CONFIDENTIAL

Mediterranean Region:
Security Penetration Test

Request for Proposal (RFP)

AXA Mediterranean Region

April 2008

Table of Contents

1 GLOBAL INTRODUCTION

1.1 COMPANY BACKGROUND

The AXA Group world - wide ranks among the world's leading financial protection providers.

Financial Protection involves offering our customers – individuals as well as small, mid-size and large businesses – a wide range of products and services that meet their insurance, protection, savings, retirement and financial planning needs throughout their lives.

The Group operates in both domestic and international markets: large international risks, assistance and reinsurance.

It has locations in approximately 60 countries and numbers some 120,000 employees (*) around the world. The AXA Group manages assets over 1 315 billion Euro (**), with 50 million customers world-wide.

(*) Excluding Winterthur
(**) Including Winterthur

Further information can be obtained from the company web site www.axa.com

Core Business: Financial Protection and Wealth Management

One Ambition: becoming the preferred company in our industry by 2012, by differentiating ourselves through the quality of our products and care as well as through our service and superior performance.

Values: The AXA values are an integral part of the AXA Vision. The Group is committed to aligning its business practices with its five core values:

Team spirit
Integrity
Innovation
Pragmatism
Professionalism

Commitments: AXA 's commitments to its stakeholders (customers, shareholders, employees, business partners, the broader community and the environment) attest to the Group's desire to contribute to the sustainable development of the communities in which it does business.

Sustainable Development at AXA:

AXA's approach to sustainable development is consistent with our responsible corporate culture. Accordingly, we have made commitments to our key stakeholders. They are set forth in the institutional pillar of our sustainable development strategy and concern human resources and human rights, clients, shareholders, the community and philanthropy, the environment and suppliers.

Managing client risk and our commitments to them over the long term lie at the heart of our business. The business pillar of our sustainable development strategy seeks to integrate the major social, environmental and governance challenges into our vision of Financial Protection. To this end, we are developing:

- Risk prevention in property-casualty insurance
- Raising awareness of the challenges of financing retirements in life insurance and savings
- Responsible investment in asset management through the integration of sustainable development criteria

1.2 AXA MEDITERRANEAN REGION

AXA Mediterranean Region comprises the countries of Portugal, Spain, Italy, Greece, Morocco, Turkey, and Gulf countries, with 8000 employees and Gross Revenues of 7.52 billion Euro (2007 data).

AXA Mediterranean Region represents 8% of the total Gross Revenue of AXA Group.

Jean Raymond Abat is the Mediterranean Region CEO

1.3 PURPOSE OF PROPOSAL

Objectives:

The main objective is to carry out an inter-country penetration test comprised between five companies. The contracted service must demonstrate eventual vulnerabilities and propose a remediation plan.

Tests must be carried out from the outside without granting any specific rights, simulating the situation and conditions of a hacker. For efficiency and cost purposes, the “White Box” method will be used and exposed IP addresses will be provided.
Five non disclosure agreements must be signed for each entity.

Scope:

The scope comprises two levels of testing, the first at network level where all open ports must be challenged and the second at the application level testing exposed Web Applications and Web Services for most common vulnerabilities (SQL Injection, Cross Site Scripting, etc.). The total number of IP addresses is 77**:**

- Greece: 10
- Italy: 10
- Morocco: 10
- Portugal: 17
- Spain: 30

Methodology:

The provider must comply with open source methodologies ISSAF (Information Systems Security Assessment Framework) and OSSTMM (Open Source Security Testing Methodology Manual).

Results and Reporting:

While a great deal of technical effort is applied during the testing and analysis, the real value of a penetration test is in the report and debriefing that must be delivered at the end. If these are not clear and easy to understand, then the whole exercise is of little worth.

There must be six reports, one with a consolidated view, and five other for each country under the test scope. Each report and debriefing should be written in English language and broken into sections that are specifically targeted at their intended audience. Therefore each report must include the following sections:

- **Executive summary:** business risks and possible solutions clearly described in layman's terms;
- **Management summary:** broad overview of the situation without getting lost in detail;
- **Technical:** a remediation plan with a detailed list of vulnerabilities to address and recommended solutions.

