Global Information Assurance Certification Paper

SANS GIAC SECURITY ESSENTIALS

PRACTICAL ASSIGNMENT

Submitted by:

Farid Hirani
SANS GSEC Security Essentials
Practical Assignment version 1.3

Original Submission
On-line Program

A Pragmatic Approach to Implementing an Information Security Management Practice

Summary
Information security is a journey towards a destination. It is also an iterative process. Information security cannot be achieved merely by implementing technology solutions. It could even be said that absolute information security assurance is an impossible goal. However, without an adequate Information Security Management Practice (ISMP) an organization's information assets, that is, its data and computing resources, and the very viability of that organization, may be in jeopardy. The successful implementation of an ISMP involves a number of critical activities, which should be accomplished in some semblance of order. Failure to do so could result in a dysfunctional practice, which would do little justice to the effort expended, much less to the security it can offer to the organization. The primary activity around developing and implementing an ISMP revolves around risk management, because each organization will have a unique perspective regarding the criticality of its information assets. Once a functional ISMP has been successfully implemented, it will be an on-going endeavor to ensure that acceptable information security and risk thresholds are maintained. The continued success of the ISMP will subsequently depend on all members of the organization, both those directly associated with it, as well as those indirectly associated with the organization.

This white paper will attempt to identify the various activities required in the setting up of an organisation's Information Security Management Practice. The particular emphasis will be on establishing an information security management framework.

Introduction
With the advent, ubiquity and proliferation of the Internet and TCP-IP networks over the past few years, it is fairly evident that the landscape of information management has changed considerably. The scope has broadened from a localized to a global environment. This change in scope has brought additional challenges to the management of an organization's information assets, which now also includes the safeguarding of that information from hostile agents and agencies.

While the safeguarding of an organization's information assets is currently only seen as an internal concern, it is almost certain that the next few years will see a significant change in this perception. The information security practices and safeguards an organization has implemented, or rather has failed to implement, will be the subject of legal proceedings and litigation, based on due diligence, or the lack thereof, on the part of organizations dealing with information.

An organization, or the principle affiliated with the organization, that fails to implement adequate controls may be held accountable for inadequate preparation against distributed denial-of-service attacks, propagation of viruses, disclosure of confidential information,

or failure to adequately protect information assets, which could in turn result in financial losses.

The shift away from a proprietary focus will be due largely to the merging of traditional business models and new business models with global scopes, which utilize the electronic frontier.

The primary goal of an ISMP is to provide information Confidentiality, Availability and Integrity assurance.

Thus, all aspects of information security management will apply universally across national boundaries, and to every organization irrespective of size, much as information flows across national boundaries today.

Oftentimes, the implementation of an ISMP is a challenge for organizations, in that they require a road map for deployment. It is hoped that by following the guidelines in this document, and the references contained herein, an organization may be able to identify the specific activities required to establish an information technology security management practice pertinent to its unique needs.

Assumptions

It should be noted that this guide does not set out to justify the requirement for information security. This guide pre-supposes an organization's acknowledgement of the requirement for information security management, that is, a commitment to provide the assurance of the Availability, Confidentiality, and Integrity of the organization's information assets. By that acknowledgement, the organization will also have accepted its responsibility in a global sense, and be prepared to allocate appropriate resources to support the practice.

It makes the assumption that there is executive approval and commitment for the establishment of an ISMP within the organization. This decision may or may not be as a direct consequence of an external audit.

As well, this guide makes no specific representation either for or against either an in-house solution or an outsourced solution for the implementation of an ISMP.

How to use this guide

The guide uses the framework of the Information Security Circle of Security – (Assessment,) Protection, Detection and Response (and Review) – complemented by the control categories of the ISO 17799 standard as the basis for the approach.

This guide attempts to provide the foundation of a systematic approach for implementing an ISMP, identifying individual aspects to consider. In developing an ISMP, an organization may use this guide to develop checklists of tasks to accomplish. (Some

excellent templates for self-assessment are available from *National Institute of Standards and Technology* [1].)

As well, "*Information Security*" by Donald L. Pipkin provides a useful reference for addressing all aspects of information security [2].

In developing an ISMP, not unlike as in any other project, it is important to *plan for success*. Thus, it is strongly recommended that implementation activities be feasible and measurable, and that they be linked to milestones with realistic timelines for completion.

A Holistic Approach

A successful ISMP may be described by the following relationship.

Information Security = Risk Analysis + Policy + Implementation + Threat/Vulnerability Monitoring + Threat/Vulnerability Response

The practice comprises the "Circle of Security", as well as the ISO 17799 controls, as shown in the diagram below.

