Conducting an Information Security Gap Analysis

When conducting an information security gap analysis, experts suggest a methodical approach, stressing pre-analysis preparation.

1. **Adopt an information security standard (if one does not already exist)**. Consider ISO 27001/2 for security-only coverage, or COBIT for IT/security governance.
2. **Define the scope of the analysis.** In a large enterprise, it may be prudent - or even necessary - to conduct multiple analyses, evaluating, for example, one location at a time, or assessing network security separate from mobile and wireless security.
3. **Assemble all relevant documents.** This includes all information security standards, policies, plans, protocols, procedures, and guidelines.
4. **Gain senior management approval.** If necessary, the chief security officer (CSO) should "run interference" for the analyst, persuading business and technical managers to cooperate in identifying - and filling - security gaps.
5. **Create a comprehensive information security questionnaire.** Use the questionnaire to elicit information about current information security practices, and expand the questionnaire as new avenues of inquiry appear. Suppose, for example, a preliminary question reveals the use of two different types of physical access controls. A follow-up question might reveal how each type is utilized, setting the stage for a new enterprise standard. In addition to improving efficiency, ***the use of a standardized questionnaire permits a year-over-year***

comparison of gap analysis results, revealing how security performance varies over time.

6. **Look for gaps from a total systems management perspective.** Information security exists within the realm of multiple systems management disciplines, including incident and problem management, change and release management, configuration management, service level management, and IT service continuity management. Ensure that information security is consistent across the full range of these functional areas.
7. **Publish a preliminary Information Security Gap Analysis report.** Before documenting any deficiencies for senior management consumption, offer security personnel an opportunity to review and challenge any findings. Where gaps are discovered, offer these same personnel the opportunity to close or reduce the gaps before a final report is issued. In this way, analysts can earn the trust and confidence necessary to perform an in-depth analysis.
8. **Develop a remediation plan.** Working in concert with the CSO, develop a plan to eliminate - or, at least, reduce - any information security gaps.

Step-by-Step Implementation

While there is no standard methodology for conducting a gap analysis, there is a basic approach, which can be followed by all organizations.

Step 1: Stage a Systems Break-In

Engage a security consulting company to conduct a systems break-in. Ask the company to operate in the manner of a hacker or cyber-terrorist and penetrate enterprise defenses. If they are successful (and, unfortunately, they probably will be), their simulated attack will offer two major benefits:

- For anyone who still needs to be convinced that security is a major issue, it will elevate the level of concern beyond the realm of perceived risk to one of real risk.
- The attack will probably target the same vulnerabilities that real-world cyber-criminals would exploit, allowing the most serious exposures to be identified and eliminated.

Step 2: Secure Senior Management Approval

Much like business continuity planning, conducting a gap analysis requires cross-organizational cooperation. In many enterprises, achieving such cooperation is only possible through the eager endorsement of senior executives. The time to gain organizational cooperation is early on as it is important to get everyone on board when it comes to gap analysis.

Step 3: Establish the Scope of the Analysis

Establish the extent of the gap analysis as well as its general objectives. This can be accomplished by asking the following key questions:

- Will the analysis include physical as well as electronic security?
- Will the investigation focus on the headquarters location, or will it also encompass branch office and remote sites?
- Will the analysis concentrate only on "customer-facing" applications or will it include all IT systems?
- What resources will be available to conduct the analysis? Budget? Personnel? Facilities?
- What is the timetable? When will management expect to see concrete results?
- What regulatory mandates must be adhered to? Are there any mandated procedures that must be used to meet them?
- Have all of the project parameters been established? In particular, have all of the issues been identified? If there are outstanding issues, when will they be resolved?

Step 4: Determine Whether to Outsource or Conduct the Analysis In-house

After receiving permission to conduct a gap analysis, the big question is whether or not to outsource. Table 1 summarizes some of the advantages and disadvantages of outsourced analysis.