Specific Clauses:

- The service provider proposes or accepts that a Controller is appointed to supervise on site all the actions;

- The service provider must provide detailed *Curricula* of all the staff involved in the test;

- The service provider undertakes to ensure that the operations are performed by a fixed team, predefined according to the following criteria:

  - The team is composed solely of members of staff on permanent contracts;
  - No sub-contractor or partner of the service provider must be used within the framework of this service, or specific conditions apply.
  - The team must not be modified during the service delivery (other than in the event of a major force and with prior notification).
  - Any disclosure of information or attempt to impede compliance with the terms of the agreement by one or more members of the team will be subject to internal sanctions from the service provider.

- The service provider must respect the basic code of ethics:

  - Avoid any test which may cause irreparable damage to or financially prejudice the information stored, processed or transmitted using the system under test.
  - Do not destroy or alter the information stored, processed or transmitted using the system under test, unless explicit agreement has been obtained.
  - Do not disrupt operational service, unless explicit agreement has been obtained.
  - Do not divulge sensitive information during or after a test, and do not leave the system exposed after penetration.

- Never publish or otherwise make available the techniques and procedures used to simulate intrusions.
- Clean up fully after the tests (delete backdoors, sniffers and other tools used for the tests);

- The service provider proposes a structured (i.e. defined in work packages) and transparent approach to the tests. It specifies where the tests will be conducted. It undertakes not to take advantage of the rights accorded to it within the framework of the service provided, or to undertake investigations into domains other than those agreed, and in particular for a third party, without obtaining prior agreement;

- High risk scenarios (to be defined) must be tested in a non-operational environment;

- If the service provider proposes recurrent system test scenarios as a result of new vulnerabilities discovered by its monitoring team, it must provide the means of distinguishing an attempted intrusion from a test conducted by itself;

- The service provider guarantees that it has the full legal and contractual right to perform the tests;

- The service provider spontaneously proposes an acceptable confidentiality agreement. In particular, it undertakes to divulge information relating to the service provided only to those persons who have a need to know and with explicit authorization of the contractor

All documents provided during the assignment shall be written in English.

You may add any additional information and document that you think will be useful for the understanding and assessment of your services.

You are invited to submit a response to this Request For Proposal ("RFP") for "Mediterranean Region: *Security Test Penetration"*.

This document and its attachments contain the instructions, information and specifications necessary for your Company to respond to our questions and statement of requirements. Your bid will be evaluated on several criteria, including but not limited to cost, quality of service, reactivity, flexibility, coverage and geographical reach. AXA's overall objective is to receive the highest possible quality of service while optimising cost and limiting exposure to risk.

1.4 VALIDITY OF BID - CONFIDENTIALITY

The terms of this RFP and all other information provided with this request, are to be treated by your Company as confidential and proprietary to AXA. These materials are to be used solely for the purpose of responding to this inquiry. Access shall not be granted to additional parties except with prior written consent of AXA and upon the written agreement by the intended recipient to treat the same as confidential. AXA may request at any time that any of its material be returned or destroyed.

All proposals must be considered final offers. Any proposal contingent upon further approval or review will be considered invalid. Withdrawal of any proposal must be made in writing and submitted to the persons in charge of this RFP:

The person/s in charge of this RFP are:

- António Campos Dionísio
  AXA Mediterranean Region
  Regional IS & BC Competence Center Office
  Information Security Manager
  Praça José Queiroz, nº 1 – Portaria 2 - 1800-220 Lisbon (Portugal)
  Tel.: + 351 218 547 536
  Fax: + 351 218 547 669
  E-mail: antonio.dionisio@axa-seguros.pt

- Gilberto Sequeira
  AXA Mediterranean Services, AEIE, Sucursal em Portugal
  Procurement Manager
  Tel.: + 351 21 350 6950
  Fax: + 351 21 350 6136
  Praça Marquês Pombal, 14 -3º 1250-162 Lisboa (Portugal)
  gilberto.sequeira@axa-seguros.pt

All the information, questions or other will be sent to each of these persons.

1.5 INSTRUCTIONS

1.5.1Response format

AXA requests both electronic and hard copies of all proposals.
Electronic responses must be send through eSourcing AXA Group tool, no later than 5th May, and, also must be sent by e-mail and by post one hard copy to the following address

Portugal
Gilberto Sequeira
AXA Mediterranean Services, AEIE, Sucursal em Portugal
Praça Marquês Pombal, 14 -3º
1250-162 Lisboa
Portugal
gilberto.sequeira@axa-seguros.pt

1.5.2 Questions

AXA welcomes questions regarding the contents of this RFP and encourages you to obtain clarification where appropriate.

