5 STEPS TO GET STARTED WITH RISK MANAGEMENT

Most large organizations have been developing risk management programs over the past several years. However, newer organizations or those who have experienced rapid substantial growth are discovering that their risk management activities are not sufficient to adequately protect the organization. In this article, we will look at how to get started (from a very high level) in risk management for your organization.

Think of risk management as a program not a project

The Project Management Institute states that "A project is temporary in that it has a defined beginning and end in time, and therefore defined scope and resources", whereas a program is "a group of related projects managed in a coordinated manner to obtain benefits not available from managing them individually".

For organizations to effectively manage risk, the first step is recognizing that Information Risk Management should be a program not a project. Information Risk management is not something that has a defined beginning and end. It is a series of connected projects that seek to reduce the overall risk exposure in the organization. Therefore, organizations are usually best served by approaching risk management through the development of an Information Risk Management Program (IRMP).

Basic Components of a Risk Management Program

While there are many versions of the basic steps in risk management, most of them will boil down to these five key steps:

1. Discover risks to the organization
2. Analyze risks and assess the impact
3. Implement Controls
4. Monitor
5. Communicate and Report.

1. **Discover Risks to the Organization**
   The first step in getting started is to discover what your risks are. You can think of this as a risk inventory. There are a couple of ways to do this. I recommend both an internal approach as well as an external review.

   Internally, oftentimes organizations assemble a risk management advisory group or task to help identify risks. This group should be more than just the IT department. Be sure to include representation from the major risk containing business units. Conducting scenario-based activities are a good way to help identify risks. By simulating the loss, deletion or exposure of information, the group can get a good understanding of how that loss impacts the organization.

   For the external review, it can be helpful to have legal counsel review your organization and help you understand what regulations apply (depending on your industry). This can be incredibly helpful in identifying any risk management areas that must be addressed quickly.

Risk management is not DIY

There are two proper paths in getting started with risk management. Hire expertise or leverage an existing consulting firm. If your IT organization has grown from a "jack of all trades" team of people, consider hiring someone with a background in risk management / information security. This role should not be something that is added to existing duties. If you are not ready yet or are not large enough to have a dedicated security professional, hire an external consulting firm. At a minimum, have them look at your activities and documents produced to confirm that you are on the right track. This will lend credibility to your efforts and may help you out later if you find yourself in legal trouble because of a security incident.

---

2. **Analyze Risk**
   Once you have a good risk inventory you can begin to analyze the risks affecting your organization. This doesn't mean a detailed analysis of everything included in your inventory. What it does mean is that organizations must develop a method to prioritize risks. While your initial reaction may be to attempt to eliminate all risks, in most circumstances this simply isn't feasible. Many scoring systems and frameworks are available that can assist with this. At the heart of all of them however is a mechanism for understanding the impact of the risk (how bad will it really be) and the likelihood of the risk occurring. By understanding these two components of risk, organization can make much more informed decisions on how to address risks.

One other component that often makes its way into the risk conversation is risk tolerance. Some organizations are very risk adverse and are willing to spend the time and effort to reduce risk as much as possible. Other organizations may be a bit more willing to accept risk if they feel the cost of addressing it is too high or doesn't offer any organizational benefit.

3. **Implement Controls**
   After inventorying risk and completing your basic risk analysis, it is important to put controls in place. Controls are policies, systems or tools that allow you to manage your risk. Most of you have heard of the stringent controls required for storing Payment Card Industry (PCI) data. These are all intended so that organizations meet the minimum level of risk of storing that data as defined by PCI. Many regulated data types will have their own controls for protecting Information Technology systems and data. However, for non-regulated data you will need to rely on industry-specific best practices or develop your own.

   Development of risk management controls an area where existing frameworks can really help organizations get up to speed with risk management. I am a big proponent of never reinventing the wheel. It may be helpful to existing documentation from NIST and other organizations to see what frameworks exist for addressing the most critical risks in your organization. Even if you do not have a mandate to achieve full compliance with a particular standard, you can leverage some of the concepts and controls that apply to your organizational concerns.

4. **Monitor**
   Once your controls are in place you need to keep track of which controls have been met and which ones the organization is still working on. By monitoring your controls, an organization can get a good picture of where they are in with regards to reducing their risk. In some situations, risk can actually go up based on mergers, acquisitions or changes in organizational structure. With robust risk monitoring in place organizations can get a much better picture of the true costs of changes to the organization and if there are any risks that may outweigh the perceived benefits of the change.

5. **Communicate and Report**
   The last step in risk management is reporting your risk activities. By providing comprehensive risk management reports to organizational decision makers, the organization can be better understand what the risk are as well as how the risks are being addressed. Reporting is also a required component if you manage any type of regulated data.

   When developing this part of your risk management program, it is important to consider your audiences. Risk management isn't something that only gets reported to one audience. Senior leadership will want to have summary information and will expect you to provide them with an overall picture of the risk exposure in the organization. They will also want to know any areas where the organization is having trouble meeting its risk reduction objectives, as well as areas where risk has been significantly reduced.

   Departmental staff will want operational information. They will want to know progress made on specific risk controls or control areas. They will also be interested in any interpretations or misunderstandings of risk controls.

Change in Culture

A successful information Risk Management Program ultimately results in a change of culture in your organization. The aim of any risk management program is to reduce (not eliminate) the amount of risk in your organization. The only way of doing this, is to instill risk management practices in every area of your organization.

Some organizational leaders will ask "when are we going to be done with risk management?" Unfortunately, the answer is "never." Risk management as a continual practice is now vital for continued organizational success.

Recommended Readings

SANS Institute InfoSec Reading Room - An Introduction to Information System Risk Management: https://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204

SANS Institute InfoSec Reading Room - An Overview of Threat and Risk Assessment: https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

NIST Special Publication 800-30 – Guide for Conducting Risk Assessments: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

NIST Special Publication 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View: https://csrc.nist.gov/publications/detail/sp/800-39/final

NIST Presentation on Risk Management Framework: https://csrc.nist.gov/csrc/media/projects/risk-management/documents/ppt/risk-management-framework-2009.pdf

ISACA – Performing a Security Risk Assessment: https://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx

ISACA – Developing and Information Security and Risk Management Strategy: https://www.isaca.org/Journal/archives/2010/Volume-2/Pages/Developing-an-Information-Security-and-Risk-Management-Strategy1.aspx

Security Intelligence – Key Components of a high performing information risk management program: https://securityintelligence.com/key-components-of-a-high-performing-information-risk-management-program/