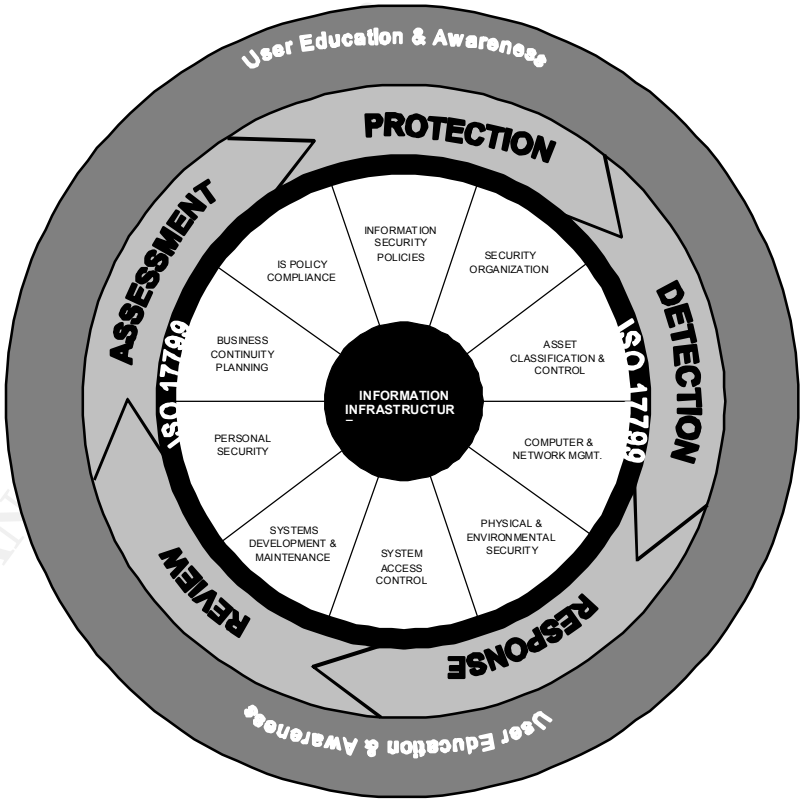

Figure 1 Representation of a Holistic Approach to Information Security

Figure 1, above, depicts an organization's core information infrastructure bounded, from the innermost layer outwards, by:

- The ISO 17799 control categories;
- The Circle of Security; and lastly,
- A program of ongoing User Education and Awareness.

Developing and maintaining a successful ISMP requires adopting a *corporate security state of mind*. To quote Rudyard Kipling,

> *I keep six honest serving men*
> *(They taught me all I knew);*
> *Their names are What and Why and*
> *When*
> *And How and Where and Who.*

Employing the "six honest serving men" will go a long way towards achieving the requisite state of mind.

Further, numerous studies have shown that organizations are far more at risk from *insiders* than they are from *external* agents. As illustrated in Figure 1, the challenge lies in engaging the minds of every user in an organization: the key to success for any information security practice is user awareness and education. A careless or uninformed user has been the undoing of many a plan.

Where to Start

In an industry, which is infamous for the existence, as well as the absence of several critical standards, an organization can in fact anchor its information security management on a standard. The ISO 17799 standard, based on the original BS7799 British Standard, provides a standardized framework for implementing an ISMP.

The purpose of the ISO 17799 standard has been described as to

> *"give recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings."* [3]

Having established an information security management standard for the organization, the next activity is to apply that standard toward the development of the ISMP – the roadmap of *how the standard will be implemented*.

For this, we refer back to the Circle of Security: (Assessment,) Protection, Detection and Response (and Review).

Thus, a comprehensive ISMP embraces both the ISO 17799 and the Circle of Security.

Before the process can be applied, however, the organization needs to determine *what* the strategy will be applied to – the term "information assets" can be nebulous.

Risks, Threats and Vulnerabilities

Before protective measures can be applied, it is important for an organization to know *what* information assets it needs to protect, as well as *what or whom* it needs to protect those assets from. In order to know this, the organization needs to conduct various assessments based on facts pertaining to its information assets.

It should be noted that, although current information security models are directed at those proprietary networks that connect to the Internet, even those organizations that do not connect to other networks, specifically the Internet, are susceptible to threats and vulnerabilities. Such organizations will have rather different sensitivities.

The term *risk* may be defined as "*the potential for loss or harm"*. Risk usually exists due to the presence of vulnerabilities to some threats.

Step 1

The implementation of an ISMP commences with the first pass of the ***Assessment Phase***.

For any organization, the starting point is to identify the specific information assets, the insecurity of which could compromise the organization. These assets identify the organization's **Statement of Sensitivity**.

Consequently, the very first step in the implementation of an information security management practice is to implement a **Risk Management Strategy**. The purpose of the Risk Management Strategy is to identify those components of the organization's information infrastructure that are vital to the functioning of the organization (the *Statement of Sensitivity*), to develop a **Risk Profile,** and to develop appropriate methods to mitigate the risks identified.

