GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Implementing an Information Risk Management Program

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

Option 2 - Case Study in Information Security

Submitted by: Daniel A. Sokulski

Paper Abstract: "Case study on implementing a comprehensive information risk management program in a large scale organization."

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

List of Figures

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Preface

Abstract

The focus of this case study is how to implement a dedicated Information Risk Management (IRM) program in a medium to large-scale organization. The task of creating and cementing this type of significant and widespread program within any organization is beyond the limits of just one person, so the scope of this document is based upon my own experiences and lessons learned as part of a small team that carried out the challenge of materializing a dedicated information risk management program within our organization. This document is intended to provide guidance on how a security professional could go about establishing an IRM program within his or her own organization based on good practices from a real-life 'success story' (albeit 'ongoing'). The following key aspects of a comprehensive IRM program are spotlighted:

- Information Risk Management Drivers (i.e. Why IRM is important and necessary)
- Formalized Information Risk Assessment process and methodology
- Information Risk Management processes, procedures, and strategies
- Information Risk Management Reporting (Industry benchmarking, Security Metrics and Control Recommendations or 'safeguards')

Preliminary Notes

Please note the following points relative to terminology used throughout this document:

- In the context of this document, the terms "Information Risk Assessment", "Information Risk Analysis", and "Information Risk Management" *are not* synonymous. Information Risk Assessment refers to the actual meeting or 'facilitated session' where an information resource is evaluated with appropriate representation from subject matter experts. Information Risk Analysis is specific to the examination and recommendation of commensurate security controls based on the completed assessment results. Information Risk Management is the overall program-level endeavor of supporting and maintaining processes and effort related to information risk assessments, industry benchmarking, security metrics, and any other IRM-related activity.
- The term **"**information resource" is synonymous with any application, system, third party arrangement, installation, development activity or other related environment that would undergo an information risk assessment. "Owners", "decision makers, and "management" are also and typically used in the context of being recipients of information risk results and other IRM-related reports.
- The term 'information risk' and 'risk' are used synonymously in this document. The focus is always on *information* risk management and never other forms of risk, such as financial risk, market risk, etc.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

Introduction

One of the most significant and common areas of weakness within organizations' information security program is information risk management. Research conducted by the Information Security Forum (ISF) which states: [1]"*in less than half the cases (49%) do organizations carry out information risk analyses for critical business applications, networks and computer installations (e.g. Data Centers). Where they were performed, critical applications typically had much stronger controls applied and were less likely to suffer incidents". Furthermore, "business risks associated with information and systems are not analyzed using a formal risk analysis method in more than half the cases*". This basically says that of all the information risk assessments being done today, only about half of them are done effectively. Until recently, the organization in this case study was no exception to this finding. Overall, Information Risk Management was simply not fully understood or staffed within what we will call "our" organization. The good news to this bleak picture is that with the steps outlined in this document, a team with three to four dedicated members has made gratifying strides towards implementing a comprehensive IRM program in a relatively short amount of time.

Previous IRM Challenges ('Before Snapshot')

Information Risk Management's principle goal is to manage the harm a business can suffer as a result of the loss of confidentiality, integrity, or availability of information. It also provides decision support by helping management understand the balance between the impact of risks and the cost of implementing measures to protect an organization from those risks. [2]The goal of IRM is to identify, measure, control, and minimize or eliminate the likelihood of a threat materializing. IRM also encompasses the variety of processes conducted to address information risk within an organization. A dedicated IRM team should be established within your organization to develop, maintain and support this collection of IRM processes and tools. The team's mission should be to **develop, integrate and support processes that enable decision makers who are responsible for information and systems to identify key risks and agree upon the controls required to keep those risks within acceptable limits.**

The inherent challenge associated with IRM is its relative immaturity within most organizations when compared to other information security disciplines (e.g. security policy, security awareness, virus protection). It is recognized as being fundamental to any Security program; however, it is still widely misunderstood, inconsistently performed, informal, and in some ways overwhelming. A mantra repeated often in this study is IRM cannot be effective without formal, consistent, and repeatable processes and methodologies. Our organization recently faced a similar scenario where we did not have a comprehensive IRM framework that took into account formal, consistent

[1] According to the Information Security Forum's *Improving Security Management Enterprise-Wide; June 2004*

[2] According to SANS Institute Volume 1.3, chapter 18; *Internet Security Technologies*

© SANS Institute 2000 - 2005, Author retains full rights.

methodologies for assessing information risk. Information risk assessments were done in an informal, ad hoc manner without defined processes or procedures. Additionally, the IRM team was not properly staffed to carry out other IRM-related activity such as security metrics and industry benchmarking. The challenge our organization and team faced can be described as the following:

General IRM Shortcomings

- Staffing inadequate to effectively develop, support and provide information risk management services.
- Management and enterprise staff did not widely understand purpose of benefits of information risk management.
- No clear strategy for evolving the Information Risk Management program within the organization.
- Industry benchmarking was not being done (i.e. determine how our overall security arrangements compared to industry peers)
- Information Security metrics not provided in defined, consistent manner
- Security Requirements not consistently gathered from Information Risk Assessment process (i.e. controls applied to applications often did not match their requirements for security, which potentially led to either unacceptable risk or unnecessary cost)

Information Risk Assessment-Related Challenges

- No consistent approach to conducting information risk assessments.
- Existing Information Risk Assessment (IRA) methodology was extremely manual. Information security staff would commonly avoid doing a risk assessment rather than undergoing the tedious methodology that was in place.
- Information Risk Assessment outputs and results were requested, documented, and stored inconsistently.
- No published procedures to help information security staff understand *when* and *how* to request and conduct information risk assessments.
- Information Risk Assessments were generally not quantitative enough.
- 'Facilitation' of information risk assessments not provided as an IRM Team service.
- IRA methodology did not adequately engage *business* side of organization.
- No consistent, repeatable manner in which to escalate information risks to appropriate levels of management.
- Lack of business understanding in information risk assessments (i.e. IRAs did not adequately account for the business perspective; they were mostly technical-oriented).

