Global Information Assurance Certification Paper

Gregory J. Brill
December 11, 2003
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b (amended August 29, 2002)- Option 1

Security Checklists: A security Service

Abstract
The last decade has seen an explosive growth in the security arena ranging from security services and products to new laws and regulations. In order to fuel this growth, IT capital planning and spending has been increasing each year. "A study conducted by Infonetics Research predicts that security spending will rocket from $4.5bn (£2.7bn) now to $8bn in 2007", as reported in VNUNET.com October 2003 issue of news center[i]. As spending increases, organizations are creating new programs and executive level positions to handle security related activities, including the traditional roles of Chief Information Officers and the new Chief of Mission Assurance.

As security (and now privacy) concerns rocket forward so are the programs used to address old and emerging security issues. One program is the development of a security checklist program. Historically, checklists have been used to fulfill a variety of needs. Today checklists exist for just about everything, some more effective then others. The purpose of this paper is to describe critical elements necessary to develop and manage an effective, risk-based, checklist program that is integrated across the organization and aligned with an enterprise security program. Critical elements include:

- ✓ Development/ Maintenance of Checklist Program
- ✓ Performing Checklist Reviews
- ✓ Enterprise Reporting
- ✓ Integration with other Organizational Programs

Deploying a Security Checklists Program

A versatile checklist program involves many well-coordinated components to achieve the goals of the program. Organizations deploying checklist programs need to determine the key goals prior to development in order to ensure a cost effective balance that also takes into account the organization's risk posture. The department or group of individuals responsible for the checklist program should recognize that they are not the only stakeholders. When designing a checklist program from within an organization, departments or groups such as IT security officers, regulatory compliance officials, and physical security officers should be consulted to ensure "buy-in" to the program and allocate resources to develop usable, effective, and technically accurate checklists. In addition,

consulting and auditing firms often leverage checklists because of their ability to quickly gather information and provide high impact results to their clients. *Note: This paper will focus on the key elements of a checklist program and not the business decisions associated with deploying such a program.*

The following elements of a checklist program are key:

- Development/ Maintenance of Checklist Program
- Performing Checklist Reviews
- Enterprise Reporting
- Integration with other Organizational Programs

Development/ Maintenance of Checklist Program

The key element of a checklist program is of course, the checklist itself. Checklists are designed to address various aspects of an organizations environment and range from addressing IT security controls to performing quality control reviews of purchase orders. The National Institute of Standards and Technology (NIST), which promulgates security standards and guidance to federal agencies, categorizes controls into three areas: management, operational, and technical. NIST's Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* discusses various controls associated within the three categories.[ii] Thus, checklists can be developed that leverage standards and guidance within an organizations industry. Within the federal industry, federal agencies should review NIST standards and guidelines when developing checklists. This section will address the various aspects of checklist associated with IT security and illustrate an example.

Comment: NIST Reference 800-26….

Checklist Format

The two basic types of checklist formats are manual, or paper based, and automated, or electronic based. Careful consideration needs to be made when choosing the format of a checklist. Elements to discern include cost factors (e.g. development, execution, and maintenance), time to deploy, return on investment, and useful life. The following chart provides additional information on the pros and cons of each type of checklist:

Type	Pros	Cons
Manual	• Short development time, allowing for quick deployment • Low cost to maintain • Easily tailored to meet changing or specific customer needs	• Requires human intervention to complete, increasing the likelihood of errors • Completion of reviews are resource intensive • Version control can be more complex • Completion of checklist and analysis, typically, relies heavily

		on the skill and experience of the reviewer
Automated	• Ability to review a large number of systems in a shorter period of time • Ability to leverage fewer resources (i.e. evaluations performed by staff or contractors) • Reports are often generated automatically	• Higher development and maintenance cost • (Consulting) Often agencies will not allow vender created software to be executed on system

A business case analysis should be deployed to address applicable considerations for the organization, as these will vary from organization to organization.

