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 Project Security Review Process within the Project Management Methodology

This paper will not discuss the pros and cons of having security policies. The presumption is that your organization is mature enough to have written and deployed security policies already. Instead, the focus will be on how to get greater penetration of these policies within the enterprise, by adding a security review process within the existing project management methodology. By working with the project office, a process can be created that includes the project approval process, assigning a security resource to projec...

Copyright SANS Institute
Author Retains Full Rights

AD

Implementing a Project Security Review Process within the Project Management Methodology

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b

Darlene Hart Rodgers

November 21, 2002

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

Abstract.....1
Why Implement Security Processes within the Project Methodology?.....2
Implementing a Project Security Review Process.....4
A Project Management Methodology.....4
Identify Areas to Insert Security into the Project Lifecycle.....5
Project Audits.....6
Project Prioritization.....6
Assign a Security Project Resource.....7
Identify Security Requirements to be Added.....7
Identify Deliverables for Each Project Phase.....7
Level of Effort Estimates.....7
Standard Deliverables.....8
Issue Resolution.....12
Audit Reviews.....12
The Security Resource.....13
Completing the Project Security Review Process.....14
The Project Office.....14
Senior Management.....15
Internal Audit.....15
Creating Awareness for the Project Security Review Process.....17
Enterprise Architecture.....17
Security Awareness.....17
Tools That May Help.....18
Risk Matrices and Lessons Learned.....19
Some Final Advice.....20
End Notes.....21
List of References.....22

© SANS Institute 2003, Author retains full rights

Darlene Hart Rodgers
GSEC 1.4b

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

It is imperative for companies to have security policies and standards defined. But, how can the company be sure the policies and standards are read, understood and followed? How can a company increase awareness about security for applications, systems and the network? What is the best way to get involved in initiatives within the enterprise so Information Security is involved early and knows that what is being implemented is low risk for the company?

Many security companies employ project managers to deliver security. A quick search with Google on "security project management" returns many entries. What seems to be missed is that security processes do not have to be separated from the project management methodology. Including security requirements, processes and policy within the project methodology creates responsibility and ownership for secure deliverables to be shared with the project manager. The project manager, in turn, will help influence the project team to consistently deliver more secure applications.

This paper will not discuss the pros and cons of having security policies. The presumption is that your organization is mature enough to have written and deployed security policies already. Instead, the focus will be on how to get greater penetration of these policies within the enterprise, by adding a security review process within the existing project management methodology. By working with the project office, a process can be created that includes the project approval process, assigning a security resource to projects, providing input to the project team, requesting standard deliverables to be met and being involved in project audit reviews. With these measures in place, risk for the organization can be lowered.

Darlene Hart Rodgers
GSEC 1.4b

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Why Implement Security Processes within the Project Methodology?

There is more to implementing a security policy than writing a policy paper, or defining standards or even implementing policies on the firewall, web servers, or routers. It also includes working with and educating the people implementing the policies, developing products, and implementing the applications that will run within the enterprise.

"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". (1) Information Security is normally responsible for completing security risk analysis. This analysis is "essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed". (2)

The risk analysis of your enterprise will show many areas of concern. One area that is always high on the list for Information Security is development. In most organizations, development occurs as part of projects – hopefully, business sponsored projects. Risk increases exponentially when these projects occur outside of the knowledge of Information Security. Many times Information Security may not find out about a project until the request for a firewall change is submitted. Even more frustrating, if applications do not need firewall updates, or access administration services, Information Security may never find out about them – until they cause a breach. Not knowing causes enormous risk to the organization's reputation, customers and bottom line.

The projects that Information Security finds out about at the last minute cause a quick and frenzied security review. Risk assessment processes are applied without much thought to consistency. Vulnerabilities are missed because the pressure is on to get the product out the door or on the web. Information Security is not seen as a partner, but as a roadblock to these projects.

For those projects that Information Security happens to be notified of early on, risk assessments can be thought through and applied more steadily. However, even with additional time, without a consistent methodology or process – scheduled risk assessments will still allow vulnerabilities to be missed, or standards to be applied inconsistently.

If there are no rules for which projects must be reviewed, the Information Security team may spend too much time on projects that have low risk and not staffing those projects that have higher risk. Sometimes external projects receive much more attention than internal, but that doesn't mean internal projects always have lower risk. There needs to be a process to ensure higher risk projects – no matter intranet, extranet or Internet – are reviewed.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

If there is no standard set of deliverables from a review, some projects will receive verbal "OKs" while others will have formal sign-off memos. Some projects will have a formal risk assessment. Others will only be memories of the person who reviewed the project documentation but didn't make any notes. Issues will get lost in the shuffle and resolution plans will not receive follow-up. Documentation will look different and be of different levels of quality. All of these inconsistencies increase the risk to the organization instead of lowering it. And, the point of a good security process is to lower risk.

