities. Might be useful in automating the process of auditing C/C++ code and useful for programmers themselves.

[unxutils.sourceforge.net]

These Win32 tools work like their unix-equivalents. Might come handy at some point and if you miss those simple unix-tools, you can now get them on Windows :) Check out what the tools are from the site.

[net calculator]

This site has a neat network calculator. It might come useful to people like me who don't understand how netmasks really affect to the amount of IP's in a subnet (or how to calculate this).

blacklisted ip addresses

This server hosts a huge IP block list that contains advertisers, spammers and many other intrusive IP-addresses that are found to be static to some extent. You might want to use the list in your setup to kill those popups or attempts to connect to some spyware servers

6.3 RESOURCES

google search strings assist in auditing

This site contains loads of google search strings that can reveal sensitive information on a site. A nice addition to put in use, maybe some day there will be a tool automating these.

soap web security

The purpose of SOAP is to allow various components to communicate using remote functionality as if they were local. This paper explains some types of attacks and defenses based on the SOAP implementation. it also acts as a nice small primer to SOAP.

ldap injection (spidynamics)

LDAP injection is the technique of exploiting web application that use client-supplied data in LDAP statements. This paper points out that even the LDAP requires proper input validation when implemented into a application.

oracle row level security - part I , part II

In this article serie Pete Finnigan explains what the row level security feature in Oracle database is, and how it is used for added security. He also explains how to audit these policies.

advanced xss attacks

Gavin Zuchlinski has written a paper about advanced cross-site scripting attacks that use POST instead of GET, with some nice examples. Interesting read, and broadened my vision a bit, again. Short but good paper.

sql injection paper (securiteam)

SecuriTeam has released an SQL injection paper that is quite good. This should help you grasp the basics of SQL injection techniques, especially if you do pentests against web-applications.

advanced sql injection paper (ngssoftware) - part I , part II

NGSSoftware's SQL injection papers. The first paper focuses on ASP/MS-SQL issues and is quite throughtout with the details. The second paper is an addennum to the first, and clarifies some issues that was not perhaps that clearly explained in the first paper.

cross site scripting faq

This paper is about Cross Site Scripting and explains to the reader what an XSS is about and why it is dangerous, giving some examples. This is a good briefer into the XSS-attacks.

fingerprinting port 80 attacks - part I , part II

In these articles is shown what actual attacks would look like in the web-logs and gives some examples what to expect. Why I posted these is that they give also clues of possible attack methods.

practical auditing of http (summercon, sensepost)

Another paper from Sensepost about practical auditing of HTTP, this paper basically digs into mapping HTTP-servers and how to dig information out of the boxes, looking for more clues and sensitive data.

application security assessment

This paper gives input on a broad detail what kind of attacks custom-made applications are prone to. I considered this to be a link into the penetration testing side because it gives one an overview what kind of stuff you can pull against a web-site or application.

url encoded attacks

This paper focuses on how to handle the usage of Unicode, web encoding, percent-encoding, escape-encoding and UTF encoding that are used interchangeably. This document aims to enlighten developers and security administrators on the issues associated with URL encoded attacks. It is also important to note that many of the encoding methods and security implications are applicable to any application accepting data from a client system. This paper is a very good point for a penetration tester and understanding this is crucial for successful testing.

sql injection paper (sans)

This is yet another SQL-injection paper. Why I decided to post this is because it breaks down quite clearly what is happening in the application/db while doing the magic. It also has a quite nice reference-list in the end that was used when writing this stuff up + personal testing.

pentesting for web applications - part I , part II , part III

This three part article explains some web application behaviour and how that can be exploited. Good reading for penetration testers at it gives a good oversight of what web application hacking is basically about.

blindfolded sql injection

This whitepaper explains how it is not always necessary to have descriptive error-messages to perform successful SQL injection attacks. It is clean and written well.

others

exploiting cisco routers - part I , part II

This article-serie shows some methods of enumerating and exploiting Cisco routers. Good read for those that require network device knowledge, but has never had the chance to experiment.

attacking the dns protocol

This paper explains pretty well some of the attacks plaguing the DNS protocol. Attacking DNS for zone transfers, cache poisoning and so on might not be the most common practice in audits, but it is good to be aware of these kind of attack possibilities.

