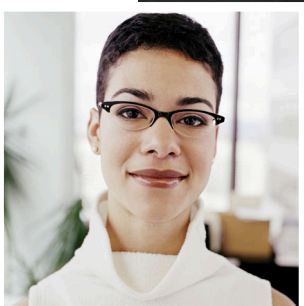


Preparing the Enterprise Security Assessment RFP



CONTENTS

Introduction	3
RFP Format	3
Project Scope	4
RFP TEMPLATE	4
Provider Profile and Qualifications	5
RFP TEMPLATE	5
Pre-assessment	6
RFP TEMPLATE	6
Project Plan	7
RFP TEMPLATE	7
Data Collection	7
RFP TEMPLATE	7
Observations and Recommendations	8
RFP TEMPLATE	8
Security Assessment Report	9
RFP TEMPLATE	9
Terms and Conditions	10
RFP TEMPLATE	10

Introduction

Securing enterprise data, applications, and information systems is an essential but complex business mandate. Attacks by malicious hackers, criminals, and even trusted employees are rising in sophistication and frequency. Risks include revenue loss, privacy lawsuits by customers, and fines for non-compliance with regulations such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance and Portability Act (HIPAA), and California SB 1386. The Department of Homeland Security and the U.S. Securities and Exchange Commission are even considering a requirement for public disclosure of company security provisions. A third-party Enterprise Security Assessment helps enterprises repel attacks, enforce security, and comply with regulations—provided the assessment provider has the right experience and a credible track record.

To ensure an effective assessment, VeriSign recommends that enterprises carefully articulate requirements in a Request for Proposal (RFP). The RFP requires a prospective assessment provider to delineate each step of the Enterprise Security Assessment process, disclose details of security experience, and provide evidence of credibility. The following suggested format includes RFP templates that may be copied or adapted.

RFP Format

- Standard Introduction Boilerplates
- Project Scope
- Profile and Qualifications
- Pre-assessment
- Project Plan
- Data Collection
- Observations and Recommendations
- Security Assessment Report
- Terms and Conditions
- Standard Closing Boilerplates

Project Scope

Describe your enterprise's network and information technology infrastructure and define expectations for the proposed Enterprise Security Assessment. The Project Scope section should include your enterprise's specific technical objectives. Bulleted objectives in the RFP Template are examples of typical security issues.

RFP TEMPLATE

The Enterprise Security Assessment must be able to analyze our security policy, determine how policy is implemented, evaluate security provisions, and recommend improvements to security measures across our entire network and IT environment. Proposals must address risks to our ____ applications, ____ hosts, ____ production servers housed in ____ data centers, connectivity infrastructure, and networking. The connectivity infrastructure for these resources includes ____ fixed nodes, ____ mobile nodes, ____ routers, and ____ switches at ____ locations in [describe cities, states, countries, continents]. Networking technology includes virtual private networks (VPNs), direct circuits, frame relay, asynchronous transfer mode, wireless radio, satellite, fiber, and dial-up.

The Enterprise Security Assessment should meet the following technical objectives:

- Provide the results of an external port scan, a penetration test, and a vulnerability assessment of the internal reachable servers and devices.
- Assess the overall security of the internal security applications and services, including Web, FTP, DNS, and VPN.
- Identify any sensitive, confidential, or company-proprietary information that is available on our servers.
- Assess security of DMZ hardware, such as VPN devices, routers, switches, firewalls, and load-balancing applications.
- Assess configuration of firewalls, DMZ server operating systems, and components, including an evaluation based on security "best practices."
- Review existing procedures for preventing denial of service attacks and responding to incidents.
- Identify network and data security vulnerabilities in the DMZ design; include an assessment of security and availability for possible future network change.

Provider Profile and Qualifications

Because the Enterprise Security Assessment is a consultant-driven process, the RFP should request explicit security-related qualifications for the Proposer as a company and for individuals on the engagement team. RFP responses should delineate capabilities beyond structured methodologies, and they should illustrate how consultants can apply their industry experience to the specific requirements of your enterprise.

RFP TEMPLATE

Provide the following Profile and Qualifications information:

- Primary contact
- Description of company
- Primary business
- Security-related products and services
- Date and country of incorporation
- Registered office address and company registration number
- Location of headquarters
- Details about ultimate holding company, such as that listed on a publicly traded stock exchange
- Number and location of offices worldwide
- Number of staff worldwide
- Number of security-related staff worldwide
- Number of dedicated Enterprise Security Assessment consultants worldwide
- List of industry awards and recognition
- Proof of financial stability
- Number of security-related customers
- Three reference customers with operations similar to our business area and scale

The proposal must acknowledge that we may, at our discretion and cost, perform a background check on any Proposer employees assigned to this project.