Without formal processes for security resources to follow, there is also no standard about what to do when there are security issues that cannot be fixed right away, or standards that cannot be met. The project's business sponsors and owners may be pushed for sign-off of risk they do not fully understand because the marketing team is pushing to complete the project on time. There may be a formal waiver process, but without sufficient review, it may not be applied consistently all the time.

So how are these problems fixed? It is obvious that Information Security needs to deploy a standard process – a project security review process. But, developing and implementing this process cannot be done only within Information Security. Without the cooperation of business sponsors, developers, and technical managers, any process will fail. So the question becomes, how can Information Security infiltrate the project team successfully? One road into the project is through the project manager.

Project managers are responsible for the project's overall results, and have direct access to the project teams. In most organizations, they have the responsibility associated with the results…[of a project]…but normally have very little authority in the overall organization. (3) Because of the lack of authority to get resources, tools and other required elements to complete their projects, they become masters at influence. Using these skills, project managers can be a great ally for security policies, standards and procedures.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Implementing a Project Security Review Process

Before developing a project security review process, it is important to understand the project management methodology deployed at the organization. There are many different methodologies in existence. Some companies buy methodologies and use them "out of the box" or modify them to meet the enterprise needs. Other companies develop their own methodology. If the review process is to succeed, it has to be inserted in the proper place in the project management methodology. Understanding the project life cycle will enable proper insertion of security policies – and the new process – within it.

Working with the "owners" of the project management methodology is mandatory. In most organizations, the methodology owners is the project office – or project management sponsor. In some organizations, project managers are scattered throughout the business lines, and indirectly report to a body that is either the CIO or a direct report of the CIO.

Not only will the cooperation of the project methodology persons be needed, it will also be important to get buy-in and agreement from them to roll out any process that project managers are required to follow.

A Project Management Methodology

For the purpose of this paper, lets look at a project methodology that is based on a seven-phase project life cycle. This life cycle has a high level of reporting, employs project audits at the end of each phase, and emphasizes strong communication plans and risk analysis.

The first three phases are considered planning phases. The project manager uses much influence during these phases, working with the project sponsors, resource managers and other senior managers to ensure resources are available and working, and that the right resources are assigned.

Concept phase – the project idea is formed, and high-level scope developed. The business case is developed and must be approved. A project charter is created – outlining the benefits, risks, roles and responsibilities, and *before* and *after* states.

Requirements phase – the business analysts are defining what this project must accomplish. The stakeholders, business process engineers, and analysts are all engaged with the project manager and IT to put together a strong requirements document. This is particularly important since the design and rest of the project

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

will be relying on and will refer to the requirements document. Success criteria, expected results and scope are detailed.

Analysis and Design phase – this is the phase where the IT department is most involved. Along with their business or operations co-parts, they help define current functionality and new, required functionality for the system. Technical design specifications are created based on the functionality and Quality Assurance or testing resources are engaged to write test plans.

The final four phases are considered execution phases. The project manager is now responsible for ensuring the project plan is executed, and technical specifications and test plans are followed. Keeping resources and keeping tasks moving requires a great deal of effort and influence.

Build phase – this phase sees the creation of the system or the modifications of the current system. Developers and technical operations experts are actively engaged to create the systems outlined in the technical specifications, and to ensure it meets business requirements and functionality. Unit testing is ongoing, and the test plan is beginning to be executed.

Test phase – this phase sees all components created and moved up into a QA or staging area. The full test plan (integration, system, regression, performance testing) will occur during this time. Defects will be logged and taken care of – possibly by putting them back into the development environment, and moving back up to QA to ensure change control and version control.

Implementation phase – all testing is complete and the final deliverables (product, system or other) is being promoted to the production environment. Code has been reviewed and accepted and signed off to the production readiness team, who will use documentation to ensure this deliverable can be supported on a go forward basis. Change management processes are employed to get approval to go to production.

Post Implementation phase – this is the time after the project has been successfully put into production. The system may be monitored for a period. Defects are logged and are either fixed with a minor release or held over to a major release. Lessons learned are organized by the project manager, and distributed. Project budget information is gathered and the project closes.