Ultimately, a successful ISMP is about managing risk. Thus, a risk management strategy is a vital component of the overall ISMP.

Information Risk Management Strategy

Risk Management is a science unto itself, and beyond the scope of this guide. A number of references are provided at the end of this document, some of which specifically address the subject of Information Security Risk Management.

The following six major steps are recognized as key elements of a generalized Risk Management strategy:

- Establish risk context
- Identify known risks
- Conduct risk analysis
- Conduct risk evaluation – develop the organization's *Risk Profile*
- Develop & implement risk mitigation measures
- Monitor & update the *Risk Profile*

Thus, following the above model, the purpose of an organizational *Information Risk Management Strategy* is to:

- Identify those elements of the information infrastructure that are critical to the organization. This is known as a *Statement of Sensitivity*;
- Assign business value or a *criticality factor* to these assets;
- Acknowledge and identify the threats and vulnerabilities to the information assets;
- Determine the safeguards already in place, or other risk mitigating factors;
- Assess the "residual" risks to the assets;
- Develop a Risk Profile;
- Determine and implement the measures to mitigate the risk;
- Continuously monitor and update the risk profile.

The following diagram, reproduced from the *Australian Standard Handbook of Information Security Risk Management* [4], describes the inter-dependencies.

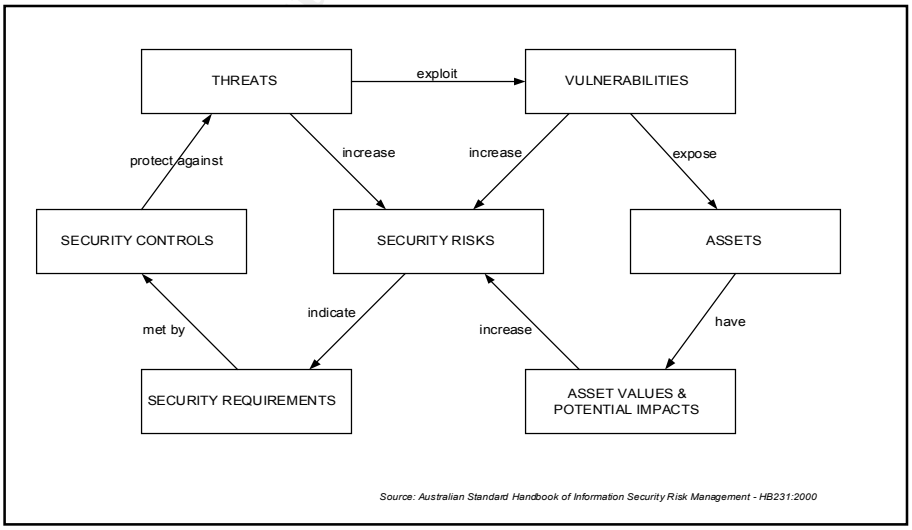

Figure 2 Risk Concept Relationship Diagram

Like the information security management *process,* risk management is also an iterative process.

Objectives of Information Risk Management

The overall objectives of an information security Risk Management practice, having accepted the fact that risk cannot entirely be eliminated, are to:

- Identify the specific risks to the security of an environment, process or object;
- Reduce the likelihood of the risk's occurrence;
- Reduce the impact in the event the risk manifests;
- Avoid the risk entirely, by removing the cause for, or the object of, the risk;
- Transfer the risk, such as through insurance;
- Accept the risk.

The Statement of Sensitivity

Thus, the logical place to start a risk analysis is to gather information pertaining to the organization's critical information assets, data, resources and services. The deliverable from this exercise is the *Statement of Sensitivity*. A sample template for an organizational Statement of Sensitivity, as well as other excellent reference material pertaining to information security risk management, is available in the *Guide to Security Risk Management for Information Technology Systems*, published by the Government of Canada [5]. A number of very useful references are also available through the *National Institute of Standards and Technology* [1].

Information collected should include, at minimum, the following areas:

- Data: Classification to include Restricted, Confidential and Public (or some form thereof);
- Critical systems, hosts and devices;
- Network access points and gateways;
- Information flow and usage: business customers and partners;
- Information communications links: Suppliers, customers, strategic partners, etc.

From the above list, it is evident that an organization's *Statement of Sensitivity* will require participation from many different areas of the organization, regardless of its size. It is critically important that this exercise not be conducted in isolation by a single area within an organization, because doing so will be a disservice to other areas of the organization. Furthermore, it will likely make inaccurate assumptions, draw an incomplete picture, and consequently reach the wrong or incomplete conclusions.