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

Proposed Solution Summary ('During Snapshot' pt. I)

Information and guidance on how we addressed the organizational challenges related to IRM are detailed in this section. The following is a summary of the major solutions and enhancements introduced over the past one-two years (if you are struggling to establish a comprehensive information risk management framework within your organization, this listing can be used as a 'checklist' to help you reach your IRM objectives):

1. Receive IRM Buy-in from Top Management: It is obvious but worth emphasizing that support from top management is crucial to an effective IRM program. We achieved management buy-in by emphasizing the benefits of IRM as well as internal and external business drivers (e.g. Corporate Governance, Industry Regulations and Legislations, Industry Standards, Internal Standards, etc.). In addition to these drivers and influences, marketing IRM as a form of *decision support* for leadership/management was an effective form of marketing IRM. More details later in this section.
2. Create Dedicated Information Risk Management Team: A dedicated IRM team was established to specifically focus on developing, maintaining, and supporting Information Risk Management activities and processes across the enterprise. The number of team members may vary depending on the organization's size; however, three or four dedicated team members proved adequate for our company. Ultimately, the team should provide the organization with services to coordinate and facilitate information risk assessment activities, as well as provide IRM consultation, consistent processes and procedures, and other forms of expertise and attention to all Information Risk Management-related matters.
3. Introduce Formal Information Risk Assessment Methodology: An information risk assessment (IRA) methodology should include a full assessment of threats, vulnerabilities, business impact, and criticality of the information resource being evaluated. The IRA methodology should also drive out tangible action items and requirements that provide solutions to address weaknesses in the environment identified through the IRA (i.e. security controls). Key participants and subject matter experts should include information security professionals as well as representation of both the business and technical aspects of the information resource being evaluated. The dedicated IRM team should provide coordination, support, and facilitation for the entire lifecycle of the information risk assessment process.
4. Develop IRM Strategy: An IRM Strategy should be agreed upon and documented. The purpose of the strategy document is to target and describe short term *and* long term objectives for information risk management within your organization.
5. Establish Process for Handling Information Risk Management Services: In the past there was no standardized way for information security staff to request IRM services. In order to address this gap, an electronic form was developed to request IRM Team services. These services include options to request an information risk

assessment facilitated session, IRM consulting, IRA information (i.e. data from a completed IRA), and IRM communications. The form includes fields for the requestor to describe scope, background and subject matter experts related to the IRM services request being made. The form is automatically sent to a dedicated e-mailbox where our team analyzes the request form and assigns an IRM team liaison to work with the requestor.

6. Take Part in Industry Benchmarking: [3]"*Benchmarking is a process in which businesses use industry leaders as a model for developing business practices*". From an information security standpoint, this involves determining where you need to improve (examples may include risk analysis or data classification) and where you are relatively strong (e.g. virus protection, information security awareness). Industry benchmarking is beneficial because it helps to determine 'how you stack up' against industry peers. Whether your organization seeks to be ahead of the pack, right in the middle, or perhaps even behind the group, industry benchmarking can help a company understand where it is performing well and where it might consider improvements.
7. Establish Means for Gathering Internal Metrics: Internal metrics provide input to help management/leadership determine strengths, weaknesses, and where additional focus and resources are required within an information security program. 'Report Cards', Scorecards, and graphical representations (e.g. 'traffic light' diagrams), and other forms of 'dashboard'/quick-glance formats are common for reporting metrics. Metrics-reporting falls within the boundaries of information risk management because it provides quantitative data on performance related to threats and vulnerabilities (i.e. viruses blocked vs. viruses experienced). Metrics in this context contain tangible statistics across multiple aspects of Information Security. It is a periodic (monthly, annually) report for management to track progress in specific categories of information security.
8. Develop IRM Processes, Procedures, and Education: Our team went through rigorous 'process modeling' sessions to define and document our processes and services, how they interrelate, and how they can benefit information security staff. Detailed procedures were also developed for each step of our process model. The new processes and procedures were communicated to information security staff through a series of presentations. Additionally, we developed a training workshop for information security staff and management to educate them on our IRM process, services, and how our team can help them succeed in their IRA efforts.
9. Adopt Quantitative and Qualitative ('measurement-based) Information Risk Assessment Approach: Qualitative combines expertise, opinions and judgment that are captured as "comments" in the IRA to provide context to the ratings given. The quantitative approach assigns numerical values to variables that determine risk (threat, vulnerability, criticality and business impact).
10. Integrate with Key Business and Technical Areas: Reaching full maturity for IRM requires a joint endeavor between your internal IRM team efforts along with with other business areas and departments. An IRM team's success is dependent on

[3] Benchmarking definition according to BambooWeb Dictionary web site: www.bambooweb.com/articles/b/e/Benchmarking.html

© SANS Institute 2000 - 2005

Author retains full rights.

collaborative efforts with other areas such as Auditing, Contingency/Disaster Recovery, Service Management, and Incident Response. Representatives from these areas can also help provide key data related to threats, vulnerabilities, etc. during the information risk assessment session.

Marketing Information Risk Management ('During Snapshot' pt. II)

Like any immature initiative, it is imperative to receive top layer management consent in order to clear the hurdles intrinsic to creating an effective IRM program. It may seem IRM would sell itself in terms of its basic benefit of being a means for organizations to exhibit 'due care' in managing risk surrounding their assets. But surprisingly, the challenge of marketing IRM and convincing management to provide adequate resources for information risk management was not simple. With the proper 'marketing', the IRM team needs to ensure management is aware how IRM can help to ensure compliance, reduce litigation exposure, and support internal and industry security standards. This section enumerates the various benefits IRM can provide an organization. The primary benefits we focused on within our company were corporate governance, regulatory/legislative compliance, and decision support but this likely would vary upon individual organizations.

IRM responsibilities derive from laws, industry regulations, market sector requirements and industry 'good' practices. The message of why to do IRM should also include information about the regulations and drivers that most concern your organization and how information risk management will help your organization be compliant. Examples include Sarbanes Oxley to HIPAA to government/military-specific requirements such as National Security Directives. Below we take a look at some of the more common and prominent external and internal business drivers that relate to IRM.

Corporate Governance

[4]*Corporate Governance looks at the institutional and policy framework for corporations—from a company's very beginning through its governance structures, company law, privatization, market exit and insolvency. The integrity of corporations, financial institutions and markets is particularly central to the health and stability of our economies.* An effective information risk management program is central to corporate governance. Information Risk Assessments that are done through a formal methodology and based on industry standards demonstrate 'due care' from a corporate regulatory standpoint.

Sarbanes Oxley

[5]*Sarbanes Oxley (SOX) is the government's answer to recent corporate scandals. It holds company executives personally accountable for the accuracy of their*

[4] Organizations for Economic Development, http://www.oecd.org/topic/0,2686,en_2649_37439_1_1_1_1_37439,00.html

[5] Inspired eLearning Inc. 2003-2005; www.inspiredlearning.com/sat/standards.SOX.htm

© SANS Institute 2000 - 2005, Author retains full rights.

organization's financial statements and includes criminal penalties for false certification. Since top management must sign off on financial reports, the law also mandates adequate 'internal controls' that ensure reliable financial reporting. This is where IT security and effective information risk management are needed to ensure compliance with SOX.

HIPAA

HIPAA standards require ([6]*sections 164.306-164.308*) Security Management Process, Risk Analysis and Risk Management:

- *Security Management: Implement policies and procedures to prevent, detect, contain and correct security violations.*
- *Risk Analysis: Conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information.*
- *Risk Management: Implement security measures sufficient to reduce risks and vulnerabilities to reasonable and appropriate level.*

California Legislation SB 1386 and AB 1950

This recent legislation requires an organization that possesses personal information of a California resident to disclose any breach of security related to that information. There is [7]speculation that all U.S. state governments are seeking similar legislations so this requirement will likely become much more extensive.

Industry/External Standards

Industry best practices should be followed in order to reduce risk. ISO 7799 is an internationally recognized code of practice offering guidelines for information security management. ISO was developed by a range of volunteer security professionals, overseen by a committee of government and commercial representatives. Many organizations use the ISO as a framework for developing their own internal information security standards. Other industry standards available in the public domain include Cobit, BS 7799, and the ISF's *Standard of Good Practice for Information Security*. Industry standards should be used as a barometer for your information risk assessment methodology. They are also an underlying influence to security metrics reporting and industry benchmarking.

Security Management

Security Management (SM) refers to the overall, day-to-day security arrangements at the enterprise level (Security Policy, Business Continuity Planning, Antivirus, Intrusion Detection, Information Security Awareness, etc.). [8]*Keeping the business risks*

[6] Federal Register Part II: "Department of Health and Human Services, Health Insurance Reform: Final Rule"; pgs 8376-8377

[7] As stated on NBC Nightly News report on Identity Theft that aired 2/15/05

[8] Information Security Forum, *Information Risk Reference Guide; December 2004*

© SANS Institute 2000 - 2005, Author retains full rights.

associated with information systems under control within an enterprise requires clear direction and commitment from the top, allocation of adequate resources, effective arrangements for promoting good information security practice throughout the enterprise, and the establishment of a secure environment.

Internal Standards:

Along with Information Risk Management, Information security policy is the backbone of any information security program. It helps protect the interests of your organization, its employees, business associates, sales force and business partners. Security Policy does this by setting standards on how to protect information from unauthorized use, modification, disclosure or destruction. Compliance with these internal standards is one way to measure risk when carrying out a risk assessment because your company's internal policies should be a major consideration.

Additional Benefits and Reasons to Do IRM:

Information Risk Management is not done solely to address external business and legislative drivers. Effective IRM also produces the following internal [9]benefits:

1. **Threat, Vulnerability, and Business Impact Identification:** Ensures the greatest risks to business operations are identified and addressed on a continuous basis.
2. **Decision Support:** IRM provides decision makers (i.e. management and leadership) with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk. The next subsection focuses heavily on how IRM directly ties to decision support.
3. **Justification of Expenditures:** Risk assessment enables the identification of areas that may need security improvement, which could help justify expenditures for information security improvements.
4. **Increased Awareness:** Increases understanding of risks throughout the organization by helping personnel better understand risk and avoid risky practices, such as disclosing passwords or other sensitive information.
5. **Improved Internal Controls:** IRM provides a mechanism for reaching consensus on controls necessary to reduce risk. The facilitated nature of risk assessments help business partners understand the need for agreed-upon controls, feel the controls align with business goals, and support the effective implementation of controls.
6. **Means for communicating results:** Standard risk assessment report formats, and the periodic nature of risk assessments, provide leadership with a means of readily understanding reported information and comparing results over time.

IRM and Decision Support

[9] According to Shelly Baird's 2004 MIS World Conference presentation, "Root canal and Risk Assessment are not Synonymous"

© SANS Institute 2000 - 2005 Author retains full rights.

The IRM model below depicts the conceptual relationship between information risk management and decision support. This model was developed internally to help information security staff and management understand the correlation between IRM's various aspects and decision making. The lowest layer represents the business drivers and requirements for doing IRM. The next layer up contains the various elements that comprise an information risk assessment. Once analysis is done on the risk assessment output, results are reported in the form of control recommendations, internal metrics, and in some cases, industry benchmarking results. These reporting mechanisms are then used as input to help management with their decision-making. We tried to convey how all IRM activities ultimately channel into decision support. Details about each aspect of the diagram are provided later in this section.

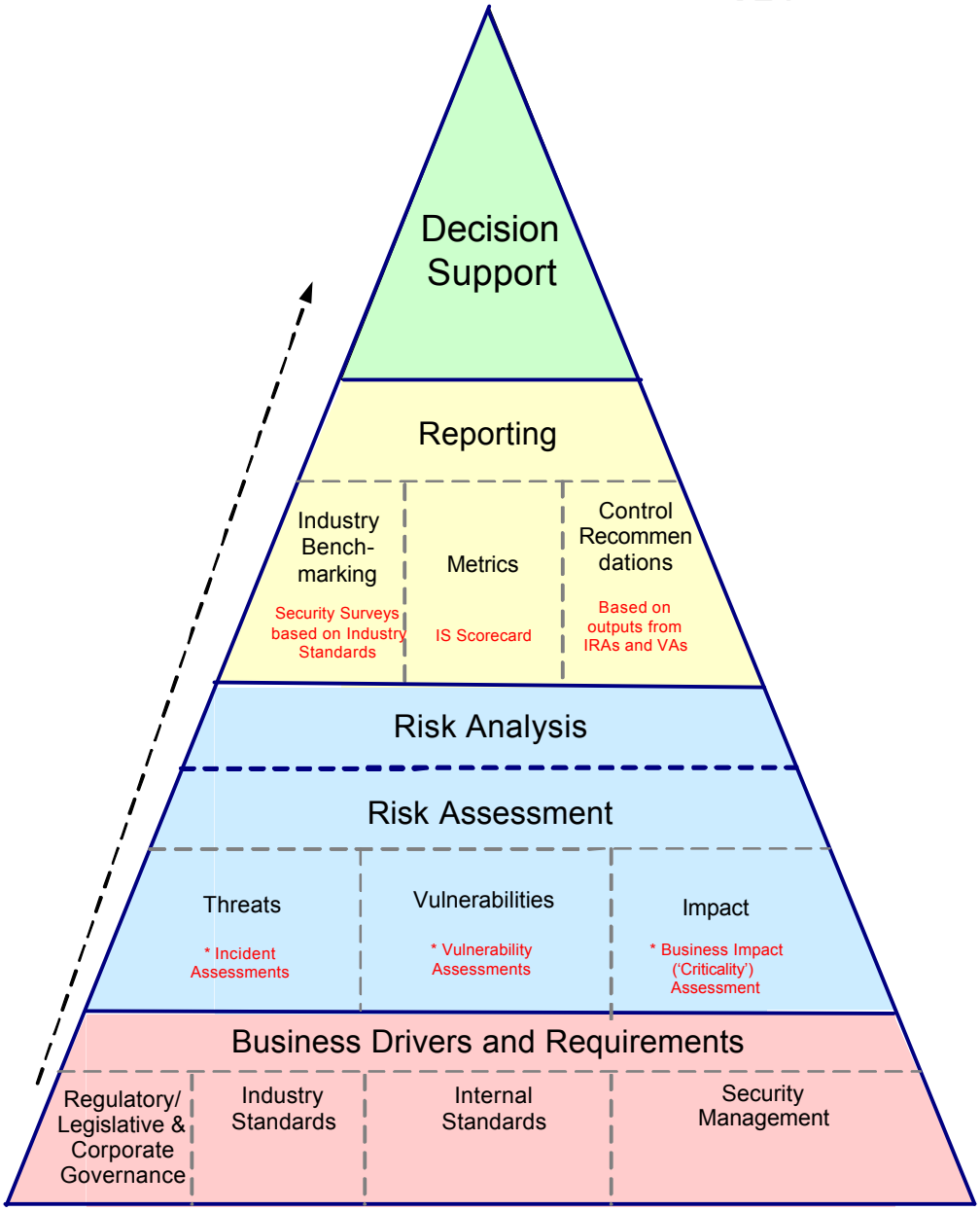

Figure 1 - IRM Decision Support

Let's take a closer look at each aspect of the IRM Decision Support Model by linking IRM tools, processes and methodologies to each aspect of Figure 1.