All questions relating to this RFP should be directed to all the following contacts:

- antonio.dionisio@axa-seguros.pt
- gilberto.sequeira@axa-seguros.pt

Please refrain from making inquiries on the evaluation of your proposal. Questioning any other AXA or AXA employees may result in the invalidation of your company's bid.

1.5.3 Submission Requirements

If this RFP states a requirement, term, or condition to which the Supplier takes exception, such requirement, term or condition must be identified in the Supplier's proposal and the Supplier must explain the exception and propose an alternative to the specific requirements, terms or conditions. AXA will assume that any requirement, term or condition to which the Supplier has not taken written exception is acceptable.

1.5.4 Deadlines

Request for Proposal send to potential providers:	21 April 2008
Answers sent to AXA:	05 May 2008
Final decision and communication to finalist provider:	12 May 2008
Start Date (Test):	19 May 2008

Your response shall be registered no later than May 5th, 2008.

1.5.5 Selection Process

a- Selection of the short listed suppliers

After analysis of the answers, the suppliers with the highest note in the evaluation template will be short listed and will participate in the next negotiation rounds.
In order to have the chance to be short listed, the suppliers have to be best ones on a certain number of criteria.

b- Selection of the selected suppliers:

Please find hereafter most of the AXA criteria which will be considered to choose the selected suppliers:

- The quality of the answer
- The transparency of the answer (total man-days of expected workload and split per profile, pricing, …)
- The competitiveness of the offer
- The geographical coverage of the suppliers (international reach and coverage of Med Region)
- The financial situation of the supplier
- The capacity to deliver the expected quality/service in the requested delivery time
- The capacity to respond to emergency situations (flexibility and reactivity)
- Qualification and proven expertise
- To be certified
- Fulfilling our requirements
- Resources allocated to the project

The position of these criteria on the list does not represent any prioritisation.

1.5.6 Awarding

Communication of awarding will be officially done by email.

2 SUSTAINABLE DEVELOPMENT

Our Core business lines - financial protection and wealth management – promote sustainable development.
It is important for AXA to ensure that the suppliers with whom it has developed and maintains lasting relationships believe that their own business development, as well as the quality of their service or product, is related to social and environmental responsibility.

2.1 Vendor Compliance with AXA's Commitments

AXA has taken some public and responsible commitments towards its stakeholders: Clients, shareholders, employees, suppliers, community and environment.
Details of those commitments can be found at www.axa.com

The commitments attest to AXA's desire to contribute to the sustainable development of the communities in which the Group does business.

Our commitments to suppliers are:

- ✓ **Maintain quality relationships: By adhering to a clearly defined code of conduct**
  AXA expects its employees to behave in an exemplary manner in their contacts with suppliers and non-exclusive distributors. Our goal is that Employees who are in charge of purchasing in AXA companies must read and sign a special code of conduct that stresses commitment to the following obligations:
  - **Disclosure/Confidentiality:** Vendor offers are strictly confidential, as is the content of any contracts entered into.
  - **Fairness/Competitive bidding:** All participants to a request for proposal issued by AXA are treated in accordance with the highest standards of honesty and fairness.
  - **Objectivity/Neutrality:** AXA employees are prohibited from accepting gifts and entertainment or substantial value from existing or potential vendors which would cast doubts on their ability to make independent judgements.
  - **Transparency/Traceability:** All relevant factors with respect to a purchasing decision must be recorded and kept on file at least until the end of the amortisation period for the property in question.
  - **By respecting the terms of payment**
  - **By promoting ongoing dialogue** with AXA's key suppliers and non-exclusive distributors to foster strong relationships are constantly strengthened.

- ✓ **Encourage our suppliers to be socially and environmentally responsible**
  AXA is working to maintain strong and sustained relationships with its suppliers and non-exclusive distributors. For this reason, it is important that they share our conviction that their long-term survival and the quality of services depend on adopting socially and environmentally responsible behaviour. AXA adds a clause to supplier agreements that requires our suppliers to comply with social and environmental regulations in force.