Checklist Coverage

Checklist coverage refers to the specificity of the checklist to address a particular environment, system, or process. Coverage in this paper will be discussed using two terms, "general" and "specific". General checklists state questions or objectives of the system or environment in non-specific terms, but require the reviewer to have a greater skill set to execute the checklist. Thus, general checklists can be used in most environments. On the other hand, specific checklists are tailored to a specific environment, system, or process.

For example, a checklist is deployed to determine whether sensitive system files comply with the following organizational policy: *Sensitive system files shall be protected against unauthorized access or modification.*

- A general checklist does not take into account the various systems deployed by the agency such as Windows NT or IBM's Mainframe security package RACF. Thus, individuals executing a general checklist will need to have the appropriate skills to assess the compliance of the system selected. In this example, a general checklist may not be the most appropriate.
  An example of a general checklist can be found at http://global.bsa.org/usa/policy/security/Govt_security.pdf[iii]. As seen in the example, the objectives are general in nature and can apply to most organization's. In addition, objective six within the example discusses backup and recover controls; however it does not specifically address the software that is used to perform backups and recovery. Therefore, the answers are more yes/no orientated.

- A specific checklist would be tailored to the system or technology being assessed. Let's assume it is an IBM's MVS OS/390 operating system. A specific checklist would clearly identify the targeted files of the system under review to ensure compliance with the policy, such as the high-level qualifier SYS1 (dataset). This checklist type could only be

used for a mainframe environment; however the results will be tailored for the environment and should be more consistent between reviews. An example of a specific checklist can be found at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/win2khg/05sconfg.asp within table 4.1.[iv] In this example, additional detail is provided that addresses the unique mechanisms of how controls are applied within the system.

At first glance it would appear that specific checklists are the better choice. However, this is not the case. In fact, elements of both the coverage of a general and specific checklist play an important role in assessing an IT security environment. Guidelines on determining coverage:

General Checklists

- ✓ Scope of the review addresses physical security and environmental measures.
- ✓ Scope of the review is to determine the completeness of a document type in accordance with a specific standard, such as NIST Special Publication 800-18 *Guide for Developing Security Plans for Information Technology Systems*[v] or the organization's template for developing a backup and recovery plan. NIST's 800-18 provides guidance to federal agencies in developing security plans. In addition, this document discusses management, operational, and technical controls previously discussed.

Specific Checklists

- ✓ Scope of the review addresses a systems security configuration.
- ✓ Scope of the review addresses a specific technology.

Risk-Based Approach

Established checklist boundaries can prevent the checklist from becoming unnecessarily detailed and resource intensive to complete (both from a evaluator and evaluatee perspective). It should be noted that the number of objectives has a direct impact on the resources needed to develop and/or execute the checklist. Thus, an intensive checklist can be perceived as a cumbersome process and will most likely diminish buy-in from stakeholders. For example, a fifty-page checklist covering a large number of critical and non-critical elements of an IT environment may be considered overwhelming. This is similar to making an on-line purchase and then being asked to fill out a one hundred question survey. By the time the customer hits question eleven they will most likely terminate the session. It is industry practice to use a "risk-based" approach when designing and/or selecting the scope of reviews.

A "risk based" approach is the criteria for making decisions and is commonly used in IT Security. The concept is to associate a risk classification to the test objectives within the checklists. Risk Decisions, a Washington state consulting

firm, defines security risk as; “A security risk is the probability of sustaining a loss of a specific magnitude during a specific time period due to a failure of security systems.”[vi] According to this definition, each checklist should focus on IT risks that have high probability, and/or if exploited have a higher probability, of negatively impacting the organization. Risks are often classified in terms of high, medium, or low. A strategy should be decided early in the development process to determine which classification of risks the checklist intends to address.

Note: If a particular checklist or the entire program is attempting to address all categories of risk, then the result may be an expensive development effort and one that may not receive stakeholder buy-in. Alternatively, using a risk-based approach, stakeholders may choose the strategy of only addressing high-risk objectives. Prior to developing a checklist, the organizations risk management group should be consulted, or recent risk assessments reviewed, to obtain an understanding of the risk environment of the organization. Integrating with other organization departments is discussed in the section Integration with other Organization Programs.