Firm Qualifications: Specify length of time your company has performed Enterprise Security Assessments and describe specific experience in our industry. Illustrate unique attributes or competitive advantages that distinguish your company from other firms. Specifically describe your company's competence relating to Web security, e-commerce, _____, _____, and other aspects of systems security.

Engagement Team Qualifications: Provide level and names of firm personnel who would be involved in an Enterprise Security Assessment. Include key engagement profiles, resumes, certifications, and narratives describing industry experience and other qualifications, and provide the number of Enterprise Security Assessments in which each team member has participated.

Pre-assessment

Pre-assessment is the setup phase of an Enterprise Security Assessment. It includes an analysis of your enterprise's security policy, an assessment of internal configurations, and collection of background information on all processes related to implementing security policy. Responses to the RFP's Pre-assessment section will show where your enterprise would need to make resource commitments for staff and management, including time for interviews with the Chief Executive Officer, Chief Information Officer, Chief Financial Officer, Director or Manager of Security, Director or Manager of IT or Network Operations, Database Administrator, Remote Access Administrator, Disaster Recovery / Business Continuity Manager, Facilities Managers, Contract Managers, Human Resource Managers, Information Systems Security Managers / Officers, Functional Area Managers, System / Network Administrators, IT Developers / Integrators, and sample end users.

RFP TEMPLATE

Describe your Pre-assessment process for the proposed Enterprise Security Assessment solution. Detail required meetings; coordination of interviews; regular reporting and communications activities; budget tracking and processing of change orders, if required; requirements analysis and security policy evaluation; and other steps required to create a project plan, collect data, make observations and recommendations, and produce a final report. Include examples of documentation requirements, questionnaires, and other relevant material.

Pre-assessment should include the following tasks:

- Review the process for creating policies and guidelines; determine whether current policies are up-to-date and effective.
- Identify policies that should be developed to enhance current and future security.
- Assess internal configurations related to security, operations, management, and technology used in the development of the security architecture.
- Ensure that the published security standards are in line with the security policy.
- Ensure that the defined security organization supports the security policy.
- Ensure that asset classification is appropriately defined and controls are aligned with the security policy.
- Determine whether business continuity and management actively support security policy.
- Assess whether security practices comply with the security policy and whether information security is being effectively managed in the enterprise.
- Review existing security reporting mechanisms.

Project Plan

Creating an actual Project Plan will require data from the Pre-assessment process. However, a preliminary Project Plan will reveal how each Proposer will organize and cost-manage the Enterprise Security Assessment. It will also show where your enterprise would need to commit implementation staff and management resources.

RFP TEMPLATE

Provide a preliminary Project Plan with detailed objectives and scope; projected tasks with milestones and schedule for completion; estimated person-hours of work budgeted for each activity; name of individual responsible for each task. The format also may be used for production of an actual Project Plan after Pre-assessment.

Data Collection

The RFP should specify all relevant tests and other types of data collection to be performed by Proposers. For an effective Enterprise Security Assessment, Proposers should conduct a broad and deep evaluation based on International Standards Organization (ISO) specifications and other criteria important to your enterprise.

RFP TEMPLATE

Describe how Proposer will test, collect, and analyze information defined under Project Scope and gathered about business and technical requirements through interviews, documentation review, and network analysis.

The following tests may be included:

- Asset and OS discovery
- Inventory and mapping
- Security vulnerability scans
- Penetration analysis
- Other technical and non-technical techniques

Proposer should test and collect data to address criteria in categories defined by ISO/IEC17799-2000, "Information Technology – Code Practice for Information Security Management," including security policy, organizational security, asset classification, personnel security, physical and environmental security, communications and operations, access control, systems development and maintenance, business continuity, and compliance.

Testing and data collection should include the following tasks:

- Detect unknown access points into our network from the Internet or extranet, or via unauthorized modem connections.
- Discover wireless frequency emanations that are in the scope of our premises, including unauthorized wireless LAN (IEEE 802.11) access points.
- Review the security of our network connection to the Internet.
- Evaluate network management and monitoring tools that we use to identify security issues on our network.
- Security Assessment for critical infrastructure systems and devices, including SMTP, naming services (DNS and NIS+), HTTP, proxy, DHCP, LDAP, routers, and switches.

