Global Information Assurance Certification Paper

Jessica Homze
December 15, 2003
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b (amended August 29, 2002) – Option 1

DEVELOPING AN INFORMATION TECHNOLOGY SECURITY SELF-ASSESSMENT PROGRAM

1.0 ABSTRACT

In 2002, the Computer Security Institute and the U.S. Federal Bureau of Investigation's annual computer crime and security survey reported more than $201 million in quantified financial losses as a result of security breaches.[1] Financial losses, privacy violations and national security concerns resulting from these breaches (e.g. viruses such as SQL Slammer, identity theft and 9/11) have rushed security to the forefront of the information technology (IT) agenda in many organizations. Organizations are increasingly relying on internal and external audits as mechanisms to evaluate their computer security posture. Facing budgetary constraints, many are turning toward self-assessments to efficiently expand the scope and coverage of traditional audits. Not only do self-assessments have the potential to provide a more efficient, expansive audit, but if implemented properly, can serve as a critical element of an enterprise-wide information assurance program.

Self-assessments have been utilized as an evaluation tool in various arenas for a number of years. The most notable example of this would be the United State's tax system. Participants (U.S. citizens) evaluate their compliance with requirements (the Internal Revenue Code) using a standardized methodology (tax returns) and submit the results to the Internal Revenue Service for validation. A similar concept can be applied to computer security. Participants (system owners) evaluate their compliance with requirements (such as federal guidelines, and industry best practices) using a standard methodology (self-assessment tool) and submit the results to a centralized function for validation. Developing an IT security self-assessment program requires a number of complex considerations. The purpose of this document is to address the basic steps of developing a self-assessment program to include the following:

- Determine if a Self-Assessment Program is a Viable Option for Your Organization
- Establish the Objectives of the Program
- Determine Key Roles and Responsibilities

---

1 *Microsoft, Chapter 1.*

- Determine Scope of Self-Assessments
- Develop Self-Assessment Tools
- Develop A Deployment Strategy

2.0 DETERMINE IF A SELF-ASSESSMENT PROGRAM IS A VIABLE OPTION FOR YOUR ORGANIZATION

With the exception of government agencies, which are required to perform self-assessments under the auspices of the Federal Information Security Management Act (FISMA)[2] through National Institute of Standards and Technology (NIST) Special Publication 800-26: Security Self-Assessment Guide for Information Technology Systems[3], a cost-benefit analysis should be performed prior to developing a self-assessment program. Specific points to be taken into consideration include:

- Would it be more cost-efficient to have an external third party perform the assessment?
- Are there resources available to develop and implement the program?
- Are there resources available to maintain the program?
- Is the IT environment conducive to a self-assessment program? If your organization has a complex information system environment, it may be more beneficial to have an external third-party perform the assessment.

In order to make a fully informed decision about implementing a self-assessment program, it would be prudent to develop a prototype self-assessment program and pilot it to a selection of participants. A pilot will provide an opportunity to test the program on a limited basis to determine the feasibility of implementing a full, organization-wide program. The pilot will also to serve to establish guidelines (e.g. how long a self-assessment should take) and allow end users the opportunity to provide feedback on the program prior to implementation. End-user cooperation and participation is critical to the program's success. Involving users in the beginning development stages will help to ensure their buy-in. If management determines that the pilot results are satisfactory and decide to move forward with the full self-assessment program implementation, lessons learned from the pilot should be incorporated into the next version of the program.

3.0 DEVELOPING A SELF-ASSESSMENT PROGRAM

Developing a successful self-assessment program requires extensive planning and forethought prior to implementation. Management participation in throughout the lifecycle of a self-assessment program is critical to its success.

---

2 http://www.fedcirc.gov/library/legislation/FISMA.html

3 http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

Key activities in developing a self-assessment program include the following: 1) determine if a self-assessment program is a viable option for your organization, 2) establish the objectives of the program, 3) determine key roles and responsibilities, 4) determine scope of self-assessments, 5) develop self-assessment tools and 6) develop a deployment strategy.

