SANS MGT442: Information Security Risk Management

Building a Risk-Based Security in 10 Easy Steps

Everyone talks about the need for a risk-based approach to information security, but nobody teaches you how to implement a focused program. The following workflow guides you through the essential steps of the process. You can also use this list to audit/assess an existing program.

1. **Develop Basic Security Policies & Standards** – You need to set out the expectations before you can assess your organization's compliance. If you are building a program from scratch, I wouldn't even bother with any other aspects of risk management until the most basic policies around Acceptable Use and Data Classification are established. For example, you can't assess a resource's risk exposure until you have a way to classify the levels of information sensitivity.
2. **Establish an Asset Inventory** – Having an asset and data inventory is such a basic part of any security program, but in many cases it looks easier than it is. There are many ways to start gathering this information if you don't already have a central database of assets including vulnerability scanning, polling infrastructure devices (DHCP, DNS, NAC, etc.), leveraging an existing asset naming convention, or referencing software licensing & maintenance contracts.
3. **Establish Information Security Leads** – ISL is responsible for ensuring the execution of security risk management controls and information security program and is responsible for overseeing the production, maintenance, use and access to information resources for that functional area. ISLs must be equipped with the knowledge, skills, time, tool, contacts and authority need to fulfill their role. ISLs are responsible for and accountable for the oversight of security administration activities within their assigned functional areas.
4. **Implement an Enterprise Risk Committee** – In most organizations the Enterprise Risk Committee is made up of senior management or their representatives. All the different functions should be represented, especially Infosec, Legal, Compliance, HR, Operations, and Finance. To be successful, you need to have a forum to escalate the most serious risks to senior management and allow them to make decisions about how to address them.
5. **Define a Common Approach to Risk Calculations** – When someone says that a particular asset is "risky", what does that mean? Does it mean that it has a low tolerance for risk exposures? Does it mean that it has a high degree of exposure? Does it have known vulnerabilities that are exploitable? It seems like everyone in the field, and maybe even within your organization, measures risk slightly differently. If you want to have consistent measurements of risk that you can compare across the organization, then you need to define a common way to calculate risk.
6. **Establish a Threat & Vulnerability Management Program** – At a basic level this should include a method of evaluating new vulnerabilities as they are identified through a notification service, and scanning the environment for known vulnerabilities. This doesn't have to be the perfect solution to cover every possibility from the beginning, start small and build from there.
7. **Establish a Compliance to Standards Review Process** – Identify your organization's most critical resources, and perform a gap analysis against your established security policies/standards. Any deviations should be identified as findings and analyzed according to the risk that they introduce.
8. **Conduct Basic Risk Assessments for Third-Party Services/ Vendors** – You will need to conduct some level of risk assessment whenever you engage a third-party vendor or service provider. This does not need to be an in-depth security audit for every third-party, rather the detail of the assessment should depend on the sensitivity of the function they are providing. Often a simple questionnaire will suffice (for example consider the BITS Standardized Information Gathering Questionnaire, known as the SIG, www.sharedassessments.org).
9. **Implement a Risk & Exception Tracking System** – You need to establish a system for tracking the state of risks in your environment. Could be as simple as a spreadsheet or SharePoint site. You want to track risks associated with different resources, and document all the details of the analysis, especially the reasoning for rating a risk at a certain level, any compensating controls, and details of the mitigation plan.
10. **Launch an Risk Awareness Campaign** – It can be hard to change the culture of your organization and often very hard to repair any misconceptions of security as a hindrance to innovation and progress. The goal of a risk-based program is to establish a methodology to assess the real needs of the organization and find the right balance of security. You may need to educate the organization about this shift from absolute security to a risk-focused culture. Get members of the organization involved in identifying risks and feeling like they have a stake in the game.

Glossary of Terms

A common challenge in the field is a misuse of several basic risk terms. This can make discussions of risk between groups or up the management chain very difficult. Use this glossary as a tool to establish a common vocabulary for risk within your organization.

Asset - something of value that can be harmed or lost (also called "resource")

Compensating Controls – existing controls that may lessen or contain the risk in some way. These controls may not match current standards, but meet the intent of the standards to some degree.

Likelihood – a measure of the probability that the threat/vulnerability pair will be realized

Mitigating Controls – additional controls that are added to lessen or contain the risk in some way

Mitigation Plan – a plan of action describing how short-term and long-term steps to lower the risk exposure to an acceptable level

Residual Risk – the estimated level of risk exposure after implementing any mitigating controls

Risk - the potential of a threat (source) acting upon a vulnerability (weakness) causing an undesirable event for an asset (target). The risk is evaluated based on the probable frequency and probable magnitude of that event, which determines the degree of exposure.

Risk Assessment Maturity – a measure of how mature the organization feels their understanding of this risk is, and their confidence level in their ability to assess it accurately

Risk Domain - a high-level logical grouping of risks affecting a certain area.

Risk Exposure - describes the likely outcome of a successful exploit of the vulnerability by the threat. Qualified by how likely the event is to happen and how severe the consequences are if it happens. This is a measurement of the risk.

Risk Sensitivity – a relative measurement of the asset's tolerance for risk exposures, similar to an evaluation of criticality or importance to the organization, independent of any particular threat or vulnerability. Typically measured on a scale of Low-Moderate-High.

Severity – a measure of the magnitude of consequences from a threat/vulnerability pair being realized

Threat – anything (also called a source or actor) capable of acting against an asset in a manner that can result in an undesired event

Vulnerability – the weakness that makes the asset susceptible to the threat

Inherent Risk - an evaluation of the risk exposure absent of any mitigating controls or constraints that may limit the actual level of exposure