Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Implementing a Successful Security Assessment Process

The goal of a security assessment, (also known as a security audit or security review), is to ensure that necessary security controls are integrated into the design and implementation of a project. A properly completed security assessment should provide documentation outlining any security gaps between a project design and approved corporate security policies. Management can address security gaps in three ways: Management can decide to cancel the project, allocate the necessary resources to correct the security gaps, o...

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia
Stay Secure

Implementing a Successful Security Assessment Process

Bradley Hart

GSEC Version 1.2e

August 21, 2001

Purpose of the Security Assessment

The goal of a security assessment, (also known as a security audit or security review), is to ensure that necessary security controls are integrated into the design and implementation of a project. A properly completed security assessment should provide documentation outlining any security gaps between a project design and approved corporate security policies. Management can address security gaps in three ways: Management can decide to cancel the project, allocate the necessary resources to correct the security gaps, or accept the risk based on an informed risk / reward analysis.

Traditionally, security considerations have been merely an afterthought (at best) in project planning and throughout the project life cycle. A white paper published by Internet Security Systems emphasizes this reality, "from senior management to customers and suppliers, security is perceived at best as a necessary evil. At worst, it is an expensive and unwanted intrusion into normal business operations." A properly implemented security assessment process can break down this perception.

A successfully implemented security assessment process in the enterprise can provide the necessary emphasis on security policy during the most important phases of a project – the planning and design phases. Furthermore, an increasing number of projects (especially those for companies engaged in e-commerce activities) require some aspect of security (authentication, authorization, etc.) as the key project enabler. As such, security requirements must be emphasized throughout the life of the project – from requirements and design, through implementation.

The purpose of a security assessment is not to determine whether a project should be implemented or not, but to provide the appropriate analysis against approved policy. This is an important notion from a customer service perspective. A project team should never be tempted to hide security issues or mislead the security manager out of fear that Security will cancel the project. Many projects may go forward with unresolved security issues because the potential reward absolutely justifies the increased risk. The security assessment simply identifies these risks and frames them properly so that senior management has a complete picture for making these risk / reward decisions.

Besides having secure systems and applications, other benefits will result from a strong security assessment policy. Project managers and management will realize that designing appropriate security controls into a project at the beginning can prevent huge expenses from fixing a security hole after implementation. Also, the assessment process can enhance other security awareness and training activities by providing a hands-on review of policies and procedures for business line project managers.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Security Policy and Risk Posture
The baseline or reference point for any security assessment should be corporate security policies. In order for security assessments to be consistent and credible, the assessment must be based on security policy that is approved and published. Security policy must be deployed so that it's known and accepted by employees, project managers, and management throughout the corporation. Information Security Policy World states that "the fundamental question is how to deploy the policies - how to deliver them. This is critical, as undelivered or badly delivered policies might as well not exist".

A security assessment policy should be part of the policy "suite". An established policy requiring a security assessment for certain types of projects is imperative. Without it, a security assessment will rarely be included in any corporate or business unit project planning activity.

Corporate security policy should represent the general risk posture of the enterprise. Every business is in the business of taking risk – that is, businesses make money by taking risk. The best way to completely eliminate security risk is to simply close up shop – not very practical for making a profit. Hence, security policies dictate the level of risk that an organization would consider normal business activity. No two organizations have the same policies because no two take the same risks. Every enterprise must determine what risks are considered standard business activities, and what risks should be avoided or reviewed as policy exceptions that could be approved under special circumstances.