3.1 ESTABLISH THE OBJECTIVES OF THE PROGRAM

After it has been determined that a self-assessment program will be implemented at the organization, objectives should be determined. The following list provides some examples of self-assessment objectives:

- Critical systems will undergo a security evaluation every three years.
- Determine compliance with government standards (e.g. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[4] for healthcare providers).
- Provide assurance to customers that their sensitive information is protected while being stored.
- Identify and document security vulnerabilities so that mitigation strategies can be developed.

These are just a few examples of potential objectives for a self-assessment program. Senior management across the organization should be heavily involved in determining the objectives of the program. IT security impacts all facets of an organization, not just those directly responsible for its management.

Objectives should be specific and measurable. Setting measurable objectives will allow your organization to more effectively evaluate its security posture over time. For organizations that routinely undergo audits from third parties, implementing a metrics program to gauge progress over time can be an invaluable testament to the progress you are making in improving your IT security environment. Metrics may also help in attaining additional IT security funding by providing evidence of return on investment. Federal guidance has been provided by NIST for using metrics to measure the state of IT security environments. Refer to NIST Special Publication 800-55: Security Metrics Guide for Information Technology Systems[5]. The publication states the following as a benefit of implementing a metrics program, "The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports."[6]

---

4 *http://www.hhs.gov/ocr/hipaa/*

5 *http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf*

6 *NIST, pg.1.*

3.2 DETERMINE KEY ROLES AND RESPONSIBILITIES

In the beginning stages of developing a self-assessment program, roles and responsibilities should be determined. In most organizations, the Chief Information Officer (CIO) or Chief Security Officer (CSO) will be the individual responsible for the program as a whole. The IT security department or division will most likely be responsible for developing and implementing the program. This group typically includes project managers, security administrators, security staff, etc. System security administrators will presumably be the individuals responsible for completing the self-assessments themselves.

Typical responsibilities for self-assessment programs include the following:

- Approving program components.
- Developing framework for the program. The framework is comprised of the following types of components: objectives, methodology to be used, roles and responsibilities, reporting strategy and budget.
- Developing assessment tools.
- Developing deployment strategy.
- Program/project management.
- Educating participants on the program and tools prior to implementation.
- Addressing questions/concerns from participants.
- Collecting results and issuing reports.
- Evaluating the success of the program.

3.3 DETERMINE SCOPE OF SELF-ASSESSMENTS

Determining the scope of the self-assessment program may be the most complex set of decisions throughout the entire development process. Many things must be taken into consideration when setting the scope, the most influential of which are: the objectives of the program, applicable computer security requirements/industry best practices, the organization's IT environment and the budget. It is important to establish a scope that will achieve the objectives of the program with available resources.

At minimum, the established scope of the self-assessment program will drive 1) the budget, 2) staffing, 3) requisite evaluation tools and 4) timeframe. Two major steps in determining the scope are to determine applicable security requirements and evaluate your environment.

3.3.1 DETERMINE APPLICABLE SECURITY REQUIREMENTS

Organizations must determine which security requirements/industry best practices that they are required to comply with in order to develop the scope of the self-assessment program. Federal agencies are mandated to comply with a

number of computer security requirements. These include FISMA[7], Office of Management and Budget (OMB) CIRCULAR NO. A-130, Appendix III[8], and certain Federal Information Processing Standards Publications (FIPS)[9]. As previously mentioned, healthcare agencies must comply with HIPPA[10] requirements. Although commercial companies are not as heavily regulated as federal and healthcare agencies, exploitations of security vulnerabilities could cost them millions of dollars in losses, therefore it is in their best interest (and that of their shareholders) to adhere to industry best practices for IT security. The SANS Institute's reading room[11] provides extensive literature on IT security best practices. One example this of this guidance is "Web Application Security – Layers of Protection"[12] written by William Fredholm, which describes resources for creating secure web applications.