2.2 Vendor Compliance with United Nations Declarations and other Social Welfare Rights and Regulations

AXA is a signatory to the United Nations resolutions on human rights, labor and the environment that is commonly known as “The Compact Policy”. The purpose of “The Compact Policy” is to create an international platform that facilitates mutual understanding and joint efforts among business, labor, civil society organizations, government, UN agencies and leading commentators from the academic and public policy communities in order to address contemporary globalization challenges. Details of this program can be found at http://www.unglobalcompact.org.
The Global Compact's nine principles in the areas of human rights, labor and the environment enjoy universal consensus.
The nine principles are:

Human Rights

- Businesses should support and respect the protection of internationally proclaimed human rights within their sphere of influence; and
- make sure that they are not complicit in human rights abuses.

Labor Standards

- Businesses should uphold the freedom of association and the effective recognition of the right to collective bargaining;
- the elimination of all forms of forced and compulsory labor;
- the effective abolition of child labor; and
- eliminate discrimination in respect of employment and occupation.

Environment

- Businesses should support a precautionary approach to environmental challenges;
- undertake initiatives to promote greater environmental responsibility; and
- encourage the development and diffusion of environmentally friendly technologies

3 BUSINESS REQUIREMENTS

3.1 INSTRUCTIONS TO QUOTE

Expectations

The supplier selected for this project will be expected to provide competitive pricing, a transparent action plan with clear deliverables and expected workload (man-days), a strong account management team and support, the highest quality service, and be very reactive and flexible.

Pricing

Note: Any pricing, rates, fees, discounts and/or rebates in your response must be valid throughout the entire bid process and resulting contract. Price will not be the only factor considered in awarding this contract, but it will be one of the most critical components. Submitted prices, rates and fees should be inclusive of all possible charges to AXA throughout the contract period.

If any component is dependent on volumes, tiers or other metrics, please be specific. If you wish to suggest alternative solutions, please describe their cost in as much detail as possible.

Currency

Currency is Euro.

Professional Fees:

The amount of workload request by project should be detail by profile “man days”.

AXA reserves his right to choose different providers in each country or one provider for all countries.

AXA expects to contract with the provider on a fixed fee basis.

AXA expects to receive a proposal that includes travel & accommodation expenses and any other related expense. Should travel costs not possible to asses, the proposal should specify it clearly, explaining the reason of not being able to evaluate these costs.

Prices must exclude VAT and other taxes.

The pricing must be valid during 90 days following its reception by AXA.

The name and information on the AXA entity to invoice will be provided at the beginning of the assignment.

The payment schedule is the following:

- 50 % at the beginning of the assignment
- 50 % at the end of the assignment

In case of not meeting the deadlines described in this RFP due to reasons attributable to the provider, AXA reserves its right to keep up to the totality of the last payment schedule in concept of indemnity for damages.

4 TERMS AND CONDITIONS

4.1 Cost of proposal

The supplier will bear all costs of the proposal process including, without limitation:

- Reviewing the RFP
- Preparation of a proposal
- Any subsequent negotiations with AXA

Regardless of whether a contract is subsequently entered into between the parties. No claim may be made by a supplier against AXA concerning the RFP or any other aspect of the proposal process.

4.2 Selection of Supplier(s) and Award of Contract

AXA reserves the right to reject any or all bids, waive irregularities or defects in any bid, accept other than the lowest bid, reject any bid which does not respond directly to the requirements of this RFP, and make any and all awards.

AXA's selection of a supplier will be based not only on cost, but also on an evaluation of the Supplier's organisation, experience, financial responsibility, availability of manpower, ability to perform the work professionally and in full compliance with the requirements and standards of AXA.
AXA will negotiate the most favourable agreement possible.

The proposals received in response to this RFP shall be incorporated into the final agreement.

Additionally, AXA reserves the right to cease negotiations with any or all suppliers, re-issue the RFP or any other related document, amend the RFP or any other related document, or withdraw the RFP or any other related document at any time with no liability to any supplier.

4.3 AXA not bound to accept the lowest price

AXA is not bound to accept the lowest priced proposal, and will not reimburse the costs of any supplier in the event that no proposal is accepted. Any contract awarded is entirely at AXA's discretion and AXA may negotiate with any one or more of the suppliers. A proposal is not accepted until a supplier receives written notice by email of a representative of AXA Mediterranean Region for this RFP.

Additionally, AXA reserves the right to award the RFP in portions to more than one supplier.