Identify Areas to Insert Security into the Project Lifecycle

Once the methodology is understood, work with the project office or project management sponsor (CIO or other) to build a security process that is layered on top of the project management methodology. There are several areas that can be targeted.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Project Audits

In many project management methodologies, project audits are used as an early warning system for potential problems. (4) Audits, or reviews, normally start in the planning phases and continue throughout the execution phases. Within the sample methodology, the reviews are located at the end of each phase – and are made up of experts that are not directly involved in the project but can provide valuable insight and guidance. (4) These audits are excellent places for security reviews to occur and deliverables to be required, since all the major project team members are present – the project manager, the QA resource, and the technical lead (architect or subject matter expert).

Not all project management methodologies will have audits or reviews at the end of each phase. Be aware of when these reviews occur – usually at least one will occur during the planning phases and another somewhere during the execution phases. Make the most of these reviews by attending and participating.

If the organization has an architecture group, there is probably some sort of architecture review as well. It may even be considered one of the project audit reviews. Being part of this review is also recommended since it will have a high level of detailed discussion around the technical solution.

Project Prioritization

Most organizations that are further along in a project maturity model (there are several different models) will likely have an approval or prioritization method for projects. For example, at the beginning of concept phase, business plan approval occurs. The business plan is based on the high level scope and costs that are known at this time. At the end of Analysis phase the business plan must be reviewed and re-approved now that the scope is well defined. Resource and financial needs are confirmed for the rest of the project. This process allows the organization to maintain a strategic view of the organization, and select those projects for execution that fall in line with the strategic plan. It is most important that the project selection process should be constantly applied and has the support of the enterprise. (4)

The security review process should be working against this approval and prioritization process as well. As is true for the rest of the organization, it ensures that if projects are not prioritized and/or approved, Information Security will complete no work. These projects will not need to be staffed, but follow up later to ensure they have not started back up.

Being involved in the prioritization process will allow Information Security to be aware of upcoming projects, and will provide knowledge about the scope of the projects that will possibly will require involvement at a later time. Being involved in the prioritization and approval process also ensures that security policies are being applied to the project from the beginning, which also reduces the need to deal with the risk of insecure solutions later.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Assign a Security Project Resource

There will need to be a point of contact from Information Security for each project that will be reviewed. This ensures the project manager and the project team know exactly whom they need to talk to when questions or issues arise. They also know that this resource is available to provide guidance to the project team, and will assist in identifying applicable policies for the project.

Many organizations employ mentors to help their project managers. These senior project managers help educate the less advanced project managers, and ensure the project is completed more successfully. The security resource should act as a mentor for the project manager in regards to security.

Identify Security Requirements to be Added

Discuss the analysis of the project lifecycle with the project office. Ask for input. Ask what will work, and ask for help to create the best approach. Remember that they are the subject matter experts for the project management methodology, and their support and buy-in are essential to the success of the process.

Once buy-in for the security review process has been established, the next step is to create the elements of the process. The process will use existing policies and standards as the building blocks, and any new deliverables will leverage the areas identified earlier.

For example, if application development security standards, database standards, web and application server standards exist, use them as the basis for any design review in Analysis and Design phase.

Identify Deliverables for Each Project Phase

Level of Effort Estimates

It is important that the security resources are putting forth the right amount of involvement and effort for projects.

A suggestion to measure level of effort and to also get some initial detail about the project is an initial Risk Analysis Checklist. The project manager can complete this checklist at the beginning of concept phase, before Information Security is heavily involved.

The checklist, since it is completed during concept phase (at the very latest Requirements phase), should only have several high-level questions that will identify the main areas of the project, since most details of the solution will not be known at this time. For example:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Does this use only existing databases?
- Does this use only existing network connections?
- Does this involve new method of authentication/authorization?
- Does this use only an established vendor interface?
- Does this involve 3rd party vendor hosting or storing sensitive data?
- Is this an Internet/Extranet project?

By receiving answers to these types of questions it will be identified if an existing or a new database will be used (more effort will be spent reviewing a new database design and implementation than an existing one that may have been reviewed prior). It will be identified if a new network segment will be required (and planning for it can begin early), if a new vendor interface will be developed, or if third party vendors are storing data.

To help scope the level of involvement, add a weight factor to each Yes answer (plus or minus), and calculate a score for the checklist (round numbers such as 10, 20, 30 make it easier to work with). Fit the total into a high, medium, or low score – which is easy for non-security folks to understand on first glance.

Based on past experience, assign a level of effort estimation (in hours) to the score. For example, 0–30 hours = Low, 31–90 hours = Medium, 90+ hours = High. As resources work the projects, ensure time tracking occurs so estimates can be refined.

This initial risk analysis checklist can also be used to identify projects that Information Security will not need to be involved in. For these projects, issue a "minimal involvement notice". This notice should include a phrase stating that if scope of the project changes, another checklist should be submitted for re-review.