To support the explanation for risk-based decision-making, the term “Materiality” has a very similar meaning and is often used in the financial world. The General Accounting Office define materiality within it Financial Audit Manual as, “The magnitude of an item's omission or misstatement in a financial statement that, in the light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the inclusion or correction of the item (FASB Statement of Financial Concepts No. 2).”[vii] As an example, an individual has an $85,000 annual gross income and is reconciling their personal financial accounts (e.g. savings/Checking/Money Market) for a particular month. Upon reconciliation, the individual discovers an un-reconciled difference (assumption the difference is causing a reduction in the accounts).

Scenario 1. The difference is $1. In most cases the individual may spend a few minutes to continue the search. If the error were not found, the individual would make an adjusting entry to force the account to balance. Why? The $1 is not material to the individual.

Scenario 2. The difference is 10% of their annual gross income or $8,500. In this case the individual, most likely, will spend whatever time is needed to determine the difference before making an adjustment. The individual may even call the bank or hire an accountant. Why? The difference is material to the individual and the cost to resolve the difference is commensurate with the potential financial loss.

Checklist Content

Checklist content refers to the level of detail used in the checklist. Though the more detailed the checklist is in terms of content will undoubtedly increase development time and costs; however, the advantages may outweigh the costs. Content should:

- Increase the consistency between reviews (related to deployment of manual checklist)
- Be clear and concise, avoiding confusion or interpretation
- Reflect the risk, or impact of failure to meet the control objective (This addresses the "So What?" question asked by the owner of the system and is important to get management buy-in that an issue exists.)
- Provide general solutions or recommendations of how to resolve an identified issue or vulnerability
- Provide a reference to the organization's policies or procedures or external influences, such as laws and regulations

Maintaining Checklist Program

Organizations developing a checklist program need to ensure it is kept current. Special consideration should be given to checklists devoted to technology areas, as these areas are constantly changing due to new versions, upgrades, or patches that are being applied through out the useful life of the system. Checklists that are out of date may result in inaccurate results or a loss in customer confidence in the checklist program or in the individual executing the review. The following areas need to be addressed to properly maintain the checklist program:

1. Periodically review checklists. For each checklist determine whether changes have occurred requiring an update to the checklist. Example of changes:
    a. Environmental changes (new data center or system that manager access cards)
    b. New laws, regulations, or policies
    c. New versions of hardware or software
    d. A major vulnerability or incident has been detected that the checklist did not address

2. Version control. As updates are applied to checklists, a process should be implemented to manage version control of the checklists deployed. It is critical that only the approved (current) checklist be used in performing reviews. A change management process will allow users and stakeholders to submit changes for review and approval. Changes made outside of the change management process should be discouraged and prevented to the extent possible.

3. Usefulness. A determination should be made of whether a checklist remains useful to the program or organization. Thus, organizations

should only allocate resources to activities that currently provide value. For example, though many of the items on a Year 2000 checklist have value, many others may no longer apply. Thus, elements of obsolete checklists that still apply to the organization should be extracted and integrated into an appropriate checklist, with the obsolete checklist retired from further use or maintenance. Usefulness can also be associated with the content contained in the checklists.

Example Checklist for RACF

The following provides an example of possible sections to include as part of a checklist. The example is based on IBM's mainframe security package RACF.

Test Objective: System and/or user accounts are placed in a revoked or suspended state after a determined number of consecutive, unsuccessful login attempts.

Reference: Organization ABC Password Policy, page 25,"password login"

Test Procedures: From the RACF "SETROPTS" security report options, review the following parameter "After X (x being a numeric value) consecutive unsuccessful attempts, a userid will be revoked" to ensure that it complies with ABC's Password Policy.

Expected Results: The number of consecutive failed login attempts as documented in SETROPTS is configured as X days. (Note: X days should be in accordance with ABC's Password Policy.)