When developing the Statement of Sensitivity it is also becoming increasingly necessary to examine *legal requirements* pertaining to specific information assets, particularly

personal information. Recently, many countries worldwide have enacted, or revised, legislations pertaining to the collection, storage, retention, and disclosure of confidential or personal information. Such legislation imposes specific legal conditions and requirements on those agencies that collect, store, retain and use personal information.

References related to legislation around information security are shown at the end of this guide.

Step 2
Following the completion of the Statement of Sensitivity, the next activity should be a ***Threat and Risk Analysis***. The Threat and Risk Analysis will describe in detail specific threats to each of the items in the Statement of Sensitivity, addressing the individual vulnerabilities identified, and assign a level of risk acceptable to the organization.

Threat and Risk Analysis
Should an external agency be hired to conduct the Threat and Risk Analysis, or can a group internal to the organization be sufficient?

The decision as to who conducts the Threat and Risk Analysis is purely academic, but requires the highest degree of accuracy and objectivity.

A successful Threat and Risk Analysis will help the organization determine which critical information assets are most at risk, and should lead to the development of safeguards to reduce the risk.

The Threat and Risk Analysis, then, will consist of developing defense strategies around the organization's Statement of Sensitivity, by identifying specific threats to and vulnerabilities in each of the information assets listed in the Statement of Sensitivity.

Some of the techniques used in conducting Threat and Risk Analyses include:

- Network penetration testing from external source(s), including port scanning;
- Host vulnerability scanning;
- Review of current information services and security practices, processes and procedures.

Threats and Threat Vectors
Unfortunately, the information security community has not yet adopted a unique terminology, and so, quite often, the terms *threat* and *threat vector* are used interchangeably. For the purpose of this guide, the terminology adopted by SANS will be followed. To whit,

Threats: Threats exploit vulnerabilities in information security, such as inherent system flaws, or lack of procedures, in order to cause some

form of harm. An example of a threat is *Social Engineering*, which preys on the vulnerability of unsuspecting users.

Threat Vectors: Threat vectors are the sources, or the agents, of threats, who through various methods manifest a specific threat. Threat vectors may be *outsiders* from Internet, or *insiders* on the internal network.

It should be noted that, although the current popularized threat vector is from cyber-space, the commonplace insider, who bypasses prescribed procedures, has proved to be a formidable threat vector.

The current *cyber* threats from both internal and external sources can take a variety of forms to include:

- Disruption. This can include disruptive viruses and denial of service attacks that could impact commercial information flows, such as banking transactions and electronic commerce;
- Exploitation. Threats of exploitation involve the compromise of sensitive or proprietary information and include identity spoofing, credit card fraud, and information theft;
- Manipulation. This can be done for political or economic reasons or just for pure vandalism. It can be something as simple such as the defacement of a web site or more serious such as the manipulation of financial and infrastructure data. Threats of manipulation may also include the installation of Trojan horse programs, which may be subsequently used to create distributed denial of service attacks.
- Destruction, Failure or Loss. This involves exploits that access systems and cause data to be wiped out on hard drives or other data storage systems, or cause systems to fail.

A number of information security Threat and Risk Analysis guides are available in the public domain; references to some of these are provided at the end of this document.

Vulnerability Assessment

Threats exploit vulnerabilities that exist within a specific host, a particular system, or an operational procedure.

As stated earlier, a Threat and Risk Analysis includes *vulnerability assessment*, which may consist of:

- Network penetration testing;
- Running vulnerability scanner tools against the network or specific hosts;
- Conducting audits and reviews of system configurations;

- Conducting audits, reviews, or verification of business processes, including policies; or,
- All of the above.

A *Vulnerability Assessment* will seek to *gauge the ability of threat vectors to exploit specific vulnerabilities to manifest a specific threat*, through the identification and characterization of all potential threat scenarios.

The organization's business goals, objectives and processes can form a good starting point for the identification of information vulnerabilities.

Risk Analysis

Risk Analysis is also science unto itself, and is widely used in the Insurance industry in which the concept of risk is a central issue. Having identified the threats and vulnerabilities, the purpose of Risk Analysis is to quantify, or to provide some rating of risk directly related to the threats and vulnerabilities, and to selectively ascertain and recommend the specific risk mitigation measures.

A final activity is a Cost/Benefit Analysis, which should ask the question "Will the proposed recommendations be cost-effective?"

There are essentially two basic forms of risk analysis: *quantitative* and *qualitative* analysis.

Quantitative Risk Analysis involves assigning a monetary value to a potential loss, and is linked to the Loss Expectancy methodology. Two methods of assessment are used, *Single Loss Expectancy* (SLE), and *Annualized Loss Expectancy* (ALE).

Quantitative Risk Analysis is calculated using the following formulae:

Single Loss Expectancy = Asset Value x Exposure Factor,

Where *Exposure Factor* represents a measure of the magnitude of loss or impact on the value of an asset. It is expressed as a percentage, ranging from 0% to 100%, of asset value loss arising from a threat event.