One note, whether the project is listed as high, medium or low, the involvement in the planning phases and all standard security deliverables are required for consistency.

Standard Deliverables

During concept phase, a project charter is created. This should be reviewed to understand the scope of the project, including the various resources that will be required, who the stakeholders or sponsors are, the critical success factors, and the expected end results. While reviewing the charter, look for areas that could become security concerns or potential risks as the project continues. Identify these to the project manager, and keep a copy for later referral. (Also ensure the initial risk analysis checklist has been completed.)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

During requirements phase, the project sponsors and project manager will ensure a business requirements document (sometimes also known as a *statement of need* document) is created. As with the project charter, review the document and identify any requirements that could cause security concerns or opens security holes to the organization. Let the project manager know, and save a copy for later referral.

During analysis and design phase, design specifications for the solution are created. These specifications are the basis for the design of the solution and will be relied upon by the developers during the Build phase. The test plan is the basis for what must be tested during the Test phase (e.g. unit, system, verification, integration, performance, regression). These documents will assist with reviewing the application setup and data flow. The security resource should expect to provide input to the specifications and review the full drafts and any updates. One suggestion is to have a security section in the specs, which outlines specific security "requirements" that does not fit in any other areas. Relevant security requirements should also be tested and must be included as part of the test plan – so a review of that document is also a must.

Also part of the analysis and design phase is the creation of network diagrams, both logical and physical. Reviewing these will assist you in understanding the architecture and layout, which will help with reviewing the network setup. The hosts involved should be identifiable; firewalls, routers, proxy servers, web servers, mail servers, ftp servers, database servers, and application servers are to be clearly identified. Using this information will provide information regarding the firewall rules that will be required to support the solution, or if a new network component will have to be inserted (e.g. new proxy server or router).

During build phase it is possible to create a detailed risk matrix based on the information received to date. The diagrams, specifications, and other knowledge about the project obtained will be the sources for the Matrix. The risk matrix should specify what risks exist with this project, compensating controls and mitigations in place, and risk level after application of the controls and mitigating factors.

This deliverable will mainly be used by Information Security and gives a snapshot of the application at the time of implementation. To ensure the snapshot is sound, this matrix may be updated several times before the production implementation – based on defect fixes, or scope changes or other issues that arise during the rest of the project life cycle. Keep the previous versions – they can be used to follow progress or deterioration. Any risks without controls or mitigation will need to be resolved before implementation. If not, a security waiver should be issued (a process that will allow a security risk or a process that does not meet security policies or standards to be accepted until it can be fixed sometime in the future), or sign-off from senior management that the risk is being accepted.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

During the test phase, once QA testing begins, the security resource will stay in touch with the project manager and follow the issue and defect lists, since fixes to these may cause changes in the final product, and its associated risk levels.

Once testing is complete, review test results. Verify that all security testing has occurred, and results are sound. If defects cause re-tests ensure that review fixes and re-test results are reviewed. Ensure the project team updates any diagrams where defects caused changes (e.g. performance testing will identify servers that are not performing to service level agreements (SLAs) which may require additional servers or a server placement changes, which in turn could impact router or firewall rules).

If the project contains an external website or application, a penetration test is recommended. Whether these are completed via internal testing or an external vendor is not of consequence, but please remember that both network and application type penetration tests exist. Given the scope of the website or application (including whether a new network has been set up to support it) – one or both types may need to be completed.

Normally the difference between the two – network penetration tests include testing for perimeter protection strength (e.g. firewall, proxy, router rules), network reconnaissance (e.g. network mapping, open ports, IP address), DOS (denial-of-service) attacks, and current known industry and technology vulnerabilities. Application testing will include application access (internal and external) and authentication methodology, unauthorized systems access capabilities or modifications, data access and protection (e.g. encryption), use of cookies (e.g. type, how used, contained data), memory leaks, thread monitoring, replay attacks, browser interaction (e.g. caching, purging, timeouts) as well as current known industry and technology vulnerabilities.

Also note that while external sites are easy to test, internal sites take a little more co-ordination, especially for external vendors, since access will need to be allowed from outside to get the tester to reach the application – or they'll have to be sitting on the internal network. Neither scenario is a great idea and goes against most organization's security policies.

During implementation phase, monitor the transition to production, and the security resource assigned to the project should be available for questions or to respond to any issues that arise. Issues that require last minute fixes could cause security risks so be careful and stay involved. Though there may not be "formal" deliverables, issue tracking and resolution is still very important.

During the post-implementation phase review the final results of the implementation, any reports stating how the application is performing, and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ensure any outstanding issues related to security has been resolved – or at least mitigated with an action plan.