- Assess logging and backup practices for servers, firewalls, applications, and network infrastructure.
- Assess data confidentiality; identify any sensitive or restricted information that is available on our network to employees and contractors.
- Assess the risk of allowing traffic to enter our network from external sources, such as over VPN tunnels.
- Review our anti-virus measures for protecting devices connected to our networks.
- Review security of connectivity, especially as it relates to sharing confidential or proprietary information with business partners over Internet, extranet, VPN, and other connections.
- Review security of applications, databases, and middleware used by our company.
- Verify that sensitive data transmitted between applications and clients/servers is encrypted.
- Verify that secure coding techniques are used when creating applications.
- Review security of deployed authentication and authorization technology.
- Review security of access controls.
- Assess password security policy.

Observations and Recommendations

This section reveals the format, depth, and utility of the Enterprise Security Assessment. The RFP should require Proposers to provide examples of typical Observations and Recommendations, including strengths, deficiencies, recommendations, and all associated standards, best practices, and regulations.

RFP TEMPLATE

Provide examples of how Proposer will document key Observations and Recommendations related to the Project Scope. Show how Proposer will document strengths and deficiencies, and explain how each strength or deficiency affects our business or technical requirements. Cite industry standards or best practices as a basis for the strength or deficiency. Acceptable standards include RFCs, Common Criteria, and other published guidelines from recognized organizations such as SANS, IETF, and Gartner. Address compliance with [insert appropriate regulations here]. List the key observations in order of priority or significance. The observations can be listed in table or paragraph format.

If the assessment is performed against an industry standard, the observations can be listed by the sections of the standard.

Provide examples of recommendations that would address the sample observations. At a minimum, the recommendations should include a brief description, the deficiency being resolved, and why it is important. It may be helpful to group the assessments into short-term, mid-term, and long-term categories.

The following items may be included:

- Description of the recommendation
- Deficiency being resolved
- Bases for the recommendation (e.g., industry standard or best practice)
- Repercussion or business risk of not implementing the recommendation (financial impact is helpful)
- Design drawings that show how to implement the recommendation
- Recommended hardware, software, or other technology to resolve deficiency
- Level-of-effort or cost to resolve deficiency (could include project plan)

Security Assessment Report

Articulate how the Proposer should organize the Report for the Enterprise Security Assessment.

RFP TEMPLATE

The Proposal should include a sample Report for the Enterprise Security Assessment. Proposer may adapt the following suggested Table of Contents:

Executive Summary

- a) Assessment objectives
- b) Key findings (strengths and deficiencies)
- c) Key recommendations

Assessment Background

- a) Assessment objectives
- b) Customer business and technical requirements
- c) Summary of assessment methodology
- d) Summary of personnel interviewed and data collected
- e) Description of how document is organized

Key Findings

- a) Detailed description of program strengths
- b) Detailed description of program deficiencies

Enhancement Recommendations

- a) Description
- b) Basis
- c) Other details based on Project Scope.

Appendices

- a) Standards used
- b) List of personnel interviewed and associated notes
- c) Data collected
- d) Other relevant information

Terms and Conditions

Adapt your enterprise's standard boilerplates for Terms and Conditions by specifying in the RFP how Proposer should articulate the basis for consulting billing and other project costs. Describe how you will evaluate responses to the RFP. The following Template illustrates how your enterprise might require pricing to be discussed in the proposal. The Template may be modified to fit your enterprise's needs, for example, by providing different values for how elements of the proposal will be weighted for evaluation.

RFP TEMPLATE

Pricing: Provide pricing for your solution. The Pricing Summary shall present the total price or range of prices for performing requirements of the RFP. Each task and deliverable is to be itemized separately and the cost for that item, as well as the anticipated hours for completion, should be included by task or deliverable. Base services and optional services or costs must be identified.

Proposal Evaluation: Key criteria for selecting Enterprise Security Assessment professional services include

- Experience and reliability of the Proposer organization and qualifications of the personnel who would perform requirements of this RFP. Evaluation weight: 25%
- Background and skills of the firm's assigned audit team, including knowledge and experience related to Enterprise Security Assessment processes. Evaluation weight: 25%
- Proposer's written plan, which demonstrates the method or manner in which the Proposer will satisfy requirements of the RFP. Evaluation weight: 25%
- Fee schedule and total cost. Evaluation weight: 25%