

# **Information Security Standards and Regulations**

**A General Guide To Compliance**

---

Alexander Hutton : MicroSolved, Inc.

May-04



# Table Of Contents

1	Executive Summary.....	1
2	Fundamentals of Organizational Security .....	2
3	The Security Process .....	3
	Establish a Baseline .....	3
	The Risk Assessment .....	3
	Set Goals.....	4
	The Gap Analysis.....	4
	Creation of the Mitigation Strategy .....	4
	Implement Changes and Controls.....	4
	Measure Change Success .....	4
	Repeat.....	5
4	Summary .....	6

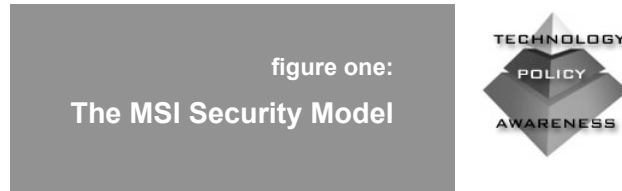
# 1 Executive Summary

Within the past few years, a number of new laws, regulations and standards have been created to ensure that organizations take responsibility for their information security. Complying with these new rules can seem like a daunting task. If an organization gives compliance and proper information security enough thought, however, they will understand that what's most important is embracing a strong methodology towards information security. Once a strong methodology is developed and implemented, compliance becomes simply a task of mapping that methodology and its subsequent documentation to the expectations of the regulatory body focused on auditing the information technology infrastructure.

This White Paper is a high-level overview of what MicroSolved believes is a methodology or information security "life cycle" that an organization can implement in order to achieve "best practices" in information security. In addition to establishing a strong security posture, achieving best practices and implementing such a life cycle creates the added benefit of compliance to most demands of any codified documentation that organization needs to adhere to (be it Sarbanes Oxley, the Graham-Leach-Bliley Act, FFIEC examiners expectations, ISO 17799, HIPAA, etc.). Compliance in the eyes of auditors simply becomes a task of mapping the current security processes an organization undertakes to the expectations of the auditing body.

## 2 Fundamentals of Organizational Security

SecureAssure™ services are designed around a three tier security model. Our model consists of three distinct layers, each of varying importance: technology, policy, and awareness.



First and foremost, information security is a human problem, not a technical issue. Understanding this concept is the first step towards real security. Awareness within the organization is the only way to truly increase security.

Second, an organization must create language that expresses security awareness. Strong and comprehensive policies will guide your organization now and in the future.

Finally, we view technology as a point solution. Implementing technology without considering a foundation of organizational awareness and strong policy will not truly mitigate business risk.

If a security initiative does not adequately address ALL three of these layers then that security initiative is doomed to fail. Only by addressing each of these issues can an organization hope to provide a true security solution.

SecureAssure™ services are designed to be part of an ongoing information security process. Networks, organizations, and attackers are constantly changing. Your organization should be aware of this constant change and have policies that are fluid enough to address this dynamic. In order to achieve best practices, whatever ongoing process an organization creates, it will address all three layers of organizational security.

## 3 The Security Process

There are many sophisticated models that have been developed that express the security process and what an organization should do on an ongoing basis to present the best security possible. However, for the purposes of most organizations, and when almost all of these sometimes complex expressions are simplified, the process is refined to five simple steps:

1. Establish a Baseline
2. Set Goals
3. Implement Changes
4. Measure Change Success
5. Repeat...

### Establish a Baseline

In this step, an organization takes a snapshot of its current security attitude and posture. There are many processes that an organization can take to help establish this baseline. If one of the organizational goals is compliance to a standard or to legislation, and especially if there is an audit involved, the following processes are generally applicable:

1. Risk Assessment (A Good Methodology will include:)
  - a. Policy and Process Review
  - b. Penetration Testing (including Social Engineering)
  - c. Creation of Mitigation Strategy

### The Risk Assessment

The Risk Assessment helps an organization take a holistic view of its attitude towards information security. Generally performed by cross-discipline team of individuals, the Risk Assessment identifies organizational threats, the assets that those threats effect, establishes how vulnerable those assets are to specific findings, and then creates a mitigation strategy to address those issues. There are many different methodologies and means to performing a Risk Assessment, MSI recommends the Octave<sup>sm</sup> Methodology developed by Carnegie Mellon for the United States Department of Defense. It's freely available, customizable and is a good starting place for any organization.

## Set Goals

This part of the process incorporates tasks that are generally included in most Risk Assessment, methodologies, but it is important that those tasks be identified outside of the Risk Assessment step, as the purpose of those tasks fall outside the Establishing a Baseline step in the security process. While Establishing a Baseline helps an organization understand their current security posture, the goal setting process direct an organization towards a more secure posture. Enumeration of what an organization needs to do to establish a stronger security posture is broken down into two steps, one step that stresses compliance to a standard, and the other that is practical application of the findings of the Risk Assessment. Those tasks are the Gap Analysis and the Creation of the Mitigation Strategy.

### The Gap Analysis

The Gap Analysis process measures the security posture of an organization against any pertinent standard. This could be as simple as an organization's codified security policy and processes, or it could be documentation created outside an organization, like ISO 17799. Various regulatory concerns may be fairly nebulous concerning their expectations of an organization (such as Sarbanes Oxley or GLBA), but it is important for an organization to note what risk non-compliance presents (as created in the Risk Assessment) to an organization and what steps should be taken for an organization to address those risks.

### Creation of the Mitigation Strategy

In creating a Mitigation Strategy, an organization defines the processes necessary to address the risks it faces. It identifies the stakeholders that need to take action, and a project plan is built to address implementation. As you can imagine, non-compliance risks an organization face are self-addressed by the current processes.

## Implement Changes and Controls

This step is the actual execution of the mitigation strategy. It closes whatever gap exists between the findings of the risk assessment and what an organization should do to become compliant with a standard. While this process methodology is solely dependent on an organization's situation, it is extremely important to consider utilizing MSI's three tiered model in addressing any risk. An organization should make the proper stakeholders aware of the risk, develop policy and processes or controls that address the risk, and implement technology to further mitigates the risk if necessary.

## Measure Change Success

Finally, an organization should measure the success of it's mitigation strategy. This measurement may be achieved by means of managed security assessments, repeated penetration testing, and/or regular policy and process reviews. What is important is that the results of these measurements are used to perform yet another

Gap Analysis between the new security posture, true risk mitigation and regulatory compliance.

## **Repeat**

Once the mitigation strategy is completed, the security process should begin anew. The reason for this is simple. Networks, like the organizations they represent, are dynamic. Patches for operating systems appear monthly (if not more frequently). New technologies and configuration changes based on IT needs are rapidly changing. Individuals involved in risk identification or mitigation may leave an organization. Security is always changing, and adhering to making the process ongoing is the only way to ensure that an organization maintains the path to compliance.

## 4 Summary

A very wise person once said, "Security is a journey, not a destination."

Organizational security should be approached as an ongoing process. The above steps are a high-level overview of what an organization can do to make security a habit, something that it incorporates into its own culture. Once that process is established and ingrained, compliance to any standard, regulation, or expectation becomes a simple matter of matching expectation to the current process.