© SANS Institute 2000 - 2005, Author retains full rights.

Decision Support

Risk assessments are a means of providing decision makers with information needed to make informed judgments concerning the extent of actions needed to reduce risk. IRM output, including risk assessment results, can assist numerous types of decision makers. The type and nature of decisions varies but decision makers supported by IRM can range from project managers and stewards to top executive-level management (and all decision makers in between, including business partners who may have requested an IRA). As a final emphasis, one fundamental purpose of IRM is to help management and leadership with decision support and to understand where to best spend its information security dollars.

Risk Assessment Process & Methodology ('During Snapshot' pt. III)

The process we implemented for carrying out an information risk assessment in our organization is as follows:

- **Prepare for Information Risk Assessment:** IRM team analyzes IRA request and assigns team member(s) to work with requestor(s). The requestor is typically a member of the information security staff. Prior to IRA facilitated session, IRM team holds initial meeting with requestor(s) to establish scope of assessment, identify attendees/subject matter experts, and determine timeline for completing risk assessment. IRA facilitated session is scheduled once this preliminary information is gathered.
- **Business Impact/Criticality Assessment (BIA):** Identify how critical the information resource being assessed is to your organization what would be the business impact of a worse-case scenario where confidentiality, integrity or availability of information was compromised.
- **Threats, Vulnerability, and Control Assessment (TVCA):** Analyze and capture threats and vulnerabilities related to information resource being assessed. Document potential controls that could address those threats and vulnerabilities. A facilitated session with representation from business owners, IT operations, and other appropriate stakeholders is an ideal format. Facilitatation should be provided by the IRM Team as an ongoing service to the organization. We find two facilitators to be most effective—one IRM team member to lead the discussion and another to document answers and 'comments' that provide context as to why certain answers/responses were given.
- **Control Recommendations/Action Plan:** Analyze IRA results and deliver recommended action plan to business owners and management. A combination of multiple control recommendations comprise what we can an 'action plan'. Each control recommendation should directly address a weakness identified in the risk assessment.
- **Decision Support:** Management/Owner(s) utilize information risk assessment reports and action plans to make decisions on security controls.

© SANS Institute 2000 - 2005 Author retains full rights.

- **Monitoring/Reporting:** Once decisions are made on recommended controls, IRM Team stores IRA results in central repository and works with initial IRA requestor to ensure action plan is updated on ongoing basis. In some cases re-assessment may be necessary to determine if the risk posture of an information resource has changed. This is because risks and threats change over time so it is important to periodically re-assess and reconsider the appropriateness and effectiveness of the policies and controls that have been selected. Additionally, the completion of an action plan from a previous IRA may show a reduced level of risk associated with an information resource upon re-assessment.

The high level workflow of the IRA process is mapped in Figure 2 below.

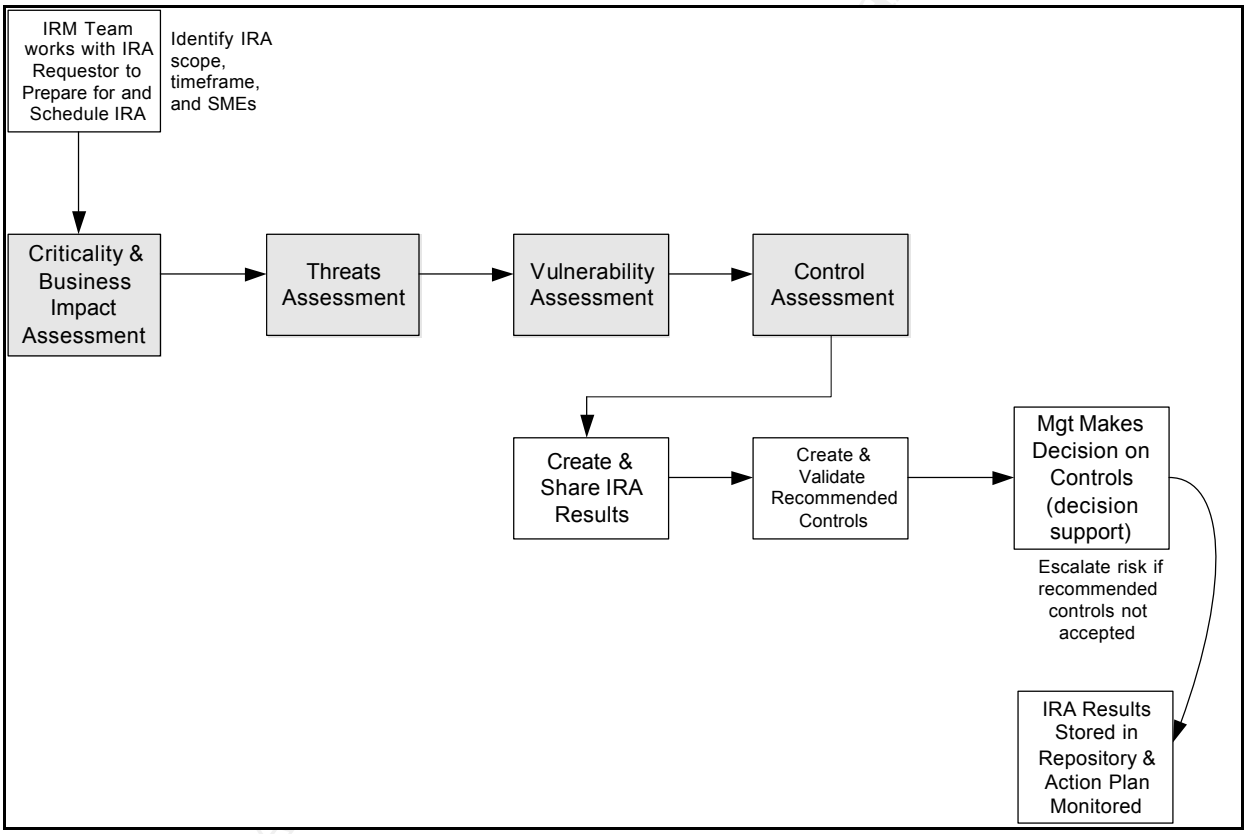

Figure 2 - IRA Process Flow

Note:

- Boxes shaded in Gray are the sub-processes that encompass a full Information Risk Assessment.

Information Risk Assessment Methodology

The formula we use to assess information risk is as follows:

Threats + Vulnerabilities + Business Impact = Information Risk (T + V + I = Risk)

The SANS official position is that known threats and vulnerabilities can be multiplied in order to measure risk within an organization. Although this is a good starting point, there is no recognition of *business impact* or how critical the information resource being assessed is to the wellbeing of the enterprise. With that in mind, we felt a more accurate formula for measuring information risk is to include business impact and criticality, in addition to threats and vulnerabilities, in order to see the whole risk picture. Threat and vulnerability only give us probability of something going wrong. It is important to combine the business context (i.e. impact of an incident or potential incidents) to the threats and vulnerabilities variables in order to quantify the risk. The methodology we implemented is built to capture this basic formula.

A sound methodology, whether developed or purchased, should also incorporate both qualitative and quantitative tactics, which are necessary to comprehensively assess risk. Qualitative means a combination of expertise or opinion based on knowledge of a resource to assess the probability and level of risk associated with it. [10]*"Qualitative [risk assessment] is easier to calculate and accomplish, and it succeeds at identifying high risk areas; however, its results are relatively subjective"*. The Quantitative approach uses numerical values to assess risk in each variable of the risk formula. This method assigns empirical values to the threat, vulnerability, probability, and criticality/business impact variables. Automated risk assessment tools are beneficial for this approach and recommended if complex statistical/probability calculations are needed. [11]*"Quantitative [risk assessment] is far more valuable as a business decision tool since it works in metrics, usually dollars"*. We have found that quantitative results in the form of charts and tables extracted from IRA results typically grasp management's attention the most.

IRA Methodology in Action:

The section above looks at the overall information risk assessment (IRA) process from beginning to end. This next section takes a closer look at steps taken in the IRA itself. Depending on your methodology, sessions can typically last two to four hours. A facilitated session with proper representation from subject matter experts and business owners is highly recommended.

We already discussed that a comprehensive information risk assessment requires consideration of all factors in the risk equation (i.e. threats, vulnerabilities, criticality, and business impact). Let's take a closer look at each of these [12]aspects.

1. Threat Assessment

[10] As stated in SANS Institute Volume 1.3, chapter 18; *Internet Security Technologies*

[11] As stated in SANS Institute Volume 1.3, chapter 18; *Internet Security Technologies*

[12] Italicized text on pgs. 14-16 indicate definitions or supporting text leveraged from the Information Security Forum's *Fundamental Information Risk Management; March 2000*.

© SANS Institute 2000 - 2005 Author retains full rights.

An organization that is relatively large in scale may be exposed to an increased amount of threats due to a commensurately large network, system complexity, or sheer volume of data that requires protection. "*A threat is a possible event that could compromise the confidentiality, integrity or availability of information associated with a system"*. Threats are difficult to quantify but can be best understood by looking at historical incident data. Threats exist in a wide variety, including external attacks, internal misuse and human error, software or hardware malfunctions, outages/loss of services, access violations, etc.

Some threats have a higher probability of occurring while others are likely to cause substantial harm if introduced to the environment. A realistic assessment of these threats allows priority to be given to the most critical threats. Our IRA methodology includes the evaluation of incidents in the above threat categories that have manifested into incidents in the past year. The best way to answer 'what could happen?' is by knowing what already has happened. The 'real life' business impact that stemmed from those incidents should also be quantified.

Systems, applications, and other information resources that suffer incidents over a given period of time are likely to suffer a similar number in the future unless remedial action is taken. The greater number of incidents experienced in the past, the greater the likelihood of major incidents occurring in the future.

2. **Vulnerability Assessment**

Vulnerabilities are circumstances that increase the likelihood of threats materializing. Some vulnerabilities can lead to significant on information risk so it is important to identify which vulnerabilities apply to the environment being assessed.

A risk assessment should look at control weaknesses in a variety of different 'control domains'. Industry research shows most incidents that cause organizations serious harm can be traced to weaknesses within some of these areas: Security Policy, Risk Identification, Security Awareness, User/System Supporter Skills, Access to Information (Authentication/Authorization), System Configuration, Special Security Controls (e.g. antivirus, encryption, intrusion detection, incident response), and Physical Security. There are other domains of control and their relevancy varies from organization to organization. Beyond the traditional security realms, Service Management processes like Change Management, Service Level Objectives (including contracts with outside parties), and Business Continuity should also be included in the vulnerabilities assessment portion of an IRA. The more weaknesses that exist within these areas, the higher chance an incident will occur. The vulnerability assessment portion of an information risk assessment should capture known strengths and weaknesses within these areas. For each documented weakness a corresponding task (i.e. 'action item') should be documented to fix or mitigate the vulnerabilities uncovered in the IRA.

Other special considerations may also increase risk, such whether or not the resource being assessed is connected to by a third party, immature or new,

© SANS Institute 2000 - 2005, Author retains full rights.

geographically dispersed, etc.

3. **Criticality and Business Impact Assessment**

   Criticality Assessments help measure business impact by determining the maximum level of harm the business could suffer if the confidentiality, integrity, or availability of key information is compromised. The criticality rating essentially indicates how valuable an information resource is to the enterprise. The way we determine criticality is to rate what the maximum level of harm the business could suffer if key information within the scope of the information resource being assessed were accidentally or deliberately:

   - Revealed or exposed to the wrong people – *loss of confidentiality*
   - Falsified or incorrectly altered – *loss of integrity*
   - Rendered unavailable (for a variety of time periods) – *loss of availability*

   Discussions in a criticality assessment should focus on a worst-case scenario that is within reason. *The higher the criticality rating, the greater the value at risk and thus the greater a need for protection*.

4. **Business Impact Assessment**

   The business impact of past incidents is an important indicator of information risk since it enables risk to be discussed in business terms. [13]Key categories of business impact include *loss of competitive advantage, incorrect management decisions, damaged reputation or customer dissatisfaction, regulatory/legislative breaches, and direct loss or delay of business*. By looking at the actual damage caused by incidents that occurred in your organization over the previous year (as identified in the threats assessment), you can better understand the impact that future incidents would have if vulnerabilities are not addressed to prevent those incidents from occurring.

   An agreed-upon set of measurements is necessary to consistently gauge business impact. This can be in the form of a table, matrix or some other 'dashboard' format. The parameters for business impact should minimally range from low to medium to high impact, with corresponding figures for common forms of business impact/harm (i.e. dollar amounts for financial loss, number of lost person-hours for degraded performance, scale of exposure for damaged reputation, and so on). Ideally, the figures should be tailored to your organization. However, in the early stages it may be a challenge to obtain these levels of impact from top management, so at the very least industry standard figures could be used. Trending reports, financial reports and other historical data can be used to help tailor these thresholds.