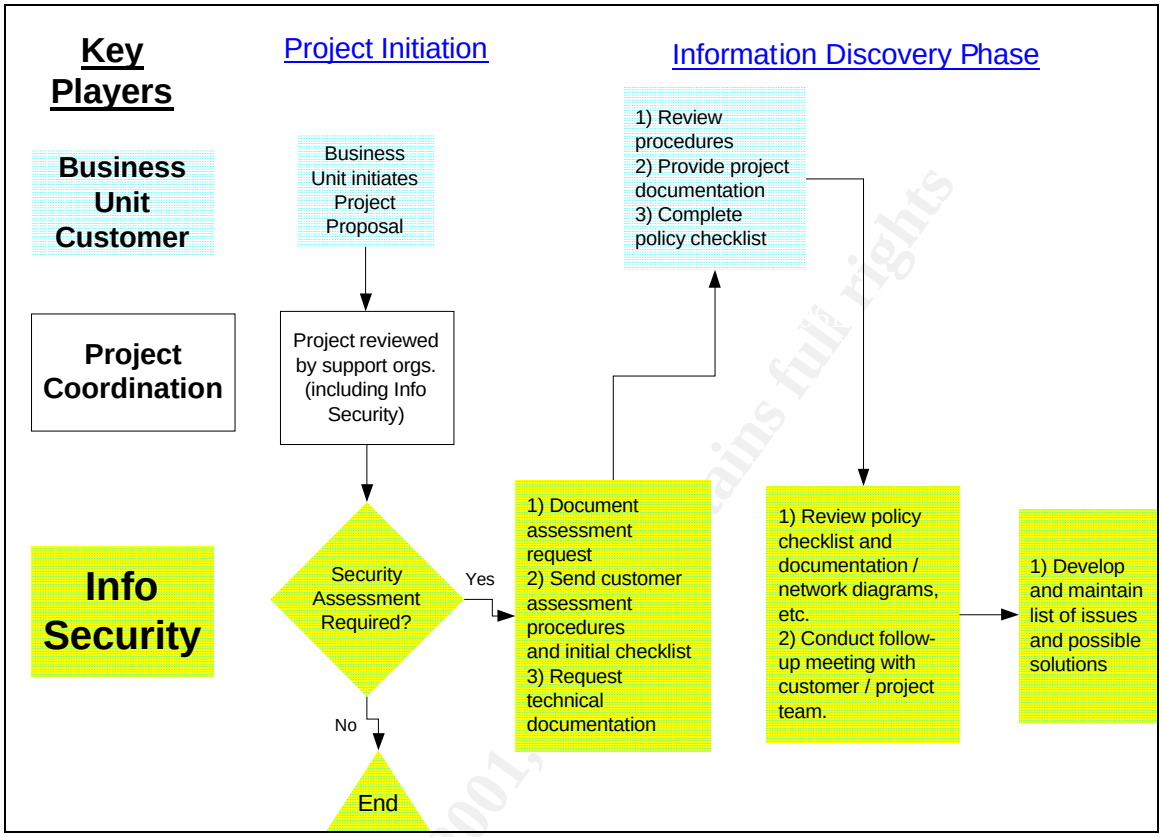
Conducting a Security Assessment
Many methodologies exist for conducting a successful security assessment. Every organization will require a slightly different approach. However, assessments are generally conducted using the same basic steps. The following assessment flow is one example of how this process can be implemented. The diagram below outlines the first two phases of a security assessment process – project initiation and information discovery.

Project Initiation
In this example a business unit proposes a project. A central project coordination team distributes the project proposal to any corporate supporting groups (IT groups – including Security, Finance, Marketing, etc.) that may need to support or may be impacted by the new project. The security assessment policy should require that any new project proposal be reviewed by Security. If Security determines that no assessment is necessary, then the process ends. Otherwise, the information discovery phase should begin as soon as the project is approved and initiated.

Information Discovery
Gathering information about a project and assessing appropriate security controls can be accomplished many different ways. One effective way for gathering high-level security information is through a security checklist. A security checklist must be based on corporate security policies and procedures. According to C & A Systems Security Ltd., "a computer audit must embrace a variety of requirements. Consideration of risk is of

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

growing importance, but fundamental to the whole security audit programme is compliance with the audit checklist and of course the organization's information security policies".



The information garnered from the checklist can be used as a "first cut" for identifying possible security issues in the project. In the above process flow, the checklist is completed by a member of the project team and returned to the security manager. The checklist usually identifies initial security issues and can serve as a guide for follow-up meetings between the project team and the security manager.

Security Assessment Categories

Any checklist questions (and subsequent follow-up discussions with the project team) should always be based on approved policy. This helps prevent senseless arguments on what is considered "good or adequate security". The following general topics and sample questions are probably relevant for most assessments. However, many more detailed questions and conversations will likely surface from each one:

- **Network Security** – If a new device is being added to the network, are the appropriate controls and protections in place (Firewalls, Intrusion Detection Systems, etc.)? Who owns and manages access to the network device? Are procedures in place for monitoring and maintaining the network device? Are production and development environments appropriately separated?

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- **System Security** – Who owns and has access to the system? How can the system be accessed (network, modem, wireless, etc.)? How are IDs and passwords managed and controlled? Are root and admin passwords changed and managed appropriately? Are system logging and audit functions active? What are the procedures for monitoring system logs? Does the OS configuration conform to corporate policy and requirements? What are the procedures for applying security patches, virus updates, etc?

- **Application Security** – Who owns and is responsible for the application? What application security mechanisms (access controls) are in place? What data does the application use? What information does the application create? Is this information appropriately classified and protected? How is the application integrated into other security components (such as using NT authorization, external access controls, and centralized logging/monitoring)?