By the end of the project, the security resource and Information Security on a whole has put a lot of effort into ensuring all deliverables are met and the application is at an acceptable level of risk. Create a customer satisfaction survey, which asks the project manager to rate Information Security's performance during the project. It can be used as a scorecard for individual resources to show high and low performance areas for them, and for the process. The general survey results can also be used to show senior management how the department is doing, which will build positive support for the process.

All these deliverables should require sign-off to indicate that they are complete before moving to the next phase. The security resource should provide this sign-off to the project manager. If sign-off cannot be given because the security resource did not receive the appropriate information from the project manager or there are outstanding issues, it should be discussed in the project audits. A plan for resolution can be created, and a decision can be made on whether the project should continue or if it must stop until Information Security has confirmed resolution or provided sign-off.

Note that the main contact for the project is the project manager – but these deliverables can be completed by another resource of the project manager's choosing. The subject matter expert, architect or the Quality Assurance resource would be good choices.

A simple handout given to the project manager will help keep track of the deliverables required for the project security methodology. The security resource can also follow it to ensure the deliverables are consistently completed for each project. A sample is shown below in Figure 1 below.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Project Name _____

Project Number _____

- **Concept Phase**
  - Risk Analysis Checklist
  - Project Charter Sign -Off
  - Optional: Minimal Involvement Notice
- **Requirements Phase**
  - Requirements document Sign-Off
- **Analysis & Design**
  - Design Specifications Sign - Off
  - Test Plan Sign -Off
- **Build Phase**
  - Risk Matrix
- **Test Phase**
  - Test Results Sign -Off
- **Post-Implementation**
  - Customer Satisfaction Survey

Figure 1: Sample Security Project Review Deliverable Checklist

Issue Resolution

During the project, team members (including the security resource) will identify issues. "An issue is a problem that will impede the progress of the project…" (5) Most issues will not be of consequence to the security of the final product or pose higher risk to the organization, but the security resource should be aware of all major issues – applicable or not. Regularly reviewing the issues list and resolutions will ensure that vulnerabilities are not missed. Scanning of the issues list should be completed fairly often, since issues have to be resolved quickly and if there is an issue requiring Information Security's involvement, it will need to be dealt with effectively. Also be sure to deal with the root causes of issues and not just the symptoms. Ensure to inform the project manager quickly of any issues that are found. Remember that not resolving an issue in a timely manner could cause the project to stop. If there is a security issue, waiting for the last minute to bring it up is not good customer service. (5)

Audit Reviews

Audit reviews area time to discuss if proper process is being followed, if budgetary, resource or other problems are holding up the project, and get a general status from the project manager. Ensure the agenda includes the requirements for Information Security. Use the audit reviews to discuss any outstanding deliverables not completed or issues that was not resolved up to this point.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Security Resource

Just as the project manager is responsible for deliverables, Information Security also has ownership and responsibility for the deliverables. By assigning a security lead to the project, it ensures deliverables are completed and passed back to the project manager in a timely manner.

Note that for the process to work, during the planning phases the security resource needs to be involved (input or review) with the requirements document, the functional and technical design specs and the test plan. By providing early input to the project manager, security requirements are brought to the forefront and are applied. Before the project manager has an audit review, the security resource should provide sign-off to the project manager, copying Information to the Security manager(s), and the project office.

Being involved in the planning phases has the added benefit of catching security issues quickly – before any effort for building and testing is completed. The security resource is able to collect enough information about scope to know if new network components or penetration testing (network and/or application) will be required before implementation. It's important to know these things early since they can be expensive components to purchase.

The security resource is also responsible for the risk matrix. As stated earlier, this deliverable is based upon data from the planning phases (such as the design specs and network diagrams) and the risk assessment will continue to be validated as build and test phases are ongoing. Before implementation the security resource has a clear picture of any security risks and controls, mitigation factors, and "final" level of risk with mitigations in place. This is a convenient useful document to have and to provide to senior management.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Completing the Project Security Review Process

Rosaleen Citron, CEO of Toronto based IT Security Services company WhiteHat, Inc, says "a good corporate network security policy is useless unless it's enforced and the company puts the necessary technology in place to enforce it." (6)
While this is true, there is more to enforcing policy than using technology. "Security, when you get down to it, is really about risk management" (7).

Evaluate where the risk to the organization is coming from – outside, inside, intranet, extranet (vendors and partners), or Internet. If insecure practices are being used to develop applications (whether internal or external) the assessment may show very high levels of risk. Organizations should understand that risk controls should include project teams – those people that decide how an application is developed and then does the work to deliver it.