Table 1. *Outsourced Gap Analysis*

Advantages	Disadvantages
In general, greater and more current security expertise.	Unfamiliarity with specific enterprise systems and operations.
More experience in gap analysis.	Ironically, the potential for exposure of critical or sensitive information to third parties.
Greater objectivity relative to enterprise security practices.	In general, higher costs.
Less reluctance to criticize enterprise security practices.	Resentment from in-house security personnel, who may feel threatened.

Step 5: Assemble a Gap Analysis Team

Coordinate all activities related to the gap analysis, including: planning, implementation, analysis, reporting, and assembling a gap analysis team. This multi-disciplinary team should include:

- In-house security experts.
- Members of the IT department.
- Customers, both internal and external.

- Trusted business partner personnel, particularly any analysts who are wrestling with the same or similar security problems within their own enterprises.

Step 6: Resolve Any "Jurisdictional" Issues

Closely related to the previous item, determine which enterprise organizations might claim jurisdiction or authority over all or part of the analysis process. Consult with groups such as:

- Finance.
- Corporate Auditing.
- Business Continuity.
- The Project Management Office (PMO).
- The Risk Management Office.

Ask these organizations to appoint individuals to participate as members of the gap analysis team to contribute their own expertise and experience and function as liaisons to their respective groups.

Step 7: Identify Current Security Standards

Determine all relevant security standards and protocols. This includes the enterprise security policy, any statement of enterprise security standards, and, depending on the affected industry, any relevant governmental regulations, such as HIPAA. Sarbanes-Oxley, and the Gramm Leach Bliley Act (GLBA).

Step 8: Collect All Relevant Security Documents

In concert with the previous item, collect all pertinent documentation relating to security standards such as policies, protocols, plans, and

procedures, plus any pre-existing analyses of the enterprise's security infrastructure. It is also important to gather all documentation relating to the deployment and use of enterprise hardware and software.

Step 9: Create a Gap Analysis Checklist

Just like any project, a gap analysis should proceed according to a specific plan or checklist. The checklist is important because it will:

- Ensure the analysis is complete and comprehensive by allowing others to review it prior to implementation.
- Provide a structure for recording (and later reporting) the results of the analysis.
- Provide a baseline for future gap analyses.

Step 10: Conduct a Hardware and Software Inventory

Conducting a hardware and software inventory is vital because it will help determine whether or not the enterprise's hardware and software systems are configured according to asset management plans.

Step 11: Review All Information Security Classifications

Because not all information assets are critical, it is important to ensure that security efforts are commensurate with the value of the information being protected. In some cases, enterprises categorize their information assets according to relative asset value and sensitivity, by applying such terms as:

- Unclassified.
- Classified.

- Confidential.
- Restricted Use.
- Limited Availability.
- Secret.
- Top Secret.

For enterprises that use such categorization schemes, answer the following questions:

- Is the classification scheme employed on an enterprise-wide basis? If not, why not?
- Is critical information properly classified? Check some common information types, such as financial data, personnel records, customer information, and research and development data.
- Are critical information assets marked as critical? In other words, are terms such as ‘classified’ or ‘confidential’ attached to each critical asset?
- Are secured information assets consistent with their classifications?
- Are the graduated security controls adequate to protect the most sensitive assets?

Step 12: Review All Information Access Controls

By one estimate, over 80 percent of all security breaches are initiated by individuals inside the enterprise, or by persons who have left the enterprise under unhappy circumstances. Some employees have

grievances, even if they have not left the company, and many also have access to critical systems. When the two converge, the effects can be deadly.

The best way to mitigate the risk is to ensure that employee access to critical or sensitive information is strictly controlled. To help evaluate such safeguards, determine the following:

- Are access privileges granted on a 'need to know' basis? If not, how are they allocated?
- Are employees required to sign non-disclosure agreements?
- Are passwords and other logical access controls routinely changed?
- Are the user accounts of terminated employees suspended?
- Are inactive or dormant accounts suspended?