- **Data Security and Classification** – What data is being incorporated into the project? What is the sensitivity (classification) of the data? Are data protection mechanisms set commensurate with the sensitivity of the data? Who will have access to the data? What access controls are in place? According to policy, what are the encryption requirements for the data (in storage, in transit, etc.)?

- **Business Resumption** – What are the procedures for system and file back-ups? What are the procedures for managing system outages and system recovery?

Assessing External Parties

Increasingly, corporate projects involve external parties either through some sort of network connection, access to data in a DMZ, or simply sending data over the Internet for external processing. Security assessments for these types of projects can be much more challenging because applying corporate security policy to external parties is difficult. The following considerations can be helpful when conducting an external assessment:

- Does the external party have their own approved security policies? Are the employees aware of and required to operate under these policies?
- What external individuals will have access to your company data? How is the access controlled and managed?
- Do you have the proper nondisclosure agreements and legal contracts in place with the external party? Do these agreements specify how your data can be handled, prohibiting any third-party disclosure without your consent? Do the agreements specifically define how your data may be used, stored, processed, etc?
- Are all network connections to third parties secured according to your policies?

Closing the Discovery Phase

Depending on the assessment scope, other topics such as physical security and business risk may be addressed in the information discovery phase. The information gathered during this phase of the assessment must be evaluated against corporate policy

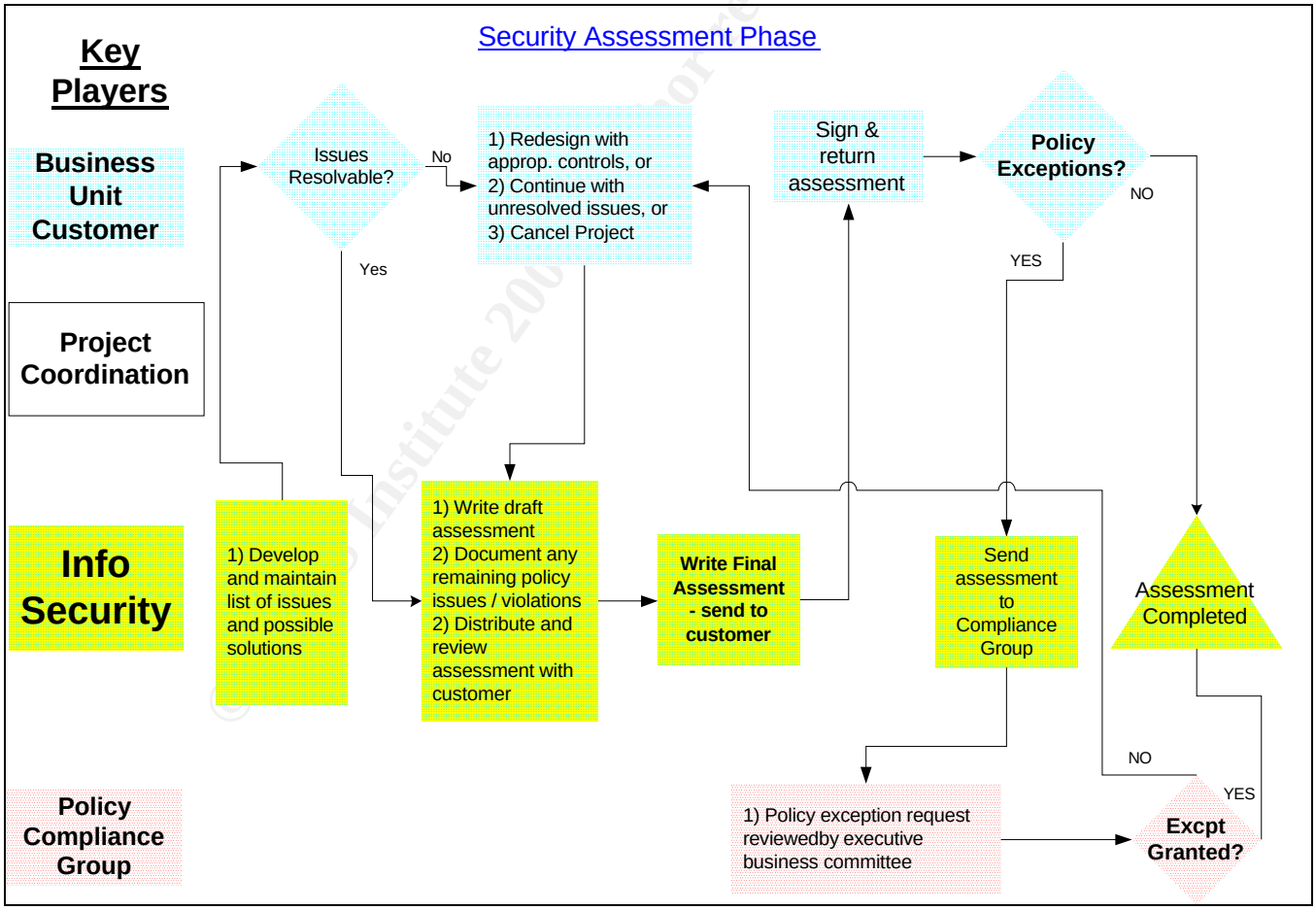
© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

requirements. Any gaps or issues with the project design should be tracked. Creating and maintaining this tracking list is the final step in the information discovery phase.