Annualized Loss Expectancy = Single Loss Expectancy x Annualized Rate of Occurrence

Qualitative Risk Analysis is the process of evaluating risk based on scenarios and determining the impact such an incident would have [6]. It involves assigning a risk rating, based on criticality, the potential impact to the organization, existing safeguards, and the likelihood of occurrence.

Qualitative risk is variously derived from the following formulae:

- *Risk rating = Threat x Vulnerability x Asset Value*
- *Risk factor = Criticality (or business value) x Vulnerability*
- *Risk factor = Impact x Probability*

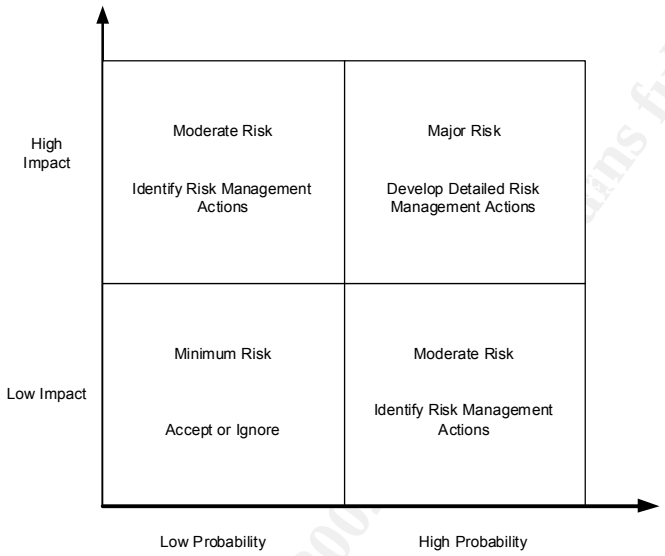

Figure 3 Risk Rating Matrix

It should be borne in mind that, although qualitative analysis using algebraic relationships is used quite extensively, its true value is in providing guidance for risk mitigation. In spite of a specific qualitative risk rating, the actual risk may be completely unacceptable, such as when the safety of personnel is compromised.

Summary of the Benefits of an Information Risk Management Strategy

To conclude the Assessment Phase, it is important to once again link a Risk Management Strategy to an effective ISMP.

The benefits include:

- A cost-justified approach to information security;
- Productivity: Audit/Review Savings;
- Breaking down barriers through business relationships
- Integration of information security in a proactive fashion, through "self-analysis";
- Increased information security awareness by involvement in various information technology projects;
- Adherence to "baseline" security and policy;
- Providing a consistent and objective approach;

- Better targeting and mitigation of security weaknesses;
- Consistency in the overall assessment and analyses of, and mitigation of risk to, information security [7].

Step 3
Having completed both the Vulnerability Assessment and Threat & Risk Analysis activities, the ***Protection Phase*** of the Circle of Security may now be commenced. This phase addresses the incorporation of the ten control categories postulated by ISO 17799.

The Protection Phase, in essence, will seek to implement mitigation strategies for the risks identified in the Assessment Phase. Note the term "risk mitigation", because it is extremely unlikely that there will be a situation where all risk is completely eliminated. The protection phase deals with the "residual risk". It should be noted that there are a growing number of instances where "residual risk" to information security may be covered by appropriate insurance policies.

The objectives of the Protection Phase are to safeguard those information assets identified in the Assessment Phase, through the implementation of specific controls, tools, and techniques. The Protection Phase, then, deals with the implementation of specific **controls** to mitigate the risks identified. Following the ISO 17799 guidelines, the control categories and examples of protective measures are described below. Note that these categories should only be considered as guidelines for the implementation of protective measures.

The specific controls that an organization will implement will derive from the recommendations of the Assessment Phase, because each organization will have a unique *risk profile*.

ISO 17799 Protection Control Categories
The ISO 17799 standard describes the following control areas [8].

Business Continuity Planning
The purpose of a formal strategy for Business Continuity Planning is to develop specific measures to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

The Business Continuity Plan needs to be detailed enough to identify individuals (both internal and external to the organisation), assets, environments and processes to minimise the interruptions to normal business activities.

One of the sub-components of the Business Continuity Plan should be the identification and formation of a *Security Incident Response Team*, and an attendant *Security Incident Response Procedure*. It is also important that the organisation regularly conduct "table-top" exercises that test the Security Incident Response Procedure.

System Access Control
System Access Control seeks to limit access based on the principle of "least privilege". In other words, the access and privilege accorded to individual users is controlled on a need-to-know basis.

System access control includes:

- Managed access to information;
- Prevention of unauthorised access to information systems;
- Protection of networked services;
- Prevention of unauthorised computer access;
- Methods for the detection of unauthorised activities;
- Applied information security in mobile computing and remote networking facilities.