broadening the scope of pen-testing techniques

Ron Gula lists 14 different things in this paper, that are quite often overlooked in penetration tests. Quite informative paper that deals with both the cons and pros of each step, and had good insights about the interaction between client and testers.

penetration testing on 802.11b networks

The paper explains some things about wireless LANs and then starts moving forward with getting the correct equipment, wardriving and penetrating the wlan. It also states some security recommendations that should be taken in account when dealing with wireless networks.

neworder.box.sk

New Order hosts lots of tools and keeps track of exploits. It is also posting security-info and lots of articles. From here you might find the right tool, paper or exploit to get you going with the task you have.

hacking guide (roelof temmingh)

Roelof Temmingh's excellent "paper" of hacking techniques, I recommend reading this one. It contains a bit humor and pretty nice description of what one would really do when h4x0ring/pentesting away.

attacklab

This paper focuses pretty well into how one can build a good penetration testing lab. If you are in a need of one and do have lots of money to spend, check this paper out :) It gives also clues how to make a little bit smaller but effective lab with less resources to spend.

assessing security

This paper gives input on a broad detail what kind of elements should be considered when you should assess your own security. This gives an overview to a pentester what the customer might expect to get from the team, especially important if you are a starting company and do not really have a clue yet.

ip spoofing introduction

This OK paper touches IP & TCP, as these are vital ones in understanding what IP spoofing really is about. The paper kindly explains several scenarios and why these are possible. The technique does not allow for anonymous Internet access, which is a common misconception for those unfamiliar with the practice. Perhaps finally those people start to understand.

hping2 primer

This paper is a nice primer to a tool called hping. It gives you some impression what you could do with it and explains in a simple way how a blind port-scan can be performed. I recommend this paper if you haven't played around with hping yet.

icmp attacks

This paper focuses a bit on ICMP-related attack methods and explains briefly what happens in the attacks and what these attacks can be useful for. It also has some nice references.

dns cache poisoning

This paper focuses on DNS cache poisoning attacks in quite in-depth style, explaining recent problems with DNS. It also has a nice reference-list to DNS-related stuff. Read this up if you're worried in DNS issues or need to get a hang of it for testing the security of DNS.

hacking with google

This is a paper written by mowse. He goes into great detail how you can use a search-engine for penetration testing. Definitely something that can be used when assessing the security of a publicly available service. It also gives tips how to prevent this kind of exploitation.

wireless penetration testing

This is a paper also written by mowse. The paper illustrates various methods how a wireless network can be assessed. This should give you enough information and clues what you could do while assessing the security of a wifi network.

oracle security testing

This site has loads of links to Oracle-related security papers, giving lots of information about how to test the security of Oracle databases & how to secure them. Very good resource if you got a database to secure or audit.

red team assessment paper

This is a student pentest-paper about demonstrating weaknesses in the security architecture proposed by Parliament Hill Firewall Practical #0063. The paper is written quite well and contains interesting scenario how to attack the system.

ollydbg

OllyDbg is a 32-bit assembler level analysing debugger for Windows-systems. Emphasis on binary code analysis makes it particularly useful in cases where source is unavailable.

analysis of the exploitation processes

This paper describe in details the how to exploit the most common security vulnerabilities in software: Stack overwrite, Heap overwrite, Function pointer overwrite, Format strings. All exploit methods are explained in detail, and example code example is given.

how to create an icmp based client/server connection backdoor

This paper will introduce the reader to an ICMP communication type (this is done by hooking a particular syscall). With this technique is possible to start a communication client/server without open a port on the remote system. A basic knowledge of C language and of syscall hooking is required.

introduction to shellcoding for overflow exploiting

This paper will introduce the reader to the shellcoding and the study of buffer overflows. It will guide the reader in the creation of a shell code from the source C code to a string ready to use in exploits.

pc assembly tutorial

PC Assembly Tutorial tries to give clues how to program in assembly-language and work as a primer. This could be useful for people trying to understand exploits and possibly create them.

smashing the stack for fun and profit

Aleph Ones paper goes through the necessary information that one needs to be able to understand buffer overflows. It breaks things down in a clear manner and explains things like the stack pretty well.

oss.coresecurity.com

Core Security offers some components used in CORE IMPACT to the community for free. These are written in Python and covers packet capture, assembly code and network protocol dissection and build.

