tracesecurity
GRC Simplified... Finally.

TRACESECURITY WHITE PAPER

Integrating Risk Assessment into Lifecycle Management

Jerry Beasley, CISM and TraceSecurity Information Security Analyst

Executive Overview

Working as an information security consultant, I visit many diverse organizations, ranging from government agencies and financial institutions to private corporations, but they all have things in common. For example, they all manage information systems, and they are all subject to regulatory requirements and/or oversight. Given these similarities, the subject of risk assessment often arises.

During one such visit, an executive described the implementation of a new enterprise information system. He was observably proud of their progress to date, and the system was almost online. At the conclusion, the executive stated, as an after-thought, "Once we get online, I guess we'll need to talk about getting a risk assessment."

The old "smoke test" metaphor immediately came to mind. This term is sometimes used by engineers when building a new electronic prototype. The builder flips the switch and hopes that the device doesn't go "up in smoke." When applied to information security, this can be disastrous, both in terms of business impact, and in terms of legal liability.

Don't be too surprised at the executive's thought process. This is a common misconception about risk assessment, and in some cases is perpetuated by the idea that risk assessment is simply a regulatory requirement. In reality, the most successful enterprises are those that integrate risk assessment, and more broadly, risk management, into their lifecycle processes. The drawback of the alternative should be obvious. If a risk assessment is done after a system is developed and tested, many changes may be required after-the-fact to integrate the required security controls.

Within this white paper, I will discuss how risk management can be integrated into lifecycle management. To get started, we'll take a quick look at what's involved in these processes we call risk management and lifecycle management.

Clearing Up the Confusion

With a simple internet search, you will find many definitions and contexts of risk management. By context, I mean that risk management processes can focus on different aspects of risk in an organization, such as operational risk, financial risk, or as is TraceSecurity's focus, information security risk.

Risk Management

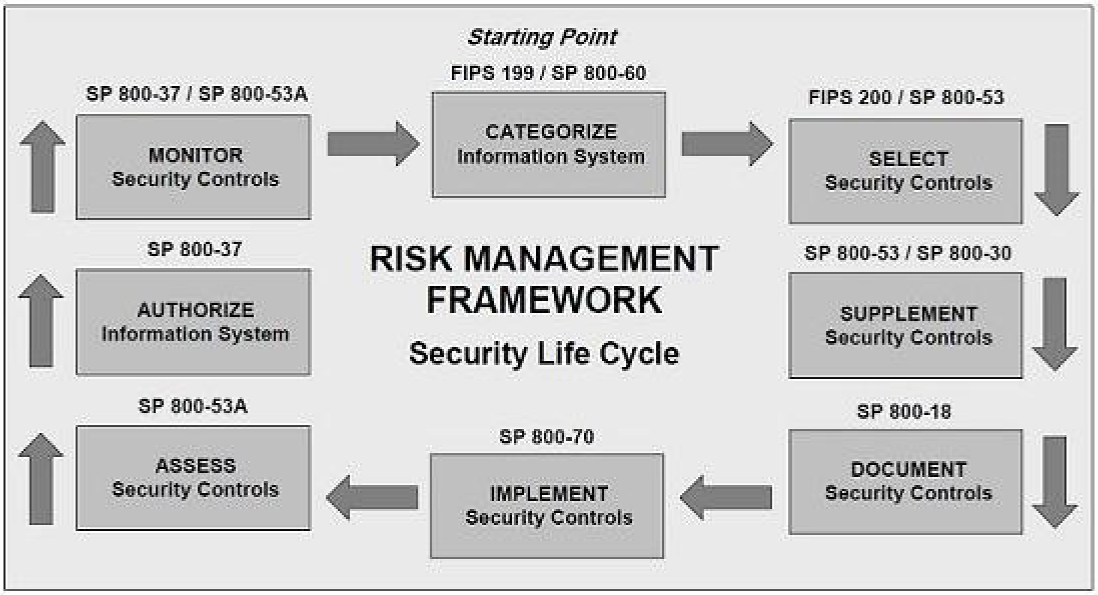
One definition of risk management states: "Risk Management is the identification, assessment, and prioritization of risks as the effect of uncertainty on objectives followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities." If that sounds a bit esoteric to you, let me provide a simpler definition.