Developer compliance with security policy is a big effort. Developers are usually more task focused than strategically focused. They understand their job to be efficiently and quickly develop code, ensure it is bug free, pass the QA reviews and move the application into production. Asking them to add another layer to their process will likely fail. It is not a lack the strategic vision; there is no time to focus on another roadblock to production.

By taking the case a step up to the project managers, compliance has a better chance. Project managers manage tasks and developers time. They are able to provide the focus the developers require to ensure security is at the forefront of the development process. Although subject matter experts provide input into project plans and generate much influence, the project manager is ultimately accountable to see the project completed successfully.

The Project Office

"People often overlook the fact that how information is presented is at least as important as the information itself, and that all policies must be implementable and demonstrably work." (8) Working with the project office ensures the process will work within the project management methodology and is presented to the project managers in the best light. They are the best source of what will work and what will not, and will provide guidance to the process creation. Project office will need to provide buy-in and support for the project review process, but they will also provide enforcement for the process.

As the project management methodology matures, so will the security review process. Stay in touch with the Project Office, and request reports regarding what is working, and what is not, the compliance level and issue resolution status. Continue to work with Project Office through new updates to the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

methodology, since the security process will need to change to meet it. Also remember that as policies and standards change it will affect the project security review process, and updates will have to be provided back to the project office.

Senior Management

To most senior management, security is very hard to understand, and risks are sometimes inconceivable – until a breach occurs. Project Management has a similar reputation. Many senior managers do not understand the importance of project management, and are usually skeptical on the value it provides to the organization. (9) However, if a project office exists in the organization, someone realizes the value. Find the Project Office sponsor and work with him/her. Including the Information Security sponsor in the discussions may help ensure success. Provide information on what the value of the process is, and how risk will be lowered for the organization. Some senior managers will be concerned that a process such as this will add extra overhead to an already high-overhead process. Ensure them that this will help root out security risk, and stop it earlier – which will mean less resources and money being lost later because of a stopped implementation (affect on customers and budget) or a breach because of an unforeseen risk after it's in production, once it is open to the extranet or Internet. Discussions should focus on dollars and business, not security. Budgets get their attention.

A discussion about stopping projects will need to occur as well. If security risks are too great and issue resolution is not occurring, implementations will have to be stopped. Bring a process to senior management (one that was developed, reviewed and/or accepted by the project office). The benefits and costs associated with stopping versus the risks and costs associated with not stopping will need to be stated. By working with senior management on the process everyone is on board when a project implementation is eventually stopped – never a fun process.

Internal Audit

Most organizations have an internal audit group – these auditors ensure that the policies and procedures of the organization are being enforced and followed. They identify weakness and opportunities for improvements. (10) In organizations such as financial institutions there may even be external auditors that ensure industry standards and procedures are also followed.

The security methodology has many benefits when yearly audit time rolls around. It is a proven procedure that is uniformly followed. The process has a standard set of deliverables – including a risk matrix of the project at the time of implementation. Be prepared to show results from the process, which would

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

include the risk matrix. These matrices can be used as baselines for risk for the applications and systems, and ensure any new releases or updates do not add new risks where there were none before. Compare these risk matrices between revisions to see how the application is progressing. Having versions will also ensure internal audit that issues are followed to resolution and risk levels for the organization are monitored. By having the matrices on hand will also reduce any fire drills to gather them before the audit. Audit preparation, and the audit itself, will be less stressful.

Some organizations will need to receive buy-in and approval from the internal audit team for the project security review process. Creating a simple, but detailed presentation or document on the process will help familiarize audit on what the process is, and how it is followed and enforced.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Creating Awareness for the Project Security Review Process

As with any security policies – the project security review process will do no good sitting on a hard disk. It needs to be communicated and enforced.

Post the information to the intranet. If a process document was created, remember to post it. If the project office has a website also post it there. Update the project management methodology documentation with the project security review process, highlighting the deliverables that will be required.

If the IT department has a newsletter or weekly highlights email, include the information in it. The project office will most likely have email distribution lists which you can also take advantage of. Email the process to the project managers and later, send FYI notes about the latest hot topic. And always remember to share lessons learned with the project managers. If there was a major security issue that is expected to occur again, promote it. Remember to also promote the resolution. The project manager maintains the issues list so they are aware of each issue that comes up on their project. If they are aware of a past problem, the rest of the project team will be aware as well.

Enterprise Architecture

Lets revisit the enterprise architecture suggestions from earlier. In larger organizations, the project team may have to go through an architecture review before being approved to execute or even implement. Be part of these reviews. But also remember to educate the architecture team. This paper's focus is on the project manager, but architecture is another area where Information Security should be tightly integrated. This group will have best practices about most everything IT and can also ensure the word gets out to the architects and subject matter experts, which would filter down to the project teams that they interact with. If there is an architecture committee, have a security resource participate.