Step 13: Examine the System Maintenance Logs

Determine if vendor security patches are being applied in a timely fashion. Consider, for example, that the Code Red worm exploited an exposure in Microsoft's Internet Information Server; an exposure that was publicized at least a month before the worm struck. Had network administrators installed the patches provided by Microsoft when the vulnerability was first discovered, the Code Red worm would probably never have taken hold.

Step 14: Examine the System Software Settings

Determine if any unnecessary options are enabled. Consider, for example, that four days after Microsoft's Windows XP shipped, a California firm, eEye Digital Security, discovered a gaping hole in the

operating system's Universal Plug and Play service; a hole that would allow a hacker to literally take control of another person's PC. Enabled by default in Windows XP, Universal Plug and Play, or UPnP, is designed primarily to help consumers link their PCs with other home appliances. While Microsoft produced a patch to remedy the problem, corporate IT departments are still overwhelmed by the number of security patches Microsoft issues each month. In March of 2008, Microsoft released eleven bulletins which repair a total of 17 vulnerabilities. In a number of instances, Microsoft was forced to issue patches for the patches, or to re-release a patch, which caused problems in the enterprise environment.

Despite the work involved and the threat of installing flawed fixes, it is not an option for an enterprise not to install the patches as they become available. Microsoft is not the only software and system vendor experiencing these problems as almost all major software programs will experience similar situations, and, the more popular the program, the more attention it draws from hackers.

One way for organizations to determined if there are problems with the various patches (i.e., the patch will not install, the patch is infected, flaws exist in the patch, etc.) is to first test the patches on individual systems before installing them on the actual corporate network. This process, alone, could save an enterprise an enormous amount of time, resources, and money.

Step 15: Verify the System Backup Procedures

While normally discussed within the context of business continuity, there is no process more fundamental to the interests of information

security than backup and recovery. If information is lost or destroyed as the result of a security breach, all or part of that information can be restored from off-site media. As a function of the gap analysis, organizations should determine the following:

- Is electronic data being backed up on a regular basis?
- Is the backup data being stored in a secure offsite location?
- Importantly, considering that offsite data can deteriorate over time, what controls are in place to ensure its continued viability?

Step 16: Interview Employees and Other "Security Users"

Despite an enterprise's best laid plans, there is often a wide gap between a system's intended use and its actual use. To measure the level of compliance with access and other security controls, interview the users on a confidential basis to ensure cooperation and candor and then try to determine the following:

- Has the importance and need for security been explained to employees?
- Are employees aware of the latest security policies, practices, protocols, and procedures?
- Do employees feel these procedures interfere with their work?
- Do employees attempt to circumvent any of these inconvenient procedures? Are they successful in doing so?
- Which procedures, if any, would employees retain, and which procedures, if any, would they eliminate?
- What would employees do if they had the responsibility for administering security?

Step 17: Evaluate Current Security Practices

Determine the efficacy of current security practices by comparing the conduct of those practices against established enterprise norms and

generally-accepted security principles. For example, most enterprises require that corporate PCs be equipped with anti-virus software. To assess compliance with this practice, ask the following:

- Do all PCs have anti-virus protection?
- Are these anti-virus packages updated as soon as vendor maintenance patches are released?

Step 18: Document All Findings and Recommendations

At the conclusion of the gap analysis, it is vital to document (in detail) all findings and recommendations.

Step 19: Develop a Remediation Plan

While not technically a part of the gap analysis, it is a good practice to develop a plan to plug the holes the gap analysis discovered. In developing a plan, schedule activities according to the severity of the exposures, with high-risk items earning first attention.

Step 20: Schedule the Next Gap Analysis

Security planning is not a one-time-only event. Because the enterprise environment is subject to constant change, and new security threats arise on a daily basis, the shelf life of a security gap analysis is relatively short. A new gap analysis should be conducted every three to six months or more frequently if enterprise resources can support it.