4.4 Standards of business conduct

On performing work towards the production of a proposal in response to this RFP, the suppliers will be deemed to have accepted the Terms and conditions of this RFP, including, but not limited to the following:

(a) The supplier shall perform its activities with AXA in compliance with all applicable laws, regulations, permits or licenses.

(b) In submitting a proposal, or negotiation a contract with AXA, the supplier will not directly or indirectly:

i. Provide any money, gift or compensation to AXA or to any employee, agent, representative or other party that is in a business relationship with AXA, for the

purpose of obtaining or rendering favourable treatment in connection with its Proposal or Contract.

ii. Make any payment or transfer anything of value to any governmental official or political party or candidate for public office, if such payment or transfer is an unlawful or improper means of obtaining business.

iii. Participate in any transaction which results in the expenditure of supplier funds for any unlawful or unethical purpose including inducements, whether monetary or otherwise, to advance the supplier's interests.

iv. Offer or make any payment, gift, loan, or offer of employment, to any employee of AXA or to a member of the immediate family of such employee.

v. Engage in the transfer of proceeds from illegal activities or structuring a transaction to hide the source of funds or avoid filing all legally required reports with respect to funds, as is commonly known as "money laundering".

vi. Fail to supervise or take reasonable steps to prevent and detect employees of the supplier from acting in a manner as will result in misappropriation, embezzlement, theft, destruction or vandalism to, or unauthorised use of, the funds, assets or property of AXA.

vii. Purchase or sell any security of, or financial instrument issued by, AXA on the basis of or making use of any material, non-public information about AXA or any client of AXA, which is obtained in the course of the supplier's dealings with AXA.

viii. Make, or have made any false or misleading entry or unrecorded accounting of funds in any books and records maintained in connection with AXA or the supplier's business dealings with AXA.

ix. Any conflicts of interest must be notified in the proposal and as they arise.

x. There must be no collusive behaviour by a supplier with another supplier or with AXA.

(c) The supplier shall institute and maintain all appropriate procedures as will implement and effectively carry out the provisions of the foregoing policies and procedures including application thereof to all subcontractors of, and consultants to, the supplier with respect to the supplier's transactions with AXA.

(d) In the event the supplier becomes aware of any violation of the standards of business conduct required hereunder or has reason to believe that a violation may have occurred, the supplier shall promptly notify AXA and shall fully cooperate in any investigation or inquiry conducted by AXA.

4.5 Disclaimer

Suppliers must satisfy themselves as to:

- All information contained in the RFP or related documents
- The work to be carried out under any contract
- The assessment of the risk and cost of carrying out such work.

The supplier is solely responsible for any further investigation concerning additional data or the relevance of any data. AXA will not accept liability for the accuracy, completeness or otherwise of any data or information in the RFP or related documents, nor any interpretations or opinions contained in the RFP or related documents. All information is indicative for the proposal process only.

The supplier enters into the proposal process on the basis that it waives all rights to make a claim in respect of any inaccuracies contained in the data or information set out in the RFP or related documents.

4.6 Anticipated Term

Initial agreement with the successful Supplier(s) shall be for the length of the project.

The proposal should state a clear guarantee of rates throughout the term of the initial contract.

Either party may terminate the contract agreement, at any time, upon 30 days prior written notice to the other party.

4.7 INDUSTRIAL AND INTELLECTUAL PROPERTY OF THE SERVICES

During the execution of an AXA order, all the information, whatever its nature (files, computer medium,..) , provided during the performance of the service by AXA to the supplier will be considered by the supplier as confidential and as the AXA property.

The term Confidential Information refers to any information or data, in particular technical, financial or commercial, communicated in writing or orally, to the supplier.

All the information being the result of an AXA order, whatever its nature (creation, invention, design, graphic, text, document, report) or any industrial or intellectual property right will be transferred in order to become the AXA ownership.

By convention, the supplier who provides a service including a creative activity (design, photos, engraving, …….) will accept to give up to AXA the author rights and moreover the reproduction and modification rights for a worldwide use limited to 50 years as soon as the payment is completed by AXA.

AXA has exclusive rights to the above described creations.

As a consequence the supplier would not have the right to re-use, for another customer or for himself, an artistic creation achieved by its departments for AXA without prior written approval.

All Confidential Information will be kept in the strictest confidence by the supplier, who will provide the same level of protection to prevent its disclosure, copy or use that it takes to protect its own confidential information.