System Development and Maintenance
The controls in this category address the inclusion of security in systems development and maintenance. Such controls

- Ensure security is built into operational systems;
- Prevent loss, modification or misuse of user data in application systems;
- Protect the confidentiality, authenticity and integrity of information;
- Ensure information technology projects and support activities are conducted in a secure manner;
- Maintain the security of application system software and data.

Physical and Environmental Security
The objectives of this section are to
- Prevent unauthorised access, damage and interference to business premises and information;
- Prevent loss, damage or compromise of assets and interruption to business activities;
- Prevent compromise or theft of information and information processing facilities.

Compliance
The objectives of this section are to:
- Avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements;
- Ensure compliance of systems with organisational security policies and standards;
- Maximise the effectiveness of and to minimise interference to/from the system audit process.

Personnel Security
The objectives of this section are to:

- Reduce risks of human error, theft, fraud or misuse of facilities;
- Ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work;
- Minimise the damage from security incidents and malfunctions and learn from such incidents.

Security Organisation
The objectives of this section are to:

- Manage the information security practice within the organisation;
- Maintain the security of organisational information processing facilities and information assets accessed by third parties;
- Maintain the security of information when the responsibility for information processing has been outsourced to another organisation.

Computer & Network Management
The objectives of this section are to:

- Ensure the correct and secure operation of information processing facilities;
- Minimise the risk of systems failures;
- Protect the integrity of software and information;
- Maintain the integrity and availability of information processing and communication;
- Ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
- Prevent damage to assets and interruptions to business activities;
- Prevent loss, modification or misuse of information exchanged between organisations.

Asset Classification and Control
The objectives of this section are to

- Maintain appropriate protection of corporate assets, and
- Ensure that information assets receive an appropriate level of protection.

Security Policy
The objective of this control category is to provide management direction and support for information security management.

Which control first?
The question often arises in organisations that have already had information infrastructures in place for some time, as to which control to implement first.

Although the actual order may vary by organisation, in the opinion of this author, the key controls, and the order of implementation, will be determined from the Statement of Sensitivity.

General consensus recommends the following:

i. Security Organisation
ii. Asset Classification and Control
iii. Security Policy
iv. System Access Control

However, if the organization is already connected to the Internet, and has not yet implemented any safeguards (such as firewalls), it may be more appropriate to implement "system access controls" immediately.

Other controls may be implemented in the order most suitable to the organisation. However, the *Compliance* control should not be neglected.

Considerations for implementing ISO 17799 Controls
In implementing the controls identified by the ISO 17799 standard, an organization should take into consideration the following points.

- Legal Requirements: FOIPP, FIPS, Bill C6, etc.;
- Implementation plan, including activities, timelines and milestones;
- Roles and responsibilities;
- Processes and Procedures, which will be derived from policies;
- Standards;
- Quality Assurance.

Protection – Some Guidelines
The following protection schemes are provided as guides; specific protective measures may be unique to each individual organization. The following are submitted for consideration:

Minimum Recommended Policies or Procedures

- Network Access Policy
- Acceptable Use
- E-mail Policy
- Data Retention and Disposal Policy
- Information Usage and Disclosure Policy
- Internet Use Policy
- Virus Control Policy
- Security Patch Policy

- Remote Access Policy
- Incident Response Procedure
- Configuration Management Policy
- Change Management Procedure
- Information Technology Projects Policy

Suggested Protection Schemes

- Authentication: Strong Passwords
- Business Resumption Plan
- Backup and Recovery
- Standard device/host configurations
- Secure network infrastructure
- Operating System Hardening
- Segregation of duties
- Documentation
- User Awareness (again!).

Many other protection schemes are possible, the relevancy of which will vary by organization.

A recent publication from CERT titled "*CERT Guide to System and Network Security Practices*" articulates some very practical protection schemes, and is strongly recommended [9].

For UNIX-specific protection schemes, refer to *Practical UNIX & Internet Security* by Simson Garfinkel and Gene Spafford [10].

How to prioritize implementation of protection

The decision to implement a particular protective measure over another can be a difficult one. However, the following formula will serve to prioritize the implementation of a specific safeguard.

$$P = (C+S) – (SC+NC)$$

where,

C=criticality, S=severity, SC=system countermeasures, NC=network countermeasures, and P=priority.

Detection Phase

Detection comprises the mechanisms, processes, strategies and techniques to monitor the effectiveness of the controls implemented, and the discovery of attempts or instances to circumvent protection measures that have been implemented.

In other words, the Detection Phase continuously seeks to answer the question "Is the Protection scheme for the security of our information assets effective? Are the controls adequate?"

And most importantly, "How do we know?"