Risk/Impact Statement: Allowing excessive attempts to access user accounts, through password guessing or dictionary attacks, increases the risk of users compromising the system to gain unauthorized access to organization resources. Compromise of these resources may negatively impact a variety of organization areas, including employee and/or customer privacy, trade secrets, financial data, costing models, legal issues, and research and development projects.

Result: Objective Passed, Objective Partially Achieved, Objective Failed

Recommendation: If the conclusion of the test reflects a failed or partially achieved result, then it is recommended that security personnel and system owners: (1) review the password policy, (2) open a security/system change request, (3) within the test environment, change the configuration setting to be in compliance with ABC's password policy, (4) thoroughly test the change, (5) approve the change, (6) implement the change within the production environment, (6) review all systems owned to ensure compliance of systems not in the scope of this review, and (7) report to the Checklist Program manager the

time frame for completing the recommendation and the date the recommendation is implemented.

Performing Checklist Reviews

A three-phased approach can be deployed in performing reviews. References to a three-phased approach are found in standards established by the Association for Certified Public Accountants (AICPA) and the General Accounting Office's Federal Information Systems Control Audit Manual (FISCAM).[viii] The three phases are Planning, Execution and Reporting. Leveraging this three-phased methodology will enable checklist program managers to effectively determine the scope of the review, complete the reviews in a timely manner according to an agreed upon schedule and report the results to applicable stakeholders. The following provides an example of the activities associated with each phase.

Planning

- Determine the scope of the reviews. Examples of scope include reviewing all platform installations of Windows 2003 Server across a department or enterprise-wide, performing follow-up reviews on systems that did not receive a favorable rating in a previous review or a targeted review of one system that recently was upgraded. Scope can be simply put as the boundary of the review. It is critical that once scope is determined, the review stays within the established boundary. The term "scope creep" is often associated with reviews that go outside of the predetermined review strategy. Scope determination might seem straightforward element of planning. However in practice, scope determination can be quite complex. Factors to consider when establishing the scope of the review:
  1. Timing of the review(s)
  2. Cost of the review(s)
  3. Availability of key resources (both that of qualified practitioners performing the review and analysis of results and those under review)
  4. Risk Factors (Not every system may qualify or warrant a review due to its risk to the organization. Therefore, systems that house non-sensitive data or perform non-essential functions may not be deemed of a high enough risk classification to expend resources on the review.)

- Gain understanding of the environment. Eric Cole, Instructor for SANS Security Essential Basics, stated in a July 2003 training program, "Know thy environment!" as a fundamental security principle. Gaining an understanding of the environment where a checklist strategy is going to be deployed is critical and addresses this principle. Understanding the environment to be reviewed will allow planners to identify critical information such as the number, type, version, and

location of the systems, applications, supporting software and hardware that could potentially be included in the scope of the review. Finally, by understanding the environment, planners will be able to ensure that checklist exists for the environment.

- Identify personnel with appropriate skill sets to conduct the review. Security practitioners performing reviews should possess the requisite skill sets. All too often this is not the case, leading to inaccurate collection and interpretation of results, as well as inefficiencies in performing the review. Thus, during planning, resources that possess the appropriate skills need to be identified.

- Coordinate reviews with appropriate parties. Reviews should be coordinated with stakeholders including system owners, security administrators, facilities management, etc. Effective coordination will ensure that security administration personnel are available to assist in the review, and that the timing of the review does not impact critical business operations (e.g. perform the review during non peak hours).

Execution

- Complete checklists. Complete checklists based upon predetermined scope of the review. Ensure each item on checklist is addressed for consistency and obtain sufficient information to support results. It is common practice to discuss results with stakeholders prior to proceeding to the reporting phase of the review. Discussions with stakeholders will ensure results are accurate, act as an education and awareness process, and most importantly obtain buy-in the results.

Reporting

- Generate reports. Provide accurate reports to applicable parties on a timely basis. Reports should be generated shortly after the review in order to be useful. Reports should address the scope of the review, the methodology deployed, contain an executive summary, use graphics/charts as applicable and focus on not only the issues identified but also the strengths of the department. As part of the reporting phase, stakeholders should have an opportunity to respond to the report indicating remediation activities to management.