Security Awareness

Although Information Security resources are great ambassadors for security policies, standards and processes, each person cannot spend 100% of their time with one project team and project manager. There will be many projects per each Information Security resource. Another source of information must be made available to the project manager when resources are not.

Education and awareness programs will provide what is needed. Project Managers follow processes each working day, but new situations mean they

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

need a base level of knowledge to apply to the new situations. Providing education modules or a frequently asked questions (FAQ) list will all help.

One suggestion is to create checklists based on the organization's security policies. The project manager and project team can see how the project stacks up against the policies by completing these checklists. Include a column for *in* or *out* of compliance – any "outs" is a quick validation that they have to fix an issue. The checklists can be used and referred back to during the project life cycle.

Providing education brown bag lunch sessions is a quick and effective way to get "lessons learned" out there, or to at least get information out there on common issues found within projects.

Another idea that can be quite successful is a series of computer-based training (CBT) modules that is based on the organization's policies. As part of the CBT, create a quiz that asks questions about particular aspects of the policy. Multiple choice and true and false works well. It's important to include feedback pages on the answer sheet, since it is an effective way to bring home a particular point. Display feedback regardless of right or wrong answers. Remember – the point is not to stump people, but to enforce ideas.

While the quiz idea may sound easy, it is quite difficult to create them. The questions need to make sense, and cover not just the most obvious points in the policies, but all others as well. However, questions should not be too obscure or misleading. And, don't get too caught up in "pass" or "fail" – focus on creating awareness, even when wrong answers are received.

Remembering who your audience is will help you develop appropriate awareness. For example, while a CBT on the General Security Standards can be used for all users, one on Application Development Security Standards would not be appropriate for the general population.

Once created, present the awareness training to the users. Post the awareness programs with the project security review process documentation (which should be in the same area as the security policies). Employ an authentication method, which can be useful to generate statistics on how many users accessed the site. This information can then be provided to senior management.

Tools That May Help

Security awareness is a whole discussion point in itself. However, if the ideas of CBTs and quizzes on security policies, risk analysis checklists, and/or customer satisfaction surveys are appealing, here are a couple of ideas about tools that may be useful.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

VigelEnt Policy Center, from Pentasafe will not only help educate and monitor knowledge of security policies, it will help with writing policies if the organization does not have them. Charles Cressen Wood's Information Security Policies Made Easy is loaded into it. It has the option of emailing reminders to people that have not completed quizzes, and reports are available on the results. This application can also be used to create a yearly compliance statement and can track that all users have read and acknowledged it. It's pretty easy to use, and can be integrated with Active Directory and other LDAP Directories for access control. It is a little expensive though, especially if the plan is to only use it for quizzes. Also note that the customization for look and feel of the site only goes so far but the sophistication of the quizzes make up for it.

InfoPoll is an online survey application that creates customized, web-based surveys. Once created, use the product to publish the surveys to a chosen user base. It provides instant results and those results can be saved to a database for reporting and analysis purposes. InfoPoll is quite easy to use and most users can be up to speed within a couple of hours or less – and with experience can generate surveys within minutes. It allows various formats for questions so all surveys do not have to look alike. This tool would be quite appropriate for the initial risk analysis checklist and the customer satisfaction survey.

Risk Matrices and Lessons Learned

Like policies, the deliverables created and provided for the project should not be tucked away and only referred to when audit time rolls around. The risk matrices should be stored somewhere where all security resources can get to them. Eventually, the store will become a useful and valuable tool in itself. Security resources can search and find similar problems and review the controls used in each situation, which will speed up security reviews and issue resolution.

Document any lessons learned and provided to the project manager and project office. If an issue went bad explain what will prevent the issue in the future and what could have prevented it this time.

The mistake many make with lessons learned is only focusing on the negative. Remember to also list what went right for the project. The Project Manager will be able to learn as much from the good as from the bad. It also helps boost the spirit of the project team to celebrate successes. Successes can also be carried forward to the next project.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Some Final Advice

If the effort is put forth to create a project security review process or methodology, ensure that it is followed not just by the project office, but by Information Security as well.

Read the project documentation, and ensure security resources go to the project audits and reviews. Commit to doing the risk matrices for each project. They are a lot of work but the resultant matrix has many useful applications.