The basic approach to detection consists of:

- Continuously monitoring critical systems and network "gateways" for unexpected or suspicious behavior, or activity;
- Investigation of anything that appears to be unusual; and
- If the investigation reveals anything that cannot be explained by authorized activity, to invoke the activities in the Response Phase.

Detection activities should, at minimum, cover the following areas:

- The integrity of the detection engines and/or systems (rootkits and Trojans);
- Monitoring of the behavior of systems, and the traffic in the network;
- Physical access to critical systems, data, including backups, and output devices (examples, keystroke-logger devices, modems);
- Alerting mechanisms, both automated and user-based. Note that "user-based" alerting speaks to the empowerment of users to report suspicious activities, and further emphasizes the need for continuous user awareness and education with respect to the organization's information security.

As indicated elsewhere, both internal and external threat vectors may manifest threats to the security of an organization's information assets.

Thus, in detecting anomalous behavior, it is just as important to address the internal "miscreant", who may set up a rogue remote access server, or who may download and install non-standard applications from the Internet, as it is to watch for network intrusion attempts from external sources.

This phase, then, also engages the ISO 17799 control category identified as *Compliance*, which seeks to ensure that internal users comply with such controls as:

- Information security policies;
- Security processes and procedures, such as Change Management; and
- Information standards.

Again, it is evident that an informed user, who has been made aware of the threats and risks, can contribute to the overall ISMP of an organization.

What activities or events may be considered unusual?
Detection of anomalous behavior or activity may prove challenging if *baseline* statistics, such as for "normal" network traffic or resource usage patterns, have not been established.

However, the following are points to consider:

- Unexpected network behavior at specific times of day, or loss of connectivity;
- Traffic to and from specific sources;
- Repeated attempts to connect to specific systems and or ports;
- External scans and probes of the network.

Detection Tools and Techniques
Detection methodology varies from basic techniques, to complex real-time systems consisting of anomaly detection engines, deployed throughout a network.

Of the different methodologies employed for Detection, some are described below.

Audits & Reviews
Security audits and reviews are an investment in the reduction of risk to information security. As well, audits and reviews provide a mechanism for addressing compliance with regulations (legislation, security policies, standards, procedures and processes), and for the validation of industry best practices (such as, secure information technology equipment configuration).

Many different approaches are possible, based on nature of the organization's primary function. However, two general guides to performing audits and reviews are:

- Scheduled reviews during the conceptual and detailed design phases, and immediately preceding the implementation of information technology projects;
- Random audits of information assets, to validate compliance with standards.

It is also important that audits and reviews bring a complementary perspective to projects and operational environments, in a non-threatening manner. Using such an approach can provide information security management personnel with more opportunities to impart education and awareness to users.

Further information on information system auditing may be obtained from publications by the *U.S. General Accounting Office* [11].

Integrity Checkers
Integrity checkers provide a means of establishing "baseline" configuration files for critical systems. By doing so they provide two measures of protection:

- Maintaining a secure backup copy of system configuration files for critical systems;
- Providing detection and evidence of changes made to those files.

Integrity checkers work by creating cryptographic signatures (checksums) of the original versions of user-specified files. Some types of integrity checkers, with built-in intelligence, provide real-time alerts when attempts are made to change the protected files.

Integrity checkers may also be deployed on entire contents of disks.

Tripwire Inc. [12] is a major vendor of integrity checking software.

Intrusion Detection Systems
As the term implies, Intrusion Detection Systems (IDS) are designed to provide alerts when an intrusion has been detected in a protected environment.

There are two basic types of IDS'es:

- Host-based Intrusion Detection Systems (HIDS);
- Network-based Intrusion Detection Systems (NIDS).

Typically, NIDS examine all network packets and compare them against known patterns of "anomalous" traffic. When such traffic is encountered, specific actions may be triggered, based on the capabilities of the specific NIDS. As may be expected, the database of known attack patterns or signatures may need to be updated on an ongoing basis, rendering the IDS more of a *reactive* tool dependent on the currency of the database.

Newer NIDS technologies also examine network packets for anomalies from a protocol perspective, thereby incorporating a *real-time* or *proactive* alerting capability.

The costs to implement NIDS can range from inexpensive, using free tools such as SNORT [13], to extensive, such as *ManHunt*, by *Recourse Technologies* [14].

Host-based Intrusion Systems are installed on designated computers, and are localised to those specific hosts. Increasingly, the differences between HIDS and Integrity Checkers are becoming blurred.

An effective Intrusion Detection System will comprise both HIDS and NIDS.

More information on Intrusion Detection Systems technology may be obtained from the *Network Security Library* [15].

Log Analysis & Management
Log files are a key tool for the collection of security events on various components of the organization's information infrastructure, such as file servers, routers, switches and firewalls.

Log files need to be regularly analyzed for anomalous activities. The information captured may also be required for the purpose providing forensic evidence in support of specific security incidents.

