INFORMATION SECURITY ASSESSMENT RFP CHEAT SHEET

Tips for issuing and reviewing Request for Proposal (RFP) documents for information security assessments.

Planning the Security Assessment RFP

Consider whether you'll benefit from issuing the RFP or whether a less formal process is better for you.

If you're not familiar with the services you need, consider issuing an RFI, rather than an RFP.

Understand what's driving your need for the security assessment, so you can be specific in the RFP.

Identify the individuals who should participate in the development of the RFP and in the review of responses.

Consider whether your environment is ready to be assessed, or whether it's best to wait.

Understand and confirm your staff's availability during the assessment to support the project.

Identify and avoid conflicts with other projects during the assessment (e.g., rollout of a new application).

In the RFP, describe the benefits of working with your organization to entice more vendors to respond.

Supporting the RFP Process

Consider various teams' perspectives (legal, IT, audit, etc.) to ensure support for the RFP and the assessment.

Decide on a realistic timeline for the RFP process, allocating sufficient time for a responses and review.

Confirm a realistic budget for the assessment, accounting for your requirements and market prices.

Clarify how the RFP responses should be submitted (email, fax, paper mail, etc.) and who will receive them.

Request itemized pricing from the RFP responders, to simplify the comparison of proposed services and costs.

Define the process for receiving timely answers to the questions you may have after reviewing RFP responses.

Defining the Assessment's Details

What business and IT objectives, including compliance requirements, should the assessment support?

What milestones and timeline (dates for starting, ending, performing testing, etc.) do you require?

What reports and other deliverables do you expect to receive? (For reports, outline desired table of contents.)

What type of a security assessment do you need (vulnerability assessment, penetration testing, etc.)?

What is a "must have" and what is a "nice to have" for the desired assessment?

Describe the size of the environment in scope for the assessment (number of systems, applications, etc.).

Consider requiring an NDA if an RFP responder asks for sensitive details for preparing a response.

Distributing the RFP

Decide whether you'll benefit from a large pool of RFP responders or whether you prefer hand-picking the vendors whom you'll invite to respond.

Consider finding potential RFP responders by researching speakers and authors who've demonstrated security assessment expertise.

If you maintain a list of firms interested in your RFPs, contact them; if you don't, consider creating such a list.

To meet promising RFP responder, participate in security events (SANS, Infragard, ISSA, OWASP, etc.).

Request a commitment to respond by a specific date, so you know whether to expect a sufficient number of RFP responses; if necessary, invite additional responders.

Consider sharing the RFP with the vendors with whom you already have a good working relationship.

Define a process for handling the RFP responders' questions fairly and comprehensively.

Selecting the Security Assessment Vendor

Assess the expertise of the individuals the vendor will assign to your security assessment.

Confirm the availability of the vendor's staff in accordance to your timeline and location requirements.

Consider inquiring about the background checks the vendor performed on the staff assigned to the project.

Examine the vendor's project management capabilities.

Define vendor selection criteria and assign weighs to each factor based on its importance to you.

Consider what information about the vendor's companies you require (e.g., revenue, locations, etc.).

Ask clarifying questions from RFP responses before making your selection.

Inquire about the vendors' references for the type of project you're looking to conduct.

Review the vendor's sample assessment reports.

Typical Elements of an RFP Document

- About Your Organization: Outline the nature of your business, workforce size, location details, etc.
- RFP Process: Clarify selection criteria, RFP timeline, submission guidelines, vendor qualifications, etc.
- Assessment Requirements: Discuss assessment objectives, scope, your infrastructure details, etc.
- Assessment Deliverables: Explain the expected deliverables, including reports and discussions.
- Terms and Conditions: Include the text provided by your organization's legal and procurement teams.

Definitions

Request for Proposal (RFP): A structured document used to solicit proposals for services or products

Request for Information (RFI): A document, often less formal than an RFP, used to assess available offerings

Non-Disclosure Agreement (NDA): A contract requiring the parties to protect sensitive data they exchange

Security assessment: A structured test of IT infrastructure, usually used to assess security posture

Additional RFP References

Beyond the Template: Writing an RFP That Works
http://sourcingmag.com/content/c070228a.asp

Sample RFP for Security Risk Assessment … Project
https://iapsc.org/...RiskAssessment.pdf

Truths and Tips on the Flawed RFP Process
http://cio.com/article/193501

Authored by Lenny Zeltser, a seasoned business and technology leader with extensive information security experience. Special thanks for feedback to Hana Park and Jefferey Saiger. File version 1.5. If you liked this reference, take a look at Lenny's other cheat sheets for IT and information security professionals.