Enterprise Reporting

The very practice of deploying a checklists program will result in collecting large amounts of information. This information must be managed effectively to be most useful to the organization as a whole. Results should not only be associated with one department or system. To be effective, the results of each review should be consolidated to give an enterprise view of the security

environment of the organization. The advantages of elevating this information to the enterprise level are to:

- Identify trends in weaknesses across the organization. For example: A checklist strategy was deployed at two departments of a ten department organization. The results identified significant non-compliance issues associated with password syntax. An enterprise reporting mechanism will identify this as a possible organizational issue requiring some type of mitigation strategy. This information can then be used to focus future reviews or assist in the organization in deploying other strategies, such training or outreach programs
- Identify the need to develop or enhance policies and procedures
- Identify security training needs of individuals that are responsible for ensuring the organization is not only in compliance with the organizations polices and procedures, but are also an acting security mechanism within the organization
- Identify security and awareness needs of users
- Ensure additional countermeasures are deployed to mitigate the magnitude of risk which the organization is exposed to

Integration with other Organization Programs

A checklist program should not be performed in isolation. In fact, a checklist program should be considered an integral part of the entity's security program and should be integrated appropriately. An integrated checklist program will have various inputs and outputs from and to other organizational programs. Examples of programs that a checklist program will integrate with are: Results from internal and external audits, Incident Response Program, Risk Management Program, and programs associated with the Systems Development Life Cycle. Each of these programs will provide information directly or indirectly impacting the operational effectiveness of a checklist program. A critical element in a checklist program is the effective coordination with other departments or groups. The following lists examples of inputs and outputs:

Inputs to the Checklist Program

- IT Security audit issues identified by the independent auditor
- Risk Assessment report(s) for a system, business process, or organizational department. This report can be used to identify higher risk systems, business processes and departments that may assist in determining where and how often to perform reviews
- Identification of new systems development or major system changes. (Coordination of with the system development activities will ensure that the checklist program remains current.)
- Identification of attempted of actual incidences from the Incident Response Program

Outputs from the Checklist Program

- Checklists used to demonstrate resolution of IT security audit issues identified by the independent auditor
- Results of checklists reviews may indicate the need for or enhancement of education and outreach programs. Results allow this program to focus its education programs.
- Deployment of new checklists to reflect the actual hardware and software used by the organization.
- Development or enhancement of checklist to address trends in the incident response program

Conclusion

Following these guidelines, an organization can create an effective security checklist program that can benefit every aspect of the organization. As a result the organization will be able to keep up with the continuing growth in the security arena, minimizing risk and integrate with the organization's security program.

References

[i] Jaques, Robert. "US security spending to rocket 80 percent." VNUNET.COM October 27, 2003. URL: http://www.vnunet.com/News/1145986 (December 3, 2003).

[ii] National Institute of Standards and Technology. "Special Publication 800-53, Recommended Security Controls for Federal Information Systems", Initial Public Draft. October 2003. URL: http://csrc.nist.gov/publications/drafts/draft-SP800-53.pdf

[iii] Business Software Alliance. "Improving the Cyber Security of Government Agencies". URL: http://global.bsa.org/usa/policy/security/Govt_security.pdf

[iv] Microsoft. Chapter 5. "Security Configuration, Account Policy, Table 4.1". 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/win2khg/05sconfg.asp

[v] National Institute of Standards and Technology. "Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems". December 1998. URL: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF.

[vi] Risk Decisions. "Definition: Security Risk". URL: http://www.risk-decisions.com/Risk-Management-Slides/sld007.htm

[vii] General Accounting Office Financial Audit Manual. "Update to Part II- Tools". April 2003. URL: http://www.gao.gov/special.pubs/01765G/d03466g.pdf

[viii] General Accounting Office. "Federal Information Systems Audit Control Manual". January 1999. URL: http://www.gao.gov/special.pubs/ai12.19.6.pdf

Cole, Eric. Instructor for SANS Security Essential Basics. "The 10 Security Principles." July 2003.