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 (Security 401)"
at http://www.giac.org/registration/gsec

GIAC Security Essentials, version 1.4b

A Practical Information Risk Management Process Framework

By Dan Landess

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

A Practical Information Risk Management Process Framework

Abstract

As managing information risk becomes an increasingly important business concern, one of the challenges for organizations is to understand when and how to integrate Information Risk Management (IRM) measures into the organization. This paper seeks to expand upon IRM thinking by presenting a practical Information Risk Management Process Framework (IRMPF). An IRMPF offers a focal point to gauge if and to what extent appropriate risk management activities are being conducted in an organization. The framework proposed in this paper is meant to be a practical, conceptual view of the numerous levels of activity that work together to affect the management of information risk. Therefore, the focus of this paper is on the 'what' and not necessarily the 'how' of IRM.

This paper combines industry standards and best practices associated to information security, risk management, IT service management and business process management to generate an IRMPF. Once information risk is defined, an IRM process model is identified and expanded to include an objective and definitions of its component parts. This IRM model is combined with business process architecture to represent an IRMPF. And finally examples of how the IRMPF can be used to assess, document and mature the IRM discipline.

Introduction

It is hard to imagine even the simplest company that is not dependent upon some form of technology to manage their information. Let alone imagine the degree of dependency large corporations place on technology to manage their information. Business as we know it cannot exist without information and the technology that delivers that information. It is this dependency on information and information technology that has raised the need to manage risk associated with information. When we factor in the consumer and regulatory drivers (i.e. GLBA, HIPAA, etc.) for managing information properly, information risk begins to reach into all layers of company governance. In fact when we consider that nearly every business process and activity is enabled by integrated information and shared information resources, it is very plausible to say that information risk intensifies all other areas of risk within a business.

While risk management as a discipline is relatively well understood for other types of risk, grasping something as ubiquitous as information and information technology risk is relatively new and somewhat daunting. The underlining premise of this paper is that an IRMPF is needed to effectively navigate the management of information risk. Furthermore, an IRMPF must encompass the depth and breadth of organizational impact that can result from information risk.

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

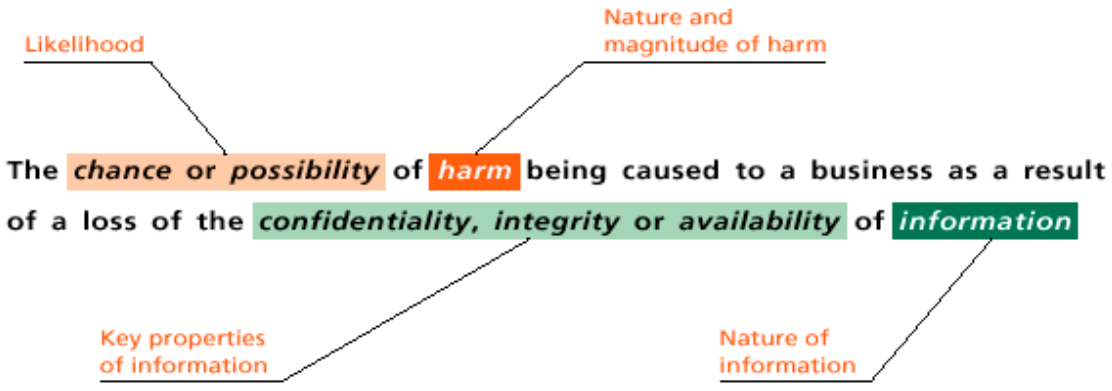
Defining Information Risk

In order to manage this new area of risk, a common definition of what information risk is must be adopted.

> "Risk, the possibility of damage or loss, is described mostly in dependencies of threat and vulnerability, or impact and probability." (Iheagwara, p.10).

Though most security professionals understand information risk, as a product of 'threats and vulnerabilities' that cause impact, capturing reliable metrics to quantify threats and vulnerabilities to information resources is very difficult. Even though threats and vulnerabilities must be considered to assess risk, they are ultimately used to determine impact and probability. Practically speaking, the 'impact and probability' descriptors are more workable in a pure definition of information risk. This leads to the question: impact and probability of what?

The long-standing (and still relevant) business requirement for information security is to maintain information's confidentiality, integrity and availability (National Research Council, p. 49)(ISO/IEC 17799, p, 1). This is also an underlying requirement in the Information Security Forum's Standard of Good Practice (SOGP), especially when risk and criticality standards are addressed. For example, many SOGP standards combine the word 'impact' with "loss of confidentiality, integrity, and availability." (SOGP sections referenced under 'Business Impact and 'Loss of' in the topic index). An excellent industry definition for information risk that combines the nature of risk (impact and probability) and the properties of information (confidentiality, integrity and availability) has been proposed by the Information Security Forum (ISF) and is shown in Figure 1. (Information Security Forum, p.4).



© Information Security Forum

Figure 1

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Defining Information Risk Management

Defining the 'management' of 'information risk' is rather straightforward. It is as simple as attaching the word 'information' to most quality industry definitions of risk management. For example; the Office of Government Commerce (OGC) definition for risk management can be adapted to read,

"Information Risk Management - the task of ensuring that the organization makes cost-effective use of an information risk process."

The OGC definition goes on to say, "Risk management requires: processes in place to monitor risk; access to reliable up-to-date information about risk; the right balance of control in place to deal with those risk; decision making processes supported by a framework of risk analysis and evaluation." (OGC, p. 36).

This industry best practice perspective on risk management becomes practical for IRM, especially if it can be described with an established risk process model comprised of common and repeatable processes.

The Risk Management Process Model

Using a generic process approach, a model can be developed to capture the essential processes needed to accomplish IRM. Numerous frameworks are available with varying perspectives and degrees of granularity on what activities comprise the actual risk management process flow. Having an open process framework that can speak to all the activities that are common among these various perspectives is recommended. For example, the diagram in Figure 2 represents the core components of a risk management process model based upon an Open Process Framework (OPF). (Firesmith, Risk Management).

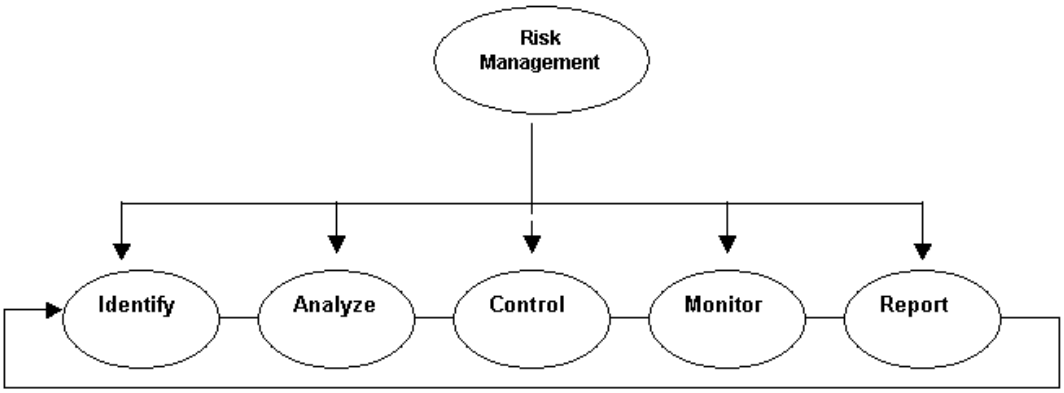


Figure 2

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Broadly written definitions for these process components can capture all the types of activities recommended in the various industry frameworks for managing information risk.

Definitions for IRM Process Components

Below is a set of proposed information risk definitions for each component of the risk process model. These definitions reflect a blend of the ideas and definitions in the SOGP, NIST and the OPF for risk management found at the following references respectively (SOGP 2003) (NIST Special Publication (SP 800-30) - July 01, 2002) (Firesmith, Risk Management).

- Identify - The identification of an event that may cause information risk.
- Analyze - The assessment, measurement and prioritization of threats and vulnerabilities to information for the purpose of selecting information security controls.
- Control **-** A policy, method, procedure or mechanism that addresses identified threats and vulnerabilities to information resources.
- Monitor - The process of systematically evaluating the organization by measuring the performance of information controls in order to initiate remedial action.
- Report - The process of systematically reporting to decision makers an accurate, comprehensive and coherent assessment of information risk.

The Objective of Information Risk Management Process

As the process model becomes more defined, a process-centric objective is also needed to better focus the IRM process. A good place to start is to consider the objective found within the Information Security Forum's (ISF) Standard of Good Practice (SOGP). The Security Management section (SM 3.3) addressing risk analysis, reads, "to 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 SOGP language is a good description of an overarching process objective for IRM. It identifies roles responsible for taking an action, and perhaps more importantly, it is left open to include decision makers at any level of an organization. Adapting this SOGP language and approach an IRM process objective can be stated as follows in Figure 3:

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The objective of the Information Risk Management process is to enable decision makers who are responsible for information and systems to understand key information risks and agree upon the controls required to keep those risks within acceptable limits.

Figure 3

Organizational Integration of Information Risk Management Process

The need to enable 'decision makers' who are the 'responsible party' is an increasingly important issue for most organizations. It helps to solve the question posed in SANS/GSEC training chapter 18 on Risk Management and Auditing, namely, "who in your organization is actually authorized to decide what level of risk the organization will accept." (Sans Institute, p.865). The excerpt from an industry paper on information security governance below is indicative of a growing trend to make all levels of an organization responsible for information risk decisions.

> *"Too often information security has been dealt with as a technology issue only, with little consideration given to enterprise priorities and requirements. Responsibility for governing and managing the improvement of security has consequently been limited to operational and technical managers. However, for information security to be properly addressed, greater involvement of boards of directors, executive management and business process owners is required."*
> (IT Governance Institute, p.11).

The ability to accommodate any layer of the company is an important requirement for expanding the IRM process into an effective framework. The generic term 'decision makers' in the objective for the IRM process implies that decision responsibility can exist at all levels of an organization and not just at the Technical/Operational level, which is usually associated with information security. If the goal is to enable decision makers with responsibility for something as ubiquitous as information and as critical to the business as information technology, the framework must address Strategic, Tactical and Operational areas of responsibility. These domains correspond with the three layers of IT Infrastructure Library. (IT Infrastructure Library, p.36). For the purposes of an IRM process framework each can be described as follows:

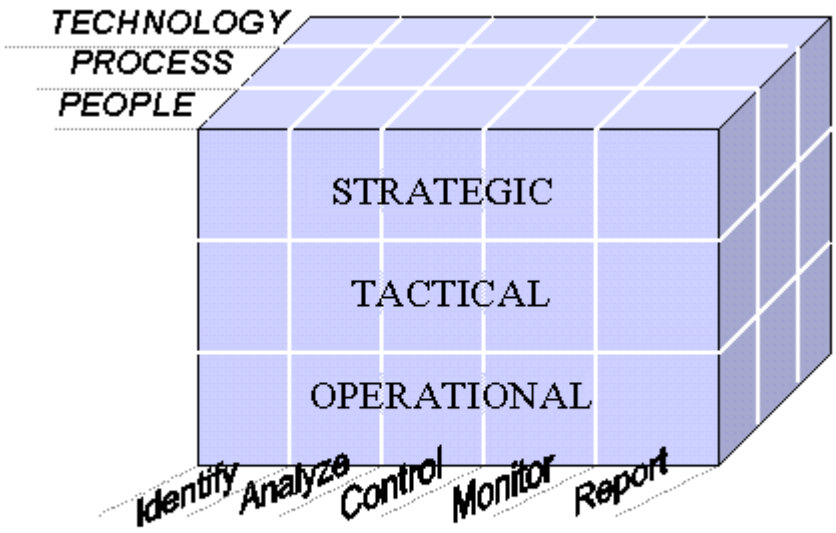
- Strategic - High-level organization objectives, develops policies and plans to achieve these objectives, management activity at the executive level

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Tactical - Mid-level tactics that apply best practice and skill to realize short-term objectives that meet the long-term strategic objectives, management activity at a program level

- Operational - Low-level processes and procedures that immediately affect day-to-day operations, implementing and supporting products, management activity at the operational level

This is the point where an individual organization may choose to use its own business architecture or modify it by adding one more axis to build out an Information Risk Management Process Framework (IRMPF). For a generic management approach, three areas of focus have been added: People, Process and Technology, primarily because information is handled and ultimately controlled (i.e. decisions made) by each of these areas. Combining these dimensions helps bring a comprehensive view of the areas of activity required to manage information risk at a truly organizational level. The illustration in Figure 4 combines the three business responsibility domains, the five IRM process components and the three focus areas. The result is a model of an Information Risk Management Process Framework (IRMPF).



Information Risk Management Process Framework

Figure 4

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Using the IRMPF to Assess Capability for Information Risk Management

By defining the process or activity required for each segment of the framework individually and any potential relationships to other segments, a descriptive capability model of conducting IRM emerges. For example, take the segment identified as Strategic/People/Control.

Using the description of Strategic and the definition of Control, it can be determined if a process exists (or needs to exist) that addresses People-related issues. There should be some strategic mandate or policy associated to educating people in the organization about their responsibility to mitigate information risks (i.e., a policy that sets expectations for a security awareness program). Since policy is a control at the strategic level, the policy can be analyzed to see what other people, process and technology expectations for information risk management (i.e. information security) are described and communicated. The strategic layer then begins to come into focus.

By answering some questions about each segment of the IRMPF, an organization can document their current and planned capabilities. The chart headings below illustrate an approach for using the IRMPF as a guide to systematically capture details surrounding each process component.

IRM	Business Domains			Focus Areas			Details of Enabling/Supporting				
Process Component	**S**	**T**	**O**	**P**	**PR**	**TE**	TASK	PROCESS	TOOL	OWNER	Etc.
Identify	**X**			**X**							
Identify	**X**				**X**						
Identify	**X**					**X**					
Identify		**X**		**X**							
Etc.											

Figure 5.

This approach can drive out the true areas of responsibility and decision making needed to effectively practice information security. The information captured in the 'details' section can be used to document the presence of IRM processes and areas for improvement in the organization.

Understanding the Control Segment of the IRMPF

This systematic capture of details should uncover a particular nuance relative to the Control segment of the IRMPF as it has been defined in this paper. For instance, if all the controls (i.e. a policy, method, procedure or mechanism) were to be identified for the Operational/Technical layer the list would be extremely

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

long. Every conceivable technical control from Biometrics to Firewalls could be listed.

Control in the IRMPF essentially means that a decision has been made about implementing specific Controls. Therefore, the Control component is the object of the other information risk management process components. For example, Identification and Analysis lead to a decision about Controls needed to manage risk (control selection). Equally, Monitoring and Reporting are assessment of existing Controls with a possible decision to loop back and repeat the process cycle as needed to manage risk (control validation). Figure 6 shows this dynamic process loop and relationship of the IRM components to the Control segment at the center of the IRMPF.

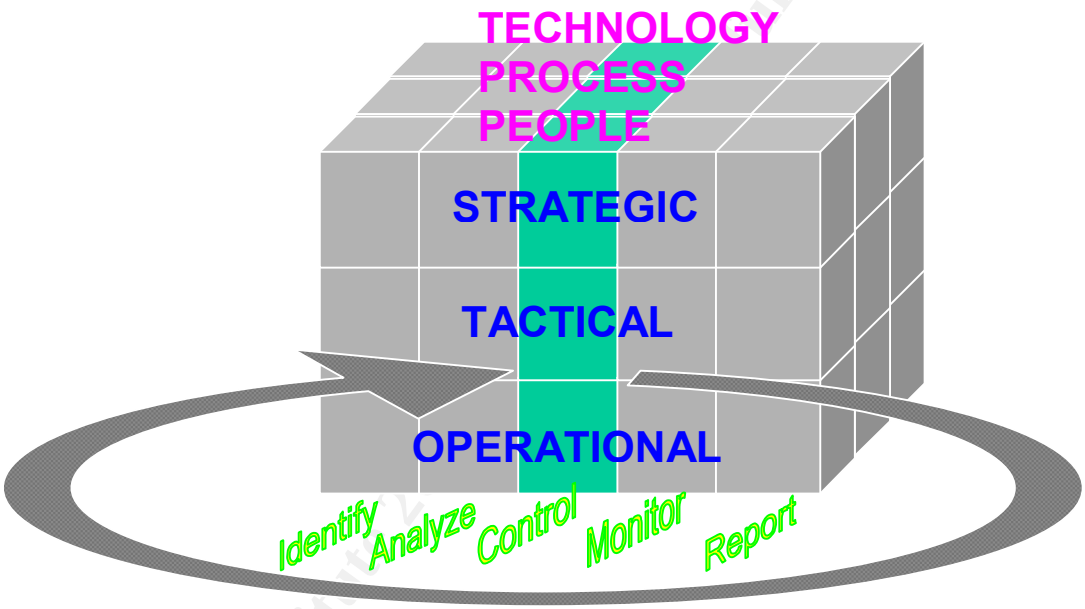


Figure 6

Knowledge of this non-process aspect of the Control segment limits the level of effort needed to document the framework details as outline in the chart above in Figure 5. However, it also points out another task; the need to develop and maintain a list of controls that associate to the business levels and focus areas of the framework. Since the stated objective for the IRM process is to reach agreement on controls, a list of controls (both old and new) must be referenced as decisions are being made concerning risk.

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

A living repository of controls seems essential to the practical functioning of the IRMPF. Using the IRMPF as a key to organize a repository of controls provides some context to how controls actually function in an organization. Figure 7 depicts a sample of the type of controls that would associate to the segments of the IRMPF.

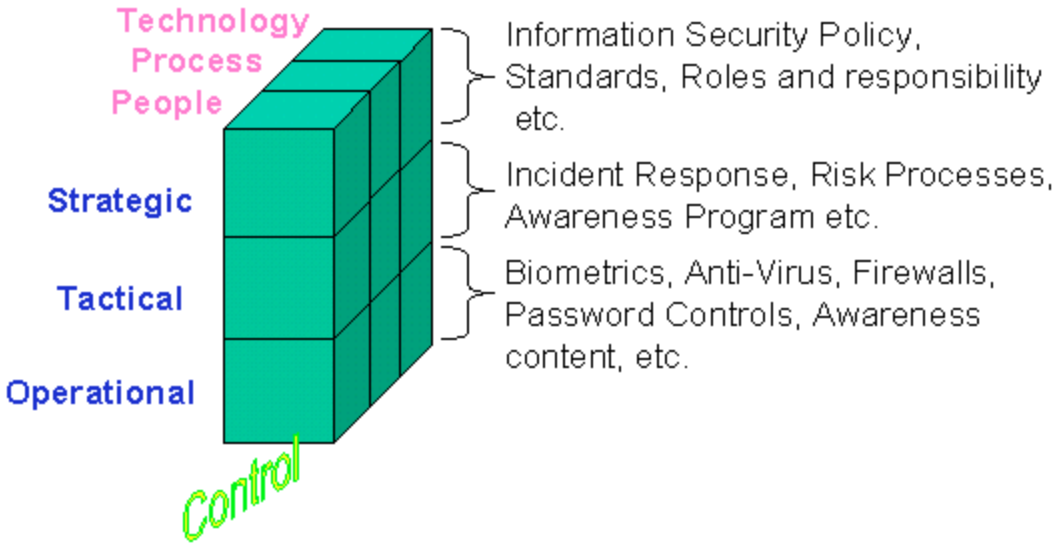


Figure 7

By considering the organizational requirements of each segment of the IRMPF a more comprehensive and lengthy list of controls can be identified. Since the total number of controls could be large and multi-dimensional using this approach, a database would be well suited to enabling a functional repository. A database-enabled repository of controls leads to the possibility of using a knowledge management system to store, organize, and manage controls. The addition of a knowledge management system to support control decisions presents the opportunity to develop workflows that automate the IRMPF. Regardless, it seems reasonable to assume that any accurate assessment of IRM capability in an organization should consider to what extent knowledge management and automation is occurring associated to control selection.

Using the IRMPF to Develop a Maturity Model

Since the IRMPF focuses on key risk management processes, there is the notion that capability within the IRMPF can be mapped to a Capability Maturity Model (CMM®). This would require that a relative rating and description of levels of maturity be assigned to the various processes. At this juncture it makes some sense not to try and develop a rating for all 45 segments. One option would be to use both of the organizational dimensions as keys and then rate the entire IRM process flow within each perspective. This limits the ratings to just nine items. For example, three capabilities can associate to how well IRM is being conducted for Strategy, (i.e. one for People, one for Process, and one for Technology).

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Repeat this for Tactical and Operational and a total of nine maturity-rating scales are generated.

The maturity scale is meant to gauge the relative degree of maturity a process area has within an organization. In addition industry and internal targets can be added as in the example illustrated in Figure 8 from the IT Governance Institute's paper on Information Security Governance. (IT Governance Institute, p.21).

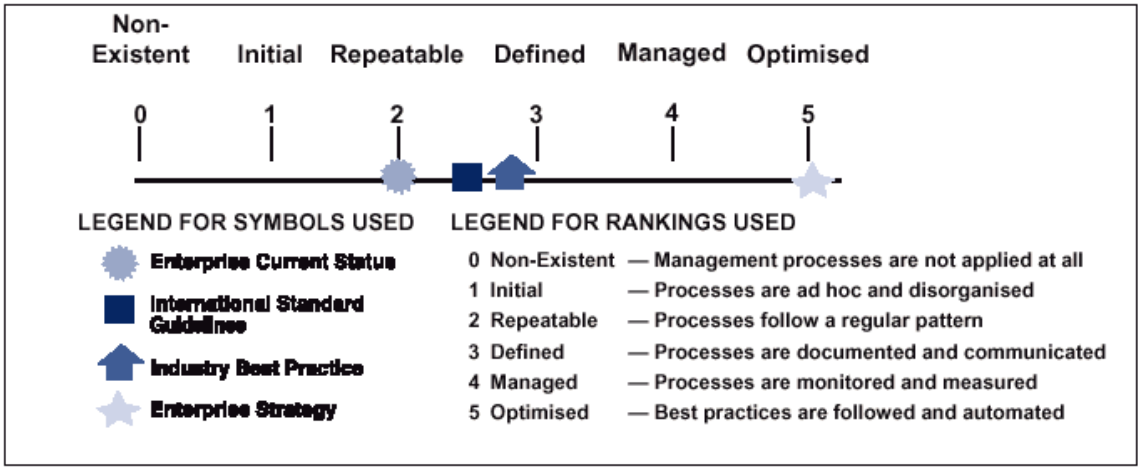


Figure 8

Careful attention to developing these rating scales offers the potential to generate performance indicators for IRM. The ability to know current and future state of the processes in the IRMPF can enable an organization to demonstrate 'due diligence' with regards to managing information risk and represents a significant value proposition for using an IRMPF.

The Value of an IRMPF

For most managers the real test of how well a particular risk is being managed is the degree to which the harm associated to that risk has impacted (or not impacted) the organization. Or to put it another way, did the controls chosen mitigate the risk in a cost effective manner? Once again the ubiquitous nature and dependency upon information in an organization makes answering this question challenging. This is where the benefit of an IRMPF becomes evident. The IRMPF has the ability to span the organization on a par with the use of information. This comprehensive nature of the IRMPF drives the management of information risk into all the areas of an organization that use and ultimately control the information. A fully functioning IRMPF provides a level of confidence in decisions to choose security controls that truly manage information risk equal to its use.

Obviously an IRMPF is just a model to organize the process of systematically managing information risk. But like any good model it helps to describe and ultimately navigate the reality of IRM. Identifying and understanding how and

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

when control decisions are made; establishing information risk tolerance levels; the integration of IRM process into existing control arrangements, etc., are the 'how' challenges that can be solved by first beginning with the 'what'; a practical IRMPF.

Summary

There does not seem to be any doubt that risk management is the foundation upon which information security decisions rest. Numerous models exist that describe what should be done to manage information risk. But 'Information Risk Management' as a discipline is still new and not well understood from an industry and management perspective. It also seems certain that information risk will continue to increase in importance, both as a business performance factor and as a consumer protection issue. The need to expand and identify ways to apply risk management rigor to information risk is key to managing this important new area of risk. A practical IRMPF can serve to focus thinking on what needs to be done to truly conduct IRM in an organization.

The stakes seem high and the challenges seem vast. However, an opportunity exists to use an IRMPF, based on industry standards, definitions and objectives to develop a more mature discipline for Information Risk Management. An IRMPF that brings a systematic and segmented approach to eating this new proverbial elephant "one bite at a time."

© SANS Institute 2003, Author retains full rights.

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Bibliography/Resources

Firesmith, Donald. "Open Process Framework - Risk Management." OPEN Consortium, website 2000-2003.
URL: http://www.donald-firesmith.com/Components/WorkUnits/Activities/RiskManagement/RiskManagement.html

Iheagwara, Charles. *"More Effective Risk Assessment."* Computer Security Journal. Volume XIX, Spring, 2003.

Information Security Forum, The. Information Risk Reference Guide. London, UK. September, 1999. Further information at:
URL: www.securityforum.org

ISO/IEC 17799. *"Information technology – Code of practice for Information Security Management."* First edition. December 12, 2000.
URL:http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=

IT Governance Institute (ITGI*). "Information Security Governance; Guidance for Board of Directors and Executive Management."* 2001.
URL:http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=6672

IT Infrastructure Library. (ITIL). Security Management. London, UK. Office of Government Commerce (OGC). 1999.

National Institute of Standards and Technology (NIST). "Risk Management Guide for Information Technology Systems." NIST Special Publication (SP 800-30) - July 01, 2002
URL: http://csrc.nist.gov/publications/nistpubs/index.html

National Research Council. Computers at Risk: Safe Computing in the Information Age. Washington D.C. National Academy Press, 1991.

Office of Government Commerce (OGC). "Draft Guidelines On Managing Risk." 2001.
URL: http://wwww.ogc.gov.uk/

SANS Institute, SANS Security Essentials: Risk Management and Auditing. Volume 1, Section 3, page 865.

SOGP 2003. "Standard of Good Practice." The Information Security Forum (ISF).
URL: http://www.isfsecuritystandard.com

Submitted by Dan Landess, **GIAC Security Essentials, version 1.4b**
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.