Consistently apply the standards, and ensure the process is up to date against the policies. Push to resolve issues quickly, to avoid the need to stop project implementations – but don't be afraid to stop them and keep them on hold until resolutions are forthcoming! Celebrate successes with the project team, and ensure to keep communicating the vision of the process through awareness.

Most importantly, have a good relationship with the project managers. The review process is meant to be a two way street. More issues will be resolved more effectively if the Project Manager is able to consult openly with Information Security. Making the effort to understanding the vision and scope of the project will make it easier to apply the appropriate policies and standards, while allowing the project team to understand and apply secure project development.

Working with the project office to create a project security review process where the project manager has ownership for secure deliverables will ensure security policies and standards are consistently applied to the project. Working closely with the project managers will ensure project teams are consistently developing secure project solutions. This will result in a higher level of security for the enterprise.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

End Notes

(1) Risk Decisions

(2) C&A Security Risk Analysis Group

(3) Black, Glenn

(4) Block, Thomas R

(5) Mochal, Tom

(6) ITBusiness Staff

(7) “Putting it all together”, p18

(8) Barwise, Mike; Bentley, Rose. p54

(9) Schulz, Yogi

(10) Howard Hughes Medical Institute

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

List of References

Barwise, Mike; Bentley, Rose. "Making the most of security." Computer Weekly. September 19, 2002, p54. Retrieved November 4, 2002 from EBSCO Publishing online database (Delaware Technical and Community College – Wilmington Campus. 7517924)

Berkun, Scott. "Strategies of influence for interaction designers." November 2001. URL: http://www.uiweb.com/issues/issue18.htm (November 17, 2002).

Black, Glenn. (2002. October). "A faster kind of project management." Professional Remodeler. Retrieved November 4, 2002 from EBSCO Publishing online database (Delaware Technical and Community College – Wilmington Campus.)

Block, Thomas R. "The Seven Secrets of a Successful Project Office". URL: http://www.systemcorp.com/2002/downloads/block_r.html (November 11, 2002).

C&A Security Risk Analysis Group. "Introduction to Security Risk Analysis". URL: http://www.security-risk-analysis.com/ (November 18, 2002).

Christensen, Mark J; Thayer, Richard H. "The Project Manager's Guide to Software Engineering's Best Practices." URL: http://www.computer.org/cspress/CATALOG/BP01199/preface.htm (November 17, 2002).

Howard Hughes Medical Institute. "Our Services the Internal Audit Division." URL: http://hhmi.org/about/iad2.html (November 17, 2002).

"InfoPoll Online Survey software and resources." URL: http://www.infopoll.com/ (November 17, 2002).

"Internal audit in banks and the supervisor's relationship with auditors." Basel Committee Publications No. 84. August 2001. URL: http://www.bis.org/publ/bcbs84.htm (November 17, 2002).

ITBusiness Staff. "Layered approach is crucial in protecting yourself from internal, external threats." Communications & Networking. November, 2002, Vol. 5 No. 11. URL: http://www.itbusiness.ca/print.asp?sid=50489 (November 11, 2002)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Mochal, Tom. "Project Management Tips and Techniques – Managing Issues." URL: http://www.quest-pipelines.com/newsletter-v3/0502_D.htm (November 17, 2002).

"Organizational Project Management Maturity Model (OPM3)". URL: http://opm3.pmi.org/ (November 18, 2002).

Project Management Solutions, Inc. "What is project management maturity?" URL: http://www.pmsolutions.com/maturitymodel/whatispmm.htm (November 18, 2002).

"Putting it all together." The Economist. October 26, 2002 Vol. 365 Issue 8296, p18. Retrieved November 4, 2002 from EBSCO Publishing online database (Delaware Technical and Community College – Wilmington Campus. 7671732)

Risk Decisions. "Definition: Security Risk." URL: http://www.risk-decisions.com/Risk-Management-Slides/sld007.htm (November 18, 2002).

Schulz, Yogi. "Selling project management to the skeptical CEO." Computing Canada October 25, 2002 Vol. 28 No. 21. URL: http://www.itbusiness.ca/print.asp?sid=50423

"Team-Based Project Management: Dealing Effectively with the "People" Side of Projects." Office of Professional Development. URL: http://www.dcs.ncsu.edu/opd/course.cfm?cid=209&sid=451 (November 17, 2002).

Thiry, Michael. "Project Management". URL: http://www.systemcorp.com/2002/downloads/thiry4_r.html (November 11, 2002).

"VigilEnt Policy Center". URL: http://www.pentasafe.com/products/vpc (November 17, 2002).

Xacta Corporation. "Proactive Enterprise Risk Management." p8. URL: www.xacta.com/docs/Hurwitz_whitepaper.pdf (November 11, 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 21st, 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