valgrind

Valgrind is a tool to help you find memory-management problems in your programs. When a program is run under Valgrind's supervision, all reads and writes of memory are checked, and calls to malloc/new/free/delete are intercepted.

memfetch

Memfetch is a handy utility for dumping the memory of a running process. helping you recover information that would otherwise be lost, and making it easier to check the integrity or internals of a running process.

defending against stack & heap overflows

This article focuses on a deep level how to defend against buffer overflows (stack & heap). This might be an useful article for a seasoned programmer, and is for a change securing stuff instead of exploiting stuff.

badc0ded

This site focuses deeply on exploiting buffer overflows and other vulnerabilities in code. Very good read if you are a programmer and might get one to understand buffer overflows even if the papers are quite technical.

gera insecure programming

This site also focuses deeply into programming errors and how to exploit those. As I'm not a programmer, I can't provide much more information, but that it feels pretty good, as badc0ded.

shatter

This paper digs into Win32 API exploiting to possibly do priviledge escalation. This explains how Win32 messaging system works, and why it is vulnerable. Interesting read and is not so technical that it would go over one's head too easily.

buffer overflows for dummies

This paper takes a more "humane" approach to buffer overflows and if you are a newbie programmer interested in the area, this could get you into the loop quite fast.

inside buffer overflows

This paper is also from SANS and digs into buffer overflows. It explains various stuff the earlier paper didn't explain, about different ways of handling information in the memory and so on.

www.netric.org

This site hosts lots of shellcode/exploit related stuff and thats the reason I rather put this in the hacking section than in the Security-sites sections. It also has papers and own advisories listed.

Last Updated (Thursday, 21 October 2004)

whois and other digging tools

These sites provide online tools for whois, DNS resolve and other similar basic tools. Good for information gathering.

www.whoisfinder.com
www.allwhois.com
www.norid.no
www.dns411.com

vulnerability databases

icat.nist.gov

ICAT is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information. It is based on CVE. This might come handy when doing vulnerability assessments and you need to find out if a specific software is vulnerable to attack.

cve.mitre.org

CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. It tries to make it easier to share data across separate vulnerability databases and security tools. In the sense if many products use the same CVE entries for specific vulnerabilities, one using many of these can correlate the results.

www.osvdb.org

This is an unbiased, vendor neutral vulnerability database that aims for full disclosure. It is similar to www.securityfocus.com or www.securitytracker.com. You might find something here that is not dealt with on the other lists.

others

it security cookbook

This site hosts the IT Security Cookbook. This book aims to touch various issues from policies to more technical level information like firewalls and respective topologies. The technical part doesn't go THAT deep that it would give hands-on information, but is anyways good read to get a understanding about the issue.

network security library

This is a network security library. It has lots of FAQs, articles and papers hosted. It also covers some "books" that are available in digital format. I see this as a good resource, as the stuff on the site is quite good quality. You can find information on lots of topics.

www.cotse.com

This site has good online tools, like name lookups, traceroute, proxy checks and so on. It also has loads of information of networking protocols and hosts the Internet Encyclopedia. There is also a plethora of tools listed on the site that can come handy at some point.

nist publications

This page holds the special publications of NIST that are mainly guidelines. You can find lots of interesting information from here that can be useful, for example you can find tips for securing public webservers, information about IDSes and so on.

isc.incidents.org

This is the Internet Storm Center. The site gets data around the world and maps the most attacked ports on the internet. They also provide analysis information about

worms, virii & exploits when these get wide-spread. You can also find some news on the site.

www.proxyblind.org

Proxy Blind is dedicated to all the people who have an interest in security, privacy, and anonymity. This site has some tutorials about privacy and has proxy/security tools available. There is also a forum where you can discuss privacy issues

7 TEAM

A-Z: Ascending Order

7.1 AUTHORS

Not yet 30, **Balwant Rathore** this time is into the invention of ISSAF along with team OISSG after his numerous award winning tasks in an Indian Police organization. He is founder member of OISSG and currently acting as President.

His contribution to technology standards involve frequent participation as both a speaker at conferences as well as a writer on information security for publications such as Inform-IT, Voice&Data and Network Magazine etc..