5. **Control Recommendations**

   Control recommendations result from the analysis done after risk assessments are completed. [14]These recommendations could come in the form of action plans,

[13] According to the ISF's *Information Risk Reference Guide; December 2004*

formal recommendation reports, or tool-generated reports. Control recommendations are submitted to leadership to assist with decision making. They should include a description of the control recommendation, which individual or area will own the task and ensure its completion, a target date for completing the recommended task, and what is its current status (i.e. not started, in progress, completed). Control recommendations should be based on information risk requirements that result from a risk assessment. For example, a requirement uncovered in an IRA may be 'the ability to encrypt data in transit and at rest (for an application hosted at a third party site)'. Possible control recommendations to address these requirements could be as follows:

- SSL encryption should be considered for HTTP traffic in transit (between your company and the third party).
- Windows Encrypting File System (EFS) with 120-bit DESX encryption should be considered for file level encryption.

6. Information Risk Escalation

Changes within the organization that introduce or increase risk to the enterprise or business areas (e.g. updating critical business applications with single sign-on passwords or some other change that increases risk) should be implemented with appropriate security controls to eliminate or mitigate the exposures. Sometimes an issue will result from a risk assessment that requires escalation. Decisions on how to address information risk is made by appropriate levels of management and should be documented in a formal, consistent manner (e.g. electronic form). An 'Information Risk Escalation' process (with accompanying procedures) should be developed to outline the steps necessary to escalate an information security issue from Security staff to management and decision makers for Risk Acceptance, Risk Transference, or Risk Mitigation/Resolution. The process you develop will depend on which layer of management can accept risk. This will typically be top management, such as an executive review board.

This was another enterprise-wide gap that existed in our company and management challenged the IRM team to address it. At the time, risk escalation was done through ad hoc means where security analysts could informally raise an issue without proper information (i.e. no supporting information risk assessment done). Furthermore, they were raised to decision makers inconsistently because there were no defined paths of escalation. This created a potential for information risk decisions to be made without proper exposure and agreement from key decision makers. The template used to document and escalate information risks should include at least a description of the issue/information risk, threats and vulnerabilities associated with risk, business impact, compensating controls, action plan identified/recommendation, and any other additional comments. An accompanying process should also clearly define an escalation path appropriate to your organization. It is also recommended that risk escalation not be permitted unless a formal information risk assessment is completed.

[14] SANS Institute refers to this step in the risk assessment process as 'Safeguard Selection' (Vol. 1.3, ch. 18, *Internet Security Technologies*).

© SANS Institute 2000 - 2005

Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

Other IRM Reporting ('During Snapshot' pt. IV)

Security Metrics

Quantifiable metrics can be attached to business or security goals with the help of a consolidated, 'quick reference' report that gauges various elements of information security.

[15]*In settings that require balancing the cost of countermeasures against the cost of risk, decision support is precisely the point of any measurement exercise. Getting the right measurements depends on knowing the right questions. In medicine, a doctor asks "what is the patient's malady?" In information security, leadership asks:*

- *How secure am I?*
- *Am I better off than I was a year ago?*
- *How do I compare with my industry peers?*
- *Am I spending the right amount of money?*
- *What are my risk transfer options?*

There are literally hundreds of different types of metrics that can be gathered. Metrics capture how often something happens, how long an event lasts for, how much an event costs, etc. Metrics are essentially a 'pile of data' that can be reviewed to make a variety of decisions, including where resource and spending should be increased or decreased based on set targets being exceeded or not met. Metrics are typically presented in question form (e.g. how many virus-infected emails are not blocked? What percentage of email traffic is SPAM? What percentage of security staff has received certification?). Management should be involved with the development of security metrics tools. We held a series of facilitated sessions with various levels of management to gather their requirements for what the metrics should consist of, how often they should be reported, how the metrics tool should be formatted, etc.

Industry Benchmarking

Our leadership sought a way to compare our overall information security arrangements with our industry peers. Industry benchmarking provides a means to compare your organization's internal security arrangements with those of your industry peers. A peripheral benefit of industry benchmarking is it enables a company to initiate its own internal improvement programs (i.e. work efforts) based on their results. In other words, if an organization rated poorly when compared to industry peers for Information Security Awareness (ISA), then it may consider bolstering your ISA campaigns. Conversely, if it rated much better than other companies for a given security topic then perhaps that organization is over-spending in that category. There are numerous types of 'Industry Benchmarking' tools and surveys available for purchase or through member-based organizations. By measuring our performance against industry security standards, we were able to gain an overall picture of our security posture, measure the effectiveness and maturity levels of our information security arrangements, and

[15] IEEE Security and Privacy web site; July/August 2003: http://computer.org/security/

© SANS Institute 2000 - 2005 Author retains full rights.

compare those results with industry peers.

IRM Process, Procedures and Training ('During Snapshot' pt. V)

One of the IRM Team's primary services is to steward the processes, tools and methodologies that help security staff and business partners conduct information risk assessments. A formal process with supporting procedures is necessary to achieve this objective and ensure information security staff understands the services you provide.
One of the most important efforts our team undertook in the past year was a complete process overhaul. The focus of our new process model was on information risk assessment because that is the primary service our team offers the organization. We have already discussed how our previous risk assessment method was tedious, vague and difficult for information security staff to comprehend. In addition, it was not consistently applied and did not properly facilitate communication between the technical and business sides of our organization (i.e. did not speak a common business language). Finally, information security staff struggled with how to engage the IRA process, where to store their completed risk assessment, and how to escalate risks and control recommendations that resulted from the completed IRAs.

All these factors prescribed a need for our team to formally define, document, and communicate a set of processes and procedures related to all aspects of carrying out an information risk assessment (from beginning to end). The process model we developed is comprised of the following phases with detailed procedures to accompany each step in the sequence:

- **Request IRM Services:** Describes how information security staff and others should engage the IRM team to request an information risk assessment or some other service, such as consulting or industry benchmarking data).
- **Analyze Request for IRM Services:** Describes how the IRM team goes about examining a new IRM service request, determining risk assessment needs, and assigning a team member to work with the requestor.
- **Prepare for Information Risk Assessment:** Involves IRM team members meeting with requestor to agree on scope of risk assessment, participants/SMEs, timeline for completing IRA, and scheduling or IRA overview and facilitated session. The IRA 'overview' is a one-hour presentation given to all IRA participants about a week prior to the facilitation session in order to establish a level set and mutual understanding among all attendees regarding the IRA methodology. Additionally, the IRA requestor should research known threats, vulnerabilities, weaknesses, etc. relative to the information resource being assessed during the preparation stage. This helps ensure the IRA facilitated session runs smoothly because key information will already be captured going into the risk assessment.
- **Participate in Information Risk Assessment:** Includes details about the activity involved in the actual information risk assessment facilitated session, such as

criticality, business impact, threats, and vulnerabilities assessments.

- **Create and Share Information Risk Assessment Results/Outputs:** Outlines the steps necessary to compile all the information gathered in a risk assessment and generate a final report. At this stage, risk requirements gathered in the IRA can be used to drive out security control recommendations. The final reports are then published in a secured, central repository and shared with management or other appropriate decision makers.
- **Create and Validate Control Recommendations:** Upon creation and sharing of final risk assessment results, the IRA requestor (typically a member of the information security staff) identifies control recommendations based on the action plan output from the IRA. Those recommended controls should also be analyzed and validated with subject matter experts in appropriate business/support areas. The control recommendations are then submitted to decision makers who either accept or reject the recommendations based on the IRA results and other relevant data in the final report.
- **Escalate Unaccepted Control Recommendations:** Outlines the steps necessary to escalate an information security issue from the IRA requestor to the proper level management for a decision to resolve or further escalate that information risk-related issue for acceptance. This process also applies to control weaknesses detected as the result of an internal or external assessment (e.g. Audit, Vulnerability Assessment, etc.).
- **Store Information Risk Assessment results in secured, central repository:** Once risk assessments are completed and control recommendations are documented, it is necessary to store the information in a common repository in order to easily access, monitor, and maintain IRA documentation (e.g. action plans, final results reports). Access to this documentation should be secured so only the IRM team and those directly involved with the risk assessment can view the information.

Once your process and procedures are developed and documented, the next step is to communicate them to information security staff and management. This can be done in a variety of ways depending on your organization's culture. Our approach was to first hold a series of brief presentations in which we highlighted enhancements to our process, why the process was changed, and how it will benefit information security staff. Once the process overviews were completed, we developed a training workshop that further explained the information risk assessment process and methodology to the same audience. These workshops typically last two to three hours and cover in depth each of the above bullet points. The number of workshops you administer will depend on the size of your organization's information security staff.

© SANS Institute 2000 - 2005 Author retains full rights.

IRM Strategy ('During Snapshot' pt. VI)

A clear, focused strategy is another important component to establishing an information risk management program. The strategy we developed states what our IRM capabilities are today and what capabilities we envision in the short term and long term future. It includes tangible, actionable, and tactical measures planned in order to achieve an optimized level of maturity. In other words, the purpose of the strategy is to describe the IRM team's strategy for achieving its objectives and to detail the necessary steps to continue information risk management's evolution within the enterprise.

Once you identify your short and long-term IRM strategy, it should be documented and communicated to management and staff. The IRM Strategy should essentially be a roadmap of timelines and key milestones to reach in order to full maturity. A key to understanding strategic needs is to compare current practices against a model of good practices (i.e. an 'ideal state' of maturity). Once the gap between current practices and ideal state is identified we can begin to define improvements. This section focuses on capturing those areas of improvement while listing the necessary activities needed for the IRM component to continue its maturity.

IRM Maturity Model

The purpose of the [16]maturity model below is to establish rankings for information risk management progress at your company, which can then be applied as:

- A method for self-assessment to determine the organization's status
- A method for using the results of the self-assessment to set targets
- Future development, based on where your organization wants to be on the maturity scale
- A method for analyzing gaps between those targets and the present status
- A method for prioritizing IRM work based on beneficial impact against its cost

By matching both past and future IRM milestones to each appropriate phase description you can better understand and articulate your organization's level of IRM maturity.

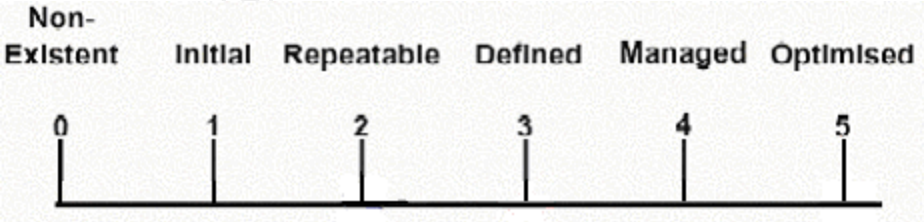

Figure 3 - IT Governance Maturity Model

[16] The maturity model was based on principles behind the IT Governance Institution's *"How to measure your enterprise's maturity level relative to information security governance".*

Our team's immediate focus was on the short-term objectives necessary to elevate our component from a stage 1 (Initial) of the maturity model we adopted. After about one year we reached the Repeatable stage and by year two we are at a Defined stage, but have yet to advance to a 'Managed' or 'Optimized' maturity level. The illustration below gives an example of how IRM maturity could be portrayed.

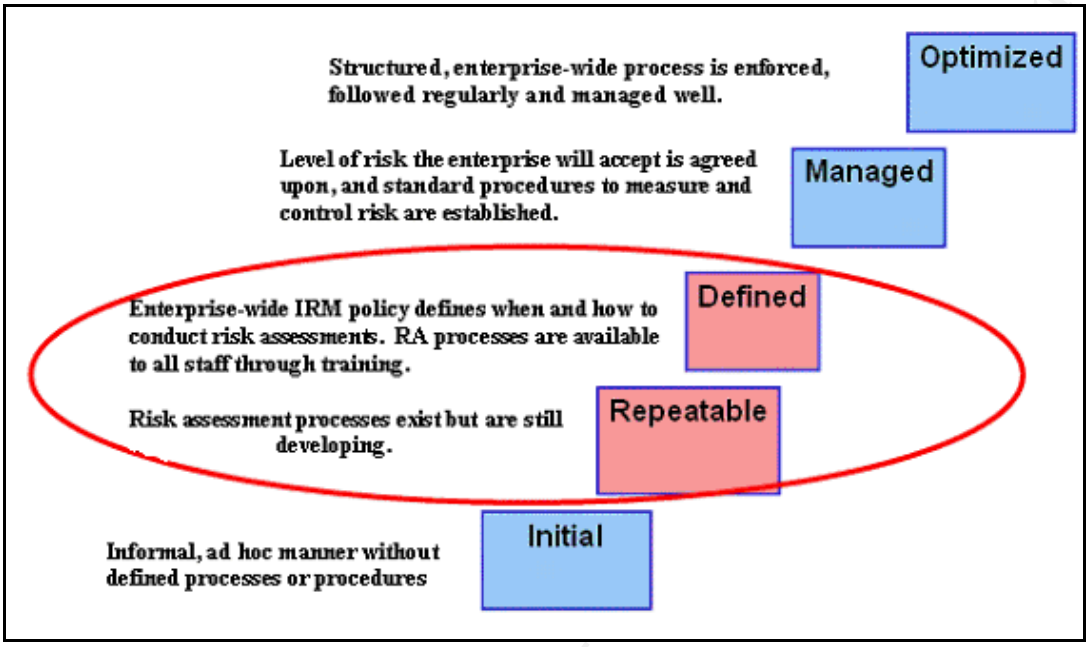

Figure 4 - Portraying IRM Maturity

Reaching Full IRM Maturity

The remainder of this section addresses some of the IRM work efforts and milestones associated with each stage above. It is estimated to take one to three years to advance each stage of maturity, but it depends on factors such as size of your organization, level of management support, and adequacy of dedicated IRM staffing.

Initial Stage: ("Informal, ad hoc manner of handling IRM without defined processes or procedures")

Our organization could be best categorized as being in the 'Initial' stage of maturity less than two years ago. Commitment and support from top management, increased staffing, and a variety of other collaborative efforts (most already discussed in this document) have allowed us to advance to a 'Defined' stage. This is a fairly rapid pace of evolution considering it is probably common for organizations to take two or more years to mature from one stage to the next.

- Establish initial team to focus on Information Risk Management activities.
- Identified and selected industry Information Risk Management tools
- Introduced and piloted IRM processes and tools

© SANS Institute 2000 - 2005

Author retains full rights.

Repeatable Stage: ("Risk Assessment processes exist but are still immature and developing")

This stage is mostly developmental with processes and training being created and documented, procedures being written, and other existing information risk assessment efforts being refined.

- Initiate 'process modeling' to formally document your IRM processes, procedures and training.
- Introduce an effective, consistent, and repeatable method to assess information risk based on threats, vulnerabilities, criticality to the organization, and business impact that would result from a loss of C, I, or A. Both automated and manual processes are available for purchase or can be developed internally.
- Develop method to communicate information security posture to senior management (through metrics reporting, industry benchmarking, other forms of control recommendations).

Defined Stage: ("Enterprise-wide IRM Policy defines when and how to conduct risk assessments; RA processes available to security staff via training")

This stage is where your IRM services are defined, documented and communicated to staff. Your team should move more from a developmental phase to a support and maintenance phase.

- IRM Processes and Procedures Published in Central Repository
- IRM Facilitation Services and Risk Escalation Process Available
- IRM Processes Linked to Security Requirements Gathering and Project Methodology
- Information Risk Assessments Documented in Central Repository
- IRM Training Available to Staff on Consistent Basis

Managed Stage: "Level of risk the enterprise will accept is agreed upon, and standard procedures to measure and control risk are established":

Our organization is currently in the 'defined stage' and it could take 1-3 more years to advance to the 'managed' stage.

- Management consistently uses risk assessment output to make decisions
- Acceptable level of risk established by business stakeholders
- Risk assessment baselines are monitored, updated, and stored in central repository
- IRM processes and services communicated and understood organization-wide

Optimized Stage: "Structured, enterprise-wide process is enforced, followed regularly, and managed well":

- Information Risk Management processes are tightly integrated with Systems Key

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Processes and other operational risk activity (e.g. Internal Audit)
- Systems and Business Partners actively drive and participate in IRM activities
- Risk Assessment outputs are being used for strategic decision making (e.g. policy, business goals, etc.)
- IRM processes are influencing industry best practices

Conclusion ('After Snapshot')

Implementing and supporting a defined information risk management program is complicated and time-consuming. It's complexity stems from not being similar to traditional efforts that can be time-boxed, planned for every step of the way, and measured for success with tangible finish dates and completed objectives. In many ways the evolution can be fluid where fluctuations occur between rapid development and periods of stagnation. However, the good news is that like any significant effort a relatively small team can accomplish the task with strong support from management and stakeholders, a clear strategy, and well defined processes, procedures and methodologies.

The primary improvements we focused on included a formalized business focus with management buy-in; implementation of a mature, consistent risk assessment method; addition of IRA facilitation as an IRM Team service provided to the enterprise; diversification of IRA reporting through benchmarking and security metrics; and development and communication of formal IRM processes and procedures.

Devising and administering a sound IRM process requires commitment, credibility, know how, and resources. Additionally, IRM implementation is a form of organizational change; therefore, organizational change principles such as continued involvement from multiple organizational levels and stakeholders, marketing of benefits to top management, and ongoing communication to business partners and staff are all keys to implementation.

After Snapshot:

Although our IRM team has recently made substantial progress, many challenges still must be overcome as we look to the future. Specific areas we plan to address in the next one to two years include the following:

- Increased ability to assess infrastructural components. Our current IRA methodology is ideal for business applications, data centers, system development activity, and arrangements with third parties; however, it is still difficult to pinpoint a scope when assessing pieces of the infrastructure. This is due to complexity and interdependencies within the environment. We continue to explore easier ways to assess the infrastructure.
- Top management defines acceptable levels of risk. We are currently doing information risk assessments that are based on equal parts industry standards

© SANS Institute 2000 - 2005 Author retains full rights.

and internal executive input. This is effective in gaining a breadth of baseline data but we could more effectively assess risk profiles if it we could compare levels of risk that result from an IRA to acceptable levels of risk defined by the enterprise.

- Increased understanding and awareness of IRA processes and benefits among business partners, to the point they actively engage and participate in IRM activities. Information Risk Management is a new area of risk management that will probably not be well understood by all stakeholders in the early stages.
- Management consistently uses IRM output to make strategic decisions. Outputs include IRA results reports, action plans, industry benchmarking reports, and security metrics.
- Information Risk Assessment results 'baselined'. This basically means we have finished enough risk assessments and can simply refer to our IRA repository to obtain risk data from previous IRAs already completed, rather than duplicate work by re-assessing an information resource.
- Information Security Staff consistently uses IRA output to drive out information risk requirements that can be fed to development activities.

Looking forward, we are on our way to meeting most of these challenges but it is a gradual progression that could take up to two or three years. The best way to reach these objectives is to complete as many risk assessments and other forms of IRM reporting as our team can sustain. This will bolster the enterprise's awareness of our services and how it can benefit from those services. If we continue to provide management with quality information to help them make decisions then we should inevitably reach an optimized IRM state.

© SANS Institute 2000 - 2005 Author retains full rights.

Bibliography

1. Information Security Forum, Improving Security Management: Enterprise-wide. The Information Security Forum. June 2004. URL: www.securityforum.org.
2. SANS Institute, SANS Security Essentials: Risk Management and Auditing. Volume 1, Section 3, chapter 18.
3. Benchmarking, BambooWeb Dictionary. "Benchmarking". URL: www.bambooweb.com/articles/b/e/Benchmarking.htmll
4. Organizations for Economic Cooperation and Development (OECD), "Corporate Governance" URL: http://www.oecd.org/topic/0,2686,en_2649_37439_1_1_1_1_37439,00.html
5. Inspired eLearning Inc. "Sarbanes Oxley". 2003-2005; URL: www.inspiredlearning.com/sat/standards.SOX.htm
6. Federal Register Part II: Department of Health and Human Services, Health Insurance Reform: Final Rule; Vol. 68, No. 34; February 20, 2003

   http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-3877.pdf
7. Information Security Forum. The Information Risk Reference Guide. London, UK. December 2004. URL: www.securityforum.org
8. IEEE Security and Privacy. July/August 2003. URL: http://computer.org/security/
9. IT Governance Institute (ITGI). *"Information Security Governance: Guidance for Board of Directors and Executive Management."* 2001.

***Note:** Other non-periodical/web site citations embedded within footnotes of document.

© SANS Institute 2000 - 2005, Author retains full rights.