To me, risk management is about anticipating what bad things might happen to your assets, then mitigating the impact of those bad things, or reducing the likelihood that those bad things will happen. In the information security context, we are primarily concerned with assuring the confidentiality, integrity, and availability of sensitive, personal and business data. We'll further address the process of doing this later.

Risk Assessment

You will often hear the term risk assessment used interchangeably with risk management. However, risk assessment should be thought of as a "piece" of risk management, albeit a very important one. Risk assessment is the analysis that takes place in order to make risk management decisions. More specifically, it is the process in which an organization identifies its information and technology assets and determines the negative impact that threats have to specific assets, what's currently being done (current controls) to mitigate the impact or likelihood of an occurrence, and what else could be done (prescribed controls) to further effectively mitigate the impact or likelihood of an occurrence.

Risk management also includes the prioritization and application of prescribed controls, monitoring the effectiveness of these controls, and ensuring that additional risk assessment is performed as the assets and the threat landscape change. It's important to note that there are numerous standards and models for risk management and assessment. Some of the more common standards or models include the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) supporting the Federal Information Security Management Act (FISMA), and the International Standards Organization (ISO) 31000 series, addressing risk management standards. An illustration of the NIST RMF is available on the NIST web site and also duplicated below.



LIfecycle Management

"Lifecycle management" is another term that is used in many contexts but in general applies to managing the development, acquisition, implementation, use, and disposition of an entity. In information processing, it is often related to the Software/System Development Life Cycle (SDLC) or sometimes the Product Lifecycle (PLC). In these two examples, the focus is on a particular system or product, but as we will see, lifecycle management often has applications beyond the confines of a "system." Depending on the model you follow, lifecycle management generally includes the following phases or activities.

- Requirements definition / specifications
- Development / acquisition / testing
- Implementation / configuration
- Operations / maintenance
- Phase out / disposition

Risk Management's Role in Lifecycle Management

In addition to the technology involved in implementing a system are the procedures, training, and physical controls. The definition of a system can include these controls as the effectiveness of the system may not be possible without them. For example, without physical controls, the technology may be damaged, lost or stolen. Without personnel controls and training, a system can be misconfigured or misused. Keeping these in mind, let's think about how risk management supports the lifecycle management process in meeting information security goals.

Requirements and Specification Development

This is likely to be the most critical phase in any lifecycle management process as it provides the roadmap to either develop or acquire a system that meets the business requirements of the organization. Inaccurate or ill-conceived requirements at this phase can translate into costly changes later in the project. It is equally important for risk management to be established at this point.

Key activities that should occur during this phase include establishing a process and responsibilities for risk management and documenting the initial known risks. At a minimum, the project managers should identify, document, and prioritize risks to the system. This process should include identifying assets to be protected and assigning their criticality in terms of confidentiality, integrity, and availability – determining the threats and resulting risk to those assets, as well as the existing or planned controls to reduce that risk. Prioritization allows the project managers to focus resources on areas with the highest risk. When necessary, the requirements and specifications should be modified to include new requirements for additional security controls identified during this phase.

System Development, Acquisition and Testing

This phase translates the requirements into solutions, so accurate classification of asset criticality and planned controls are critical to successful development or acquisition. For example, if the system has a requirement to transmit data across a public network and the criticality rating for the confidentiality of that data is high, then some control, such as application encryption or a virtual private network, may become part of the solution. As the system is developed, testing of each control is necessary to ensure that the controls perform as designed.

Implementation and Configuration

During this phase, the system is implemented and configured in the form that it is intended to operate. Testing is equally important in this phase, especially to confirm that the designed security controls are operational in the integrated environment. The system owner will want to ensure that the prescribed controls, including any physical or procedural controls, are in place prior to the system going live.

Operations and Maintenance

Very few systems are static, so changes to a system are expected. Most organizations acknowledge that a means to control the system configuration is necessary. A configuration management process helps to ensure that changes to the system hardware, software, or supporting processes are reviewed and approved prior to implementation. The piece that is sometimes missed is the resulting change to the risk posture of the system.

Any change to a system has the potential to reduce the effectiveness of existing controls or to otherwise have some impact on the confidentiality, availability, or integrity of the system. The solution is to ensure that a risk assessment step is included in evaluating system changes. For organizations that employ a configuration control board, the addition of a risk manager or security specialist to this body can facilitate the integration of risk assessment into configuration management.

We've acknowledged that systems change, but unfortunately, threats can change as well. When new threats are identified, new controls may be necessary to bring risk to an acceptable level. This is why periodic risk assessments are important, even when a system changes infrequently. Risk assessment can provide an added benefit in this phase as a means to improve the effectiveness of policies, procedures, and training. When control deficiencies are identified, support personnel and users may need new training or guidance to minimize risk to the system.

Phase Out and Disposition

This phase deals with the process of replacement and/or disposal of a system. If a risk management plan was developed at project inception, it should have identified the risk to confidentiality of residual data during this phase. Given that known risk, the risk management plan will have identified the proper procedures or controls to reduce the risk of data theft or retrieval due to improper disposal. Given the dynamic nature of many systems, the disposition planning is often overlooked. However, by identifying the risk early in the project, the controls could be documented in advance ensuring proper disposition.

Conclusion: Taking the Next Step

One might ask, "Well, all these are great ideas, but where do I start?" Fortunately, there are many resources available. Solutions might include simple process descriptions, data gathering tools, or more sophisticated risk analysis and automation tools. Since no two organizations are the same, no model or solution is "one size fits all". TraceSecurity recommends you become familiar with the available resources and whether independently, or with the assistance of a trusted provider, establish a risk management program that best meets your organization's needs.

About TraceSecurity

As the leading pioneer in cloud-based security solutions, TraceSecurity provides risk management and compliance solutions for organizations that need to protect critical data or meet IT security mandates. With a unique combination of people, processes and technology, we give decision-makers a holistic view of their security posture and enable them to achieve effective data protection and automatic compliance. By streamlining and assuring effective IT GRC management in this way, we dramatically reduce the complexities of ever-changing threats and technology – and empower organizations to better pursue their strategic objectives.

TraceCSO

TraceCSO is a ground-breaking innovation that finally puts enterprise-class IT GRC management within the reach of any organization, most of which don't have the benefit of a Chief Security Officer or a dedicated IT security team. By transforming IT GRC into a unified and easy-to-manage business application, it changes the game in big ways:

It introduces automatic security and compliance, with built-in expertise and best practices that eliminate guesswork, as well as the need for internal security specialists. The interface, controls, documentation and reporting functions are simple and can be easily mastered by non-technical users.

It delivers dramatic savings, with a simple year-to-year browser-based subscription model. It is affordable, scalable, and eliminates the need for capital investment. This results in a savings of more than 80% over the installed cost of comparable point solutions, and a total cost of ownership (TCO) estimated to be up to 50% lower.

It enabkes rapid deployment, because it is a unified, browser-based platform and includes expert implementation services from TraceSecurity. Typically, TraceCSO can be up and running in a matter of weeks, without any business disruption – versus conventional solutions that have been known to require deployment schedules exceeding 12 months.

It accommodates on-going change, thanks to its platform architecture, integration with the UCF database, and combination with TraceSecurity professional services and consulting. TraceCSO is the market's only long-term IT GRC solution. It is complete in its functionality, designed to accommodate new functions and features, easily scales to thousands of users, and is always current with every regulatory and industry mandate in the world.

To learn more about TraceSecurity, TraceCSO or our information security services, call 877-275-3009 or visit www.tracesecurity.com

ISO 31000 Risk Management Standards: http://www.iso.org/iso/home/standards/iso31000.htm
FISMA: http://csrc.nist.gov/groups/SMA/fisma/index.html
NIST Risk Management Framework: http://csrc.nist.gov/groups/SMA/fisma/framework.html
NIST Special Publication (SP) 800-64, Security Considerations in the System Development Life Cycle:
http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
NIST SP 800-30, Guide for Conducting Risk Assessments: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
FFIEC Information Security Risk Assessment: http://ithandbook.ffiec.gov/it-booklets/information-security/information-security-risk-assessment.aspx
TraceSecurity Risk Assessment Support: http://www.tracesecurity.com/services/risk-assessment.stml

tracesecurity
GRC Simplified... Finally.