Mark Brunner

Mark Brunner is a graduate of Seneca College of Applied Arts and Loyalist College in Toronto Canada. As the Security Incident Response Coordinator for the Canadian Imperial Bank of Commerce, he is mandated with managing and coordinating response efforts for one of the largest and most respected financial institutions in the world. Mark has worked at Symantec Corporation, and taught at Seneca College during his 25+ year IT career.

Mark's broad experience in Information Technology was gained by working in the trenches for multi-national law firms as well as local Toronto system integrators, scaling from single, small, local area networks to complex networks with global points of presence. Mark has worked with many security technologies, but has focused more on policy, process and procedure development, preferring the management of tactical and strategic elements. He has designed change management programs, information security strategies, and computer incident handling procedures. Mark currently holds several vendor specific certifications, and holds an SSCP designation from ISC2.

Miguel Dilaj Born in 1971 Started using computers in 1982 (venerable C64). Migrated to Amiga in the late 80's (still have and use regularly a PowerPC Amiga) Became involved with PC and AS/400 in the 90's. First serious use of Linux in 1998 (RedHat 5.1), tried FreeBSD, NetBSD and OpenBSD and fall back to Linux RedHat-based, Slackware-based and Debian-based distros tried. Currently using Debian-based, Continuous Windows use from 3.0 up to XP Pro Became deeply into IT Security in '98, when it started to be possible to have real control of the situation (i.e. Linux!) Started training other people in Linux and IT Security in 2000, currently working in the Quality Assurance and Automation fields (Computerized System Validation) Interested in clusters and their use for password auditing.

Omar Herrera

Omar was born in 1976; he started as an independent computer virus researcher and

antivirus programmer in the early 90's. He has worked as information security consultant with Insys and later with Deloitte in the areas of risk analysis, security auditing and penetration testing. He is currently working at Banco de México, where he is responsible for the incident prevention and response team, internal security assessments, intrusion detection and malware analysis. He holds the CISA and CISSP certifications

Piero Brunati

Co-founder of Nest (www.nestonline.com) where he performs Research, Ethical Hacking and develops software, he tries hard to mitigate customers' nightmares. He begun butchering computers since the good old 70's, when he spent his first salary to buy the components he used to solder his first computer (8008 CPU, 2k static RAM, 2k EPROM, serial and parallel I/O).

Rama K Subramaniam

Rama Subramaniam is Director of Valiant CISSTech and Tejas Brainware Systems, based in Chennai, India. His companies provide information security consulting, assurance and training services across different countries in Asia and he currently serves as Vice-President (Accreditations) of OISSG. He is former Global Chair of E&A Group of GAISP and has served on boards of Chennai and Dubai Chapters of ISACA and was Charter President of the first ISSA chapter in India. He is a doctoral research scholar in the area of digital forensics and cyber crimes at the University of Madras.

Subash Raman

Realizing that being the sharpest knife in the cutlery board could end up leaving one on the cutting edge as a bleeding specialist, Subash turned his sights to a more appropriate role as an agent provocateur. In a career spanning various verticals including manufacturing, banking, hospitality, shipping across the globe, he has constantly sought to shape his experiential insights into contributions that can help data transform to the value added asset it is when used for informed decision making. Currently he is based in Woodbridge, in the cold frozen tundra that lies north of Toronto. In his role as a business transformation specialist he constantly depends on the Information part of Technology, and is grateful that OISSG is around to keep him from having to focus on the means instead of the ends.

On being inducted into the OISSG, he did have this to say "When the landscape begins to look no place like Kansas, one could use a yellow brick road I guess".

Umesh Chavan

Umesh Chavan has nearly nine years of experience in Information Risk, Network & Security Management and holds a CISSP. He is currently working as a consultant with i-flex Consulting. He has been involved in the ISSAF framework right from its conception and continues to enjoy working on the framework with the same zeal and enthusiasm since the day it was started.

He has worked with various companies in different roles involved in technical systems administration to managing projects and acquiring certifications. This has given him a unique blend of technical & process knowledge. His strengths are thinking out of the box, positive attitude & high-level of initiative. His hobbies include traveling, biking & photography.

7.2 KEY CONTRIBUTORS

Arturo Busleiman is an Independent Professional that has dedicated his life to Development and Information Systems Security. At the early age of 12 he began his career in the GNU/Linux world and has actively contributed with software, audits and patches to many of the most important projects of the Free Software Foundation and derivatives, like Samba, Nmap, Audacity and MPRL. Meanwhile he dictated Security seminaires and courses, and written copious documentation, always with a Free Software and Open Source perspective, having contributed this way to the current position of the Argentinian Free Software market, where "Buanzo", as he's called by members of the corporate environment and FOSS community, is recognized as a referent of GNU/Linux.