Security Assessment Phase

The process flow for the assessment phase (see diagram below) begins with a detailed evaluation of the identified security gaps, or issues. The security manager should work closely with the project team to define and understand these gaps. To be successful, the security manager must develop an open and trusted relationship with key members of the project team. In a recent Information Security magazine article, Ira Winkler emphasizes the importance of this relationship:

> "In an assessment, the assessor should have the full cooperation of the organization being assessed. The organization grants access to its facilities, provides network access, outlines detailed information about the network, etc. All parties acknowledge that the goal is to study security and identify improvements to secure the systems. An assessment is potentially the most useful of all security tests, but it is also the hardest to define."



Though the security manager can provide advice on security solutions, the project team is the one responsible for identifying specific tools for mitigating security risk, and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

integrating these tools into the project design. After the gaps are defined and solutions identified, a draft assessment can be written. The draft assessment will describe the overall project design, the security controls that are currently implemented, and any outstanding security issues that remain. Based on resource requirements, the project manager may address some security issues, but not others.

After reviewing the draft assessment with the project manager, a final assessment can be written and distributed. Policy should require that the project sponsor sign the assessment. This sign-off provides an essential audit trail showing that the project sponsor received and understood the assessment, and acknowledged the existence of any outstanding security risks.

Policy Exceptions

If no policy violations are identified in the assessment, then the process is essentially complete. If the assessment contains identified policy violations (previously not addressed), then a special approval, or policy exception must be obtained to proceed. Most organizations have a group of senior managers that set policy, including security policy. This committee makes decisions on strategy, projects, business risk issues, etc. In the above process flow, this group is identified as the Policy Compliance Group. Such a group would evaluate whether the project should proceed given the gaps identified in the security assessment. If a policy exception is granted, the project will proceed. If not, the project is either cancelled or redesigned with the appropriate security controls.

Educating project managers and business line managers of this exception process is very important. They should understand that identifying security gaps during the assessment process does not mean that their project is doomed. Furthermore, security does not cancel projects single-handedly. The decision to cancel or redesign a project should lie with a committee of senior business managers who understand the security issues and the risks. Certainly, a senior security manager should be a key player on this committee. Remember, security's job is simply to interpret and apply policy. The Secure Network Group adds, "You should develop and maintain a strict set of security policies. Attackers look for weaknesses in procedures as well as systems, so the policies must be applied firmly and consistently".

Policy exceptions should be temporary so that the risks are not forgotten. When an exception is approved, an expiration date should be attached. The project team should work to resolve any policy exceptions even after the project is implemented. If resource requirements prohibit a permanent solution, the exception may be re-visited and re-approved after the exception has expired. This process provides continued visibility for projects that contain increased security risk.

A Final Word on Security Assessments

The assessment process should facilitate and enable business objectives, not hinder or prevent innovation. Designing security into a project can enable business strategies that would otherwise be too risky or technically infeasible. Security should strive to be a partner with the project team in identifying security solutions to make the project

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

successful. Finally, integrate the assessment process into your security policies and into existing corporate project planning and project management processes. In this way, security will always be at the forefront of project planning, management and implementation.

© SANS Institute 2001, Author retains full rights

References

Internet Security Systems. "Creating, Implementing and Managing the Information Security Lifecycle", Page 3.
URL: http://documents.iss.net/whitepapers/securityCycle.pdf (August 21, 2001).

Information Security Policy World.
URL: http://www.information-security-policies-and-standards.com/ (August 21, 2001).

C & A Systems Security Ltd.
URL: http://www.securitypolicy.co.uk/securityaudit/index.htm (August 21, 2001).

Secure Network Group.
URL: http://www.securenetworkgroup.com/resources/article-01.html (August 21, 2001).

Winkler, Ira "Audits, Assessments, & Tests (Oh, My)", Information Security. July 2000.
URL: http://www.infosecuritymag.com/articles/july00/features4.shtml (August 21, 2001).

© SANS Institute 2001, Author retains full rights

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced