

White Paper

Developing a Information Security Policy and Standard

Developing Information Security Policy and Standards: *The Foundation of Information Risk Management*

Overview

The information security program statement, information security policies, and accompanying standards are the essential foundations of an effective and comprehensive Information Risk Management (IRM) program. These foundational documents, along with guidelines and procedures, are the primary means by which management translates its expectations for minimum information security requirements into specific and measurable goals and objectives. On the contrary, if a company does not implement these requirements and goals the result is often risky decisions made by staff, partners and computer users in general. For this reason Aeritae refers to the information security program statement, policy, standards and supporting documents as the Information Risk Management (IRM) Foundation. This document describes the basic steps for developing an effective IRM Foundation and includes a set of recommended components and steps.

It is important to note that the mere existence of these foundational components may not be enough. Strong executive support and sponsorship also influences the success of an IRM Program.

Approach

When developing or enhancing a client's IRM Foundation, Aeritae considers the following aspects:

- **Accountability** – Roles and responsibilities for Information Security must be clearly outlined including the implications of violations of stated or documented information security requirements.
- **Business Perspective** - Information security controls must address all relevant business requirements, especially protection of mission critical assets including information, Intellectual Property, competitive position, etc.
- **Proportionality** - The level of information security controls must be commensurate with the classification level, value and business criticality of the information and associated systems.
- **Integration** - Information security controls must be integrated as part of the standard business practices.
- **Compliance** - Information security controls must meet legal and regulatory requirements. The IRM Foundation must clearly define the approach for protecting the confidentiality, integrity and availability of information.

IRM Foundations Development Process

The following provides an outline to develop security policies and procedures. These are important considerations when advancing the IRM maturity.

Identify the risks - A high-level review of risks to the business establishes the tolerance for risk and the minimum security requirements. This risk assessment must identify threats and countermeasures, and lay the basis for specifically tailored policy statements.

Outline the primary business objective - Knowing the primary objectives of your business allows accurate scoping of the IRM program. For example, one organization may require extensive audit,

Leaders in bringing balance, innovation and performance to IT organizations.

monitoring, and backup and recovery processes because of business and regulatory requirements, where another company may just need to protect trade secrets and client and employee information. The goal is to have a reasonable and cost effective IRM foundation that is business aligned. In other words, the policy and standards establish the minimum information security requirements that personnel must adhere to.

Define management security goal(s) – This should be a clear and concise statement of the core values most important to your organization in the context of information risk management.

Identify and classify key information resources - A data-centric approach for the creation of information security policies and standards is a common best practice. In today's IT environments, information is a critical asset and should be treated accordingly. Cataloging and classifying your information processing resources enables informed decisions. This also lays the basis for applying the most cost effective security controls on those assets.

Analyze data flows - Perform a data flow analysis for critical information from generation through deletion. This analysis identifies the trust points that touch your data. For instance, in a transaction processing system, data may flow through browsers, web, data, and other servers or firewalls and be stored in databases, on magnetic tape or paper. By tracing the flow of your data through your processing assets, you can later determine the type and placement of logical and physical controls to protect those assets. This process is essential for security architecture because it is the basis for threat analysis and threat analysis is the most efficient way to architect effective security controls.

Develop a threat profile – Identify the threats that can reasonably be expected in the environment. Then determine what the probability is of a threat manifesting itself into an actual problem, and what

Leaders in bringing balance, innovation and performance to IT organizations.

the ramifications, costs and consequences would be. Threats vary widely between different environments. The threats and consequences of attacks to a financial network processing monetary instruments will be different than the threats and consequences of attacks to an online photo gallery that only displays art.

Align the common control framework - -The most common way to build a basic information security policies and standards structure is to leverage a common control framework. Common frameworks include ISO: 27002, COBIT or specific regulations or mandates such as PCI-DSS, GLBA, or the HIPAA Security Rule. Combining several of these frameworks will help to address all aspects of the organizations security requirements.

Meet the requirements of the law - Compliance with regulatory requirements is necessary. A company must avoid violations of any law, statutory, regulatory or contractual obligations. Regulatory requirements include, but are not limited to: US Federal and state statutes, international laws, and standards for protection of personal information. As companies use tools such as instant messaging, blogging and email as well as other digital technologies to conduct business, they must consider and understand the legal impact of these communications, as well as how they affect productivity and storage efficiency.

Construct the information security policy - The information security policy should be created based on the steps outlined above. The policy establishes high level requirement statements and communicates management expectations for an employee or customer and for computer system users. These expectations include confidentiality, integrity, and appropriate management of the data. An information security policy does not, in itself, establish the specific requirements of information systems or

Leaders in bringing balance, innovation and performance to IT organizations.

technologies. It instead defines management's expectations in broad terms. For example, the policy might include a requirement that there must be access controls and then refers the reader to the appropriate standard for those details. The policy should be written in plain and simple language. Any technical terms used should be defined in a glossary.

Create the supporting standard - The supporting information security standards, should provide the specific interpretations of the policies and instruct users, customers, technicians, management, and others on how to implement the policies in specific areas. For example, an access control standard will spell out the details of how access to systems is protected. This may include principles such as role based access controls and specific requirements such as unique user IDs and password length and strength.

Create guidelines and procedures as needed - Guidelines are optional because they suggest rather than mandate an approach or action and in that many companies do not use them. Guidelines can be useful and helpful in providing giving direction to system users when standards and procedures may not be appropriate. There is no need to create a guideline for every standard rather they should be developed in areas that users have problems implementing a control. An example is a password guideline that provides suggestions for how users can create strong but easy to remember passwords.

Procedures are often a requirement, especially for PCI-DSS compliance. Procedures document how the controls defined in the information security standards are implemented. Operational procedures are important for two reasons:

Leaders in bringing balance, innovation and performance to IT organizations.

- 1) Consistency of implementation – Personnel must be instructed to carefully follow procedures for critical control processes to insure that they are implemented fully and consistency.
- 2) Audit evidence – Documented procedures, with evidence of both use and regular review/updates show auditors that controls are being implemented.

Conclusion

The information security policy and accompanying standards are the foundation on which an effective information security program is built. They are the foundational documents that define and describe the minimum information security requirements for the organization. They define governance of employee and/or partner behavior within the organization. They are designed to enable business to move forward with revenue generating projects while reducing risk to the organization. Without effective foundational security documents an organization is in effect allowing company employees to make their own rules and introducing different levels of risk unnecessarily. Additionally, the absence of policy and standards, or inappropriate ones, can put the company in legal jeopardy.

An information security policy should clearly state the organizations ' expectations, and should be based on an evaluation of the specific business environment. . A risk-based approach enables development of an IRM Foundation specifically tailored to an organization's needs.

An effective and robust information security foundation is essential for any organization that depends on the confidentiality, integrity, and availability of their data. Customers, employees, investors and

Leaders in bringing balance, innovation and performance to IT organizations.

other stakeholders entrust their information to the company to maintain and secure. Policy and standards show how a company is implementing that trust.

Leaders in bringing balance, innovation and performance to IT organizations.

Aeritae provides offerings that speak to the needs of information risk managers in these difficult times. Our staff of over a dozen senior risk professionals delivers solutions through proprietary methodologies designed to align risk management with business needs. We also enable your staff to excel by supplying experienced consultants to meet your special requirements.

A key differentiator in Aeritae’s methodology is one of our company’s foundational principles – *balance*, which is what “aeritae” means in Greek. Aeritae’s proprietary offerings balance the requirements of regulatory compliance with managing business risks and opportunities.

Aeritae consultants provide an unmatched depth and breadth in knowledge of best practices, process design, evaluation, tool integration, program management, improvement, and consolidation engagements going **ABOVE and BEYOND** to serve your ITSM solution needs.

Aeritae Information Risk Offerings

Assessment Services

1. Health Checks
 - a. ISO Health Check
 - b. PCI Health Check (Top40)
 - c. HIPAA Health Check
2. Risk Assessments
 - a. ISO 27001
 - b. FISMA
 - c. HIPAA
 - d. Client Standards
 - e. Multi-Standard
3. PCI-DSS Validation Assessment
4. IRM Foundations Assessment

Program Services

1. aboveGPS – an IRM baseline
2. IRM Foundations – Policy & Standards
3. Consolidated Control Framework
4. Security Spend Re-Alignment

Build/Remediate Services

1. Security Architecture Development
2. Vendor Risk Consulting
3. Remediation Services (ID / Access management, network security, PCI remediation, compliance program management)

Security Validation Services

1. Vulnerability Scanning and Analysis
2. Network Penetration Testing
3. Application Penetration Testing

Security Operations

1. Third Party Risk Portfolio Manager