IT security requirements/best practices exist at many different levels and in various categories. NIST 800-26 provides mostly high-level security requirements in three categories: management, operational and technical. An example requirement from 800-26 is "2.1.1 Has the system and all network boundaries been subjected to periodic reviews?"[13] This requirement does not specify specific criteria (such as how often "periodic" should be or what exactly is meant by "system and network boundaries"). Conversely, Microsoft provides volumes of documentation on very specific best practice configuration settings to secure their products. One such documents is the "Microsoft Windows 2000 Security Hardening Guide". An example requirement from this document is, "To prevent a possible malicious program from starting when media is inserted, create the following Registry key to disable autorun on all drives.

Key Path: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	Format	Value
Key: Explorer Value Name: NoDriveTypeAutoRun	REG_DWORD	255

"[14]

The organization must determine at which level to develop self-assessment program. Higher-level requirements leave much room for interpretation by the participants and will results in more diversified results. Having a limited range of specific outcomes via a more focused assessment will allow for greater ease in aggregating the across the organization for analysis and reporting purposes. The self-assessment should be designed taking into consideration the objectives of the program and the level of effort for all parties involved (i.e. developers,

---

7 http://www.fedcirc.gov/library/legislation/FISMA.html

8 http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

9 http://www.itl.nist.gov/fipspubs/

10 http://aspe.hhs.gov/admnsimp/pl104191.htm

11 http://www.sans.org/rr/

12 ***Fredholm, Web Application Security – Layers of Protection***

13 *NIST, p.A -7.*

14 Microsoft, *Chapter 5.*

individuals responsible for evaluating the results and the participants). The assessment needs to be carefully designed so that it is easily understood, yet accomplishes the objectives it was created to satisfy and does not require a tremendous level of effort by any of the groups participating in the program.

3.3.2 EVALUATE ENVIRONMENT

If your organization has not done so already, a thorough inventory of your organization's systems should be conducted. This inventory should document, at minimum, major/critical systems and their 1) purpose, 2) location, 3) technical specifications, 4) contact and 5) system owner. Examples of technical specifications include the following:

Applications:

- Hardware description (vendor, name, version, etc.)
- Supporting operating system name and version
- Security software names and versions
- Database names and versions

Networks:

- Routers
  - Hardware description (vendor, name, version, etc.)
  - Operating system and version
- Firewalls
  - Hardware description (vendor, name, version, etc.)
  - Operating system and version

If the organization has undergone a risk assessment or has drafted a Disaster Recovery and/or a Business Continuity plan, then an inventory of critical systems has probably already been conducted.

3.4 DEVELOP SELF-ASSESSMENT TOOLS

Based on the established scope, the means to evaluate compliance with the security requirements (i.e., a tool) must be developed. The tool can be as simple as a word table or as complex as a web-enabled application with an intelligence engine to calculate results and generate reports automatically. Examples of vendors that supply this type of software include:

- SAFEOperations™ - SAFEOperations™ Intelligent Security Enterprise Assessment Tool[15]. This application allows organizations to deploy web-based assessments and generate reports from the results.
- datacure - Security Self-Assessment Tool (SSAT). The tool is described as by the following from the company's website, "SSAT is a Web-based software application that is designed to provide Government Agencies with a standard

[15] http://www.relyonrma.com/products.html

approach to collecting and analyzing critical information related to their Agencies security posture." [16]

Regardless of the type of tool developed, the following elements should be captured for each self-assessment:

- System name and description.
- Contact name and telephone number for individual responsible for the self-assessment for that system.
- Each security requirement being evaluated and the following information for each:
    - The relevant computer security regulation and/or best practice.
    - The method for determining whether the security control is in place or not.
    - The results. The organization's audit documentation requirements and how much information has been deemed necessary to adequately evaluate the self-assessment results will drive how much supporting evidence the participants will have to supply with their results.
- Participants should also have a place to provide suggestions for improvement to the self-assessment program, documentation, additional explanations, etc.

As previously mentioned, documentation requirements will also have to be determined. In other words, how much supporting evidence will participants have to submit with their assessments? Will supporting evidence be provided only for tests and/or requirements that the participants say they are in compliance with? What type of supporting evidence will be required? If a participant maintains that they have a system security plan, should they submit it with the self-assessment? For specific security settings, will screen shots or appropriate system reports need to be submitted ((e.g. specific registry settings in Windows NT or the Global System Options (GSO) report from CA-ACF2))? These considerations should be carefully weighed against 1) what is the necessary amount of supporting evidence to adequately evaluate self-assessment results and 2) the amount of time and resources it will take participants to generate the documentation.

It is important that all information collected by the tool during the self-assessment process be safeguarded with appropriate access controls, as it will contain a large amount of sensitive information.

16 *datacure, pg.1.*

3.5 DEVELOP A DEPLOYMENT STRATEGY

After the primary elements of the self-assessment program have been determined, a deployment strategy should be developed. A deployment strategy will document the elements necessary for implementing the program across. This section documents the elements that should be addressed in a deployment strategy.

3.5.1 PROGRAM MANAGEMENT

A program management function for the overall self-assessment program will need to be established. The project manager will be responsible for determining the timing of self-assessment related activities, the budget, staffing, deploying the program and overall quality control. The project manager should be involved with the program from its inception to ensure a solid knowledge base for its management.

3.5.2 COORDINATION ACROSS THE ORGANIZATION

In order to make the most efficient use of resources, it is important that the lines of communication be established throughout the organization. Effective communication can allow for efficient knowledge transfer, potential cost savings from leveraging previous audit/review findings and functional expertise, a greater level of program acceptance and an overall cohesiveness in program results. Coordination throughout the organization will also help to eliminate duplication of efforts.

An example of effective coordination in a organization would be that the internal audit department recently reviewed a system about to undergo a self-assessment and agreed to allow the system owner to utilize the audit results in completing the self-assessment. This would save the system owner time, money and staff resources.

3.5.3 TRAINING AND AWARENESS

Awareness training should be conducted prior to the deployment of the self-assessment program, especially if there is an automated tool involved. Participants will need to be made aware of the process for completing the self-assessments, documentation requirements, how to submit the results and who they can contact with questions. It would be beneficial to provide the participants with training materials that they can take with them as points of reference. Additionally, training provides a good opportunity to discuss the benefits of the self-assessment program in order to gain support and buy-in from the users.

At the conclusion of training, participants should be given an idea of what to expect as the next steps in the self-assessment process. This should include: when they will be given access to the materials, when the self-assessments should be submitted and what the reporting process is going to be.

3.5.4 TIMING

How valuable would a self-assessment be if it took participants three years and a total of $100 million to complete? The organization should establish realistic timeframes for completing self-assessments. If a pilot was conducted for the program, it should provide a good basis for estimating the amount of time required to complete a self-assessment.

In order to get comprehensive coverage of all critical systems and their components (operating systems, applications, network components, etc.), a rotation schedule will likely need to be developed for completing self-assessments. An example of a rotation schedule is outlined below:

- Year 1: All NT and Unix servers housing critical applications.
- Year 2: Application and database reviews for the most critical applications.
- Year 3: A selection of firewalls and routers connecting the components of critical systems.

The rotation schedule should be developed based on the self-assessment program's objectives, applicable requirements/best practices, resource requirements and ensuring that critical systems receive adequate coverage.

3.5.5 HELP DESK FUNCTION

A help desk function should be established to assist participants with completing the self-assessment. This will help serve a number of purposes, including ensuring that the assessment results are of an acceptable quality, submitted timely and complete. It will also help to identify flaws in the self-assessment process and/or tools. Evidence of flaws would be seen in an increase in the occurrence of calls concerning a particular question or aspect of the self-assessment program.