Christian Martorella comes from Argentina, he has 9 years of experience in IT, most of it is into Information Security; where he is expert in the area of Security Assessment.

Right now he is working as Tiger Team Leader in a information security firm in Spain and tests security of big government organizations.

He is board of director of OISSG, leads Barcelona local chapter and organizes FIST conferences in Spain. A frequent participants and collaborator in open source projects and speaks at several security conferences. He also holds industry standard certification like CISSP and others.

Dieter Sarrazyn has been an information security consultant and trainer for more than 6 years now. He is a certified and experienced Professional in the areas of creating secure information systems and network architectures, Performing Security Audits of Systema and Network infrastructures, performing penetration tests and installing and configuring firewall and VPN solutions. Dieter has earned the following certifications: CISSP, GSEC, GCIH, CCSA & CCSE.

Hernán Marcelo Racciatti is an independent security researcher who lives in Buenos Aires, Argentina. He currently works as an Information Security Consultant, giving advise to public and private companies, conducting controlled penetration tests, and as speaker in IT Security related events and conferences.

Karmil Asgarally has more than 8 years experience as both a financial auditor and an IT auditor. After working for Andersen Worldwide and KPMG, he obtained exposures in Mauritius, the African continent and the Middle East region from both a business and security perspective. He is currently working with an Oil Company in the United Arab Emirates. He holds ACCA, CISA, CISSP and CISM qualifications.

7.3 CONTRIBUTORS

Andres Riancho
Anish Mohammed
Arshad Husain
Bernardo Reino
Bob Johnston
Clement Dupuis
David Stern
Dhanya Thakkar
Dharmesh Mehta
Diego San Esteban
Dragos Ruiu
Frank Sadowski
Gabriel O. Zabal
Galde Edgar
Gareth Davies
Hamid kashfi
Hari Prasad
Hiten Desai
Jayesh Thakur
Jeremy Martin
Joel Weise
Kalpesh Doshi
Kartikeya Puri
Krishnakant Duggirala
Laurent Porracchia
Major Gajendra Singh
Niels Poulsen
Niloufer Tamboly
Oliver Karow
Oscar Marín
Param Singh
Pieter Danhieux
Rahul Kashyap
Rajendra Armal
Richard Gayle
Richard Zaluski
Rocky Heckman
Ross Patel
S. Saravanan
Salman Ashraf
Saman Ghannadzadeh
Samir Pawaskar
Sandhya Kameshra
Soorendrana
Travis Schack
Vicente Aguilera
Vicente Diaz
Vinay Tiwari
Viraf Hathiram

A-Z, Ascending Order

8 FEEDBACK FORM

To improve the usefulness of ISSAF please take a moment to evaluate it. Your feedback is invaluable to OISSG's efforts to fully serve the profession and further ISSAF releases.

Please complete this feedback form and send it to issaf-feedback@oissg.org If you can't fill this form, we will also appreciate a quick email.

The material in ISSAF were:	**OFTEN**	**Some Time**	**Rarely**
Detailed enough?			
Too much in Detail?			
Not Detailed?			
Easy to use?			
Easy to understand?			
Well Designed?			
The Practicality of inputs in ISSAF were			
Very helpful			
Helpful			
Not very helpful			
The Design of the ISSAF were			
Very Nice and neatly arranged			
Not Designed and Organized			
Just Arranged and Organized			
Which is the section/topic/material needs improvement and what (please describe)?			

Which is the section/topic/material was useful (please describe)?
Overall How ISSAF can be improved to better satisfied your needs?
Others:

Please provide us any specific comments and/or suggestions you may have concerning errors and omissions, enhancements, references and format.	
Page No.	**Description**

If you wish please include your Name, Address and Contact Phone Numbers so we may follow up with you for betterment of ISSAF.

If you have any sanitized data or case study information that you could share with us or with the broader base of ISSAF users, please send it at issaf-contact@oissg.org

Thanks for your time and patience and kind to give this feedback.

Feedback: issaf-feedback@oissg.org
Support: issaf@oissg.org