Individuals staffing the help desk should have an in-depth knowledge of the self-assessment process and be available during the timeframe established for the self-assessments.

3.5.6 DATA COLLECTION

A determination will need to be made as to how participants will be required to submit self-assessment results. Examples of options for submittal include hardcopy reports or electronic files (via email, storage media or an online application). This determination should be based on a number of factors including the level of effort and cost to submit, maintain and secure the information.

3.5.7 REPORTING

A process will need to be developed for evaluating the self-assessment results and drafting reports of findings to return to the participants. At minimum, the following elements should be included in the report:

- Finding: Documents the identified vulnerability.

- Requirement: Documents the applicable computer security requirement or best practice not being met.
- Risk: Describes the risk of not mitigating the vulnerability.
- Recommendation: Provides a suggestion to mitigate the vulnerability.

Additionally, overall program results should be compiled and reported. If a metrics program were being utilized, a baseline would need to be established during the first implementation of the self-assessment program for future comparison.

3.5.8 RETENTION REQUIREMENTS

Retention requirements should be established for the self-assessment results. A number of factors will influence how long an organization decides to maintain the documentation. These potentially include legal requirements, internal policies, the rotation schedule (e.g. would documentation be maintained, for reference purposes, until that particular self-assessment was conducted again?) and the cost of maintaining the information.

3.5.9 LESSONS LEARNED

Throughout the self-assessment process, lessons learned should be documented and, at predetermined intervals, compiled for integration into the program. This will ensure continual improvement of the program.

3.5.9 CHANGE MANAGEMENT

A change management strategy will need to be maintained for updating both the tool and the overall program elements. This strategy should be in compliance with established organizational policies.

4.0 CONCLUSION

A properly developed and implemented self-assessment program has the potential to provide organizations with a valuable assurance tool for evaluating the state of their IT security programs.

Sources:

datacure. "Security Self-Assessment Tool (SSAT): Enterprise Application Software for Federal Agency Security Management and Compliance." URL: http://www.datacure.com/ssat_wp.pdf (28 November 2003).

Fredholm, William. "Web Application Security – Layers of Protection". SANS Infosec Reading Room. 26 January 2003. URL: http://www.sans.org/rr/papers/index.php?id=965 (28 November 2003).

Microsoft. "Microsoft Guide to Security Patch Management." TechNet. 2003. URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/patch/secpatch/Part_I/P1CH1.ap (28 November 2003).

Microsoft. "Microsoft Windows 2000 Security Hardening Guide." TechNet. 11 April 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/win2khg/default.asp (28 November 2003).

National Institute of Standards and Technology (NIST). "NIST Special Publication 800-26: Security Self-Assessment Guide for Information Technology Systems." NIST Special Publications. November 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf (28 November 2003).

National Institute of Standards and Technology. "NIST Special Publication 800-55: Security Metrics Guide for Information Technology Systems." National Institute for Standards and Technology Special Publications. July 2003. URL: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf (28 November 2003).

Office of Management and Budget. OMB Circular A-130, Management of Federal Information Resources Appendix III. November 28, 2000. URL: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html (28 November 2003).

Public Law 107-347 [H.R. 2458], The E-Government Act of 2002, Title III—Information Security (Federal Information Security Management Act (FISMA) of 2002. December 17, 2002. URL: http://www.fedcirc.gov/library/legislation/FISMA.html (28 November 2003).

"Health Insurance Portability And Accountability Act of 1996." 21 August 1996. URL: http://aspe.hhs.gov/admnsimp/pl104191.htm (28 November 2003).

SAFEOperations. "SAFEOperations™ Intelligent Security Enterprise Assessment Tool." 2001. URL: http://www.relyonrma.com/products.html (28 November 2003).

SANS. SANS Infosec Reading Room. URL: http://www.sans.org/rr/ (28 November 2003).