However, some of the challenges around security events log can be daunting:

- Logs are distributed on multiple data storage devices
- High rates of event logging, amounting to potentially staggering volumes of data;
- Lack of a universal format for logs in heterogeneous systems;
- Analyses are resource intensive;
- Reporting requirements, from multiple devices, can be quite complex.

In order to provide effective log analysis, management and reporting, a comprehensive system is be necessary. One such application is *neuSECURE* by *GuardedNet* [16].

Comprehensive Virus Detection and Alerting
Over the past few years, various threats to information security have been manifested through the proliferation of *malicious code,* such as viruses, worms and Trojan horse programs.

While one reason for the success of such attacks is numerous vulnerabilities in software applications, the more disturbing reason is the success of *social engineering* attacks. Often, malicious programs prey on the trusting nature of users to execute e-mail attachments with malicious content, or to download applications from the Internet which masquerade as useful programs, but in reality are Trojan horses.

Two effective methods of protection against malicious code are:

- A comprehensive anti-virus technology solution;
- User education and awareness.

Enterprise technology solutions should implement protection in a layered approach: at gateways, on e-mail servers, on file servers, and on individual desktops. A centralized deployment should ensure that the following functionality is available:

- Centralized logging and alerting;
- Timely deployment of virus signatures updates;
- Reporting on departures from, and enforcing the corporate anti-virus policy;
- Protection of devices that access the corporate network remotely.

An example of a product that is attempting to address most of the above points is *"epolicy orchestrator"* from *McAfee Security* [17].

Thus, the primary objective of detection methods is to *quickly* become aware of any anomalous behavior, such as attempts to subvert information security protection schemes, departures from policy, procedure by-passing, and unauthorized access.

The consequence of detection is appropriate and timely response, the subject of the next phase.

Response Phase

The Response Phase is activated by the detection of an instance or event that may be considered to be a security event.

The key factors of response are:

- Timeliness;
- Appropriateness;
- Completeness or thoroughness;
- Forensics: Preserving the chain of evidence.

If a formalized Security Incident Response Procedure has been formulated, its efficacy will be validated here.

A useful reference on response activities is available from CERT® titled "*Responding to Intrusions*" [18].

Thus, in the event of a security event, the Security Incident Response Team will be engaged in the following activities:

- Identification: What has been detected?
- Analysis: How serious does the event appear to be? Is there a need for escalation, perhaps a call to activate the Business Continuity Plan? Do external agencies need to be alerted?

- Assessment: Review of the analysis; Detailed assessment of the event; Collection of evidence;
- Containment: Are more systems likely to be affected?
- Eradication: Such as in the case of a virus, or Trojan horse, incident;
- Recovery: Restoration of normal functions and services;
- Report: May also include a "review of the incident response".

Above all, communication amongst and by the Security Incident Response Team will be a critical activity, and may involve external agencies and/or business partners.

Review Phase

This phase is sometimes contained within the Response Phase, and is associated with specific responses to information security breaches.

However, for the purpose of this document, the Review Phase is identified as a separate phase, in order that it may be implemented independent of specific incident responses. Doing so enables an organisation to engage in a review of information security practices in response to a new information technology project undertaking.

The Review Phase has also been termed the "Improve Phase". Again, for the purpose of this document, improvement is an included item in the Review Phase, because, in order to improve, a review is necessary.

Security audits can also perform a useful role in the Review Phase.

Thus, the Review Phase may include of the following.

Review of the Incident Response Procedure

Addressing a specific incident response event, the review will seek to answer the question, "How effective was the incident response procedure? What lessons were learned?

Review of the Information Technology Environment

In most organisations, the information technology environment is constantly changing – new systems and technologies are introduced, or existing systems are continually being enhanced.

These changes may have the potential to change the organisation's Statement of Sensitivity, and the attendant Risk Profile.

Review of Information Security Integration

A successful information security practice permeates through all departments and all levels of an organisation, and is integral to all aspects of the organisation's information technology, including:

- Systems development;
- Infrastructure services;
- Operations management; and,
- Business processes.

A review will identify areas of weakness.

Review of User Awareness
As has been emphasised throughout this document, user awareness and education is a primary key to success, and should be an on-going activity in any organisation's information security management practice.

Periodic "awareness campaigns" and surveys will serve to gauge the extent to which users have assimilated information security practices.

Review of Security Countermeasures
The review phase should also seek to determine whether the information security countermeasures that have been implemented are adequate, and whether they are best serving the purposes for which they were intended. Examples could include:

- Are the appropriate security devices and events being monitored and logged?
- Is the logging of security devices and events adequate?
- Are the security logs being monitored?
- Are the detection and alerting mechanisms working effectively?
- Are the system hardening checklists being used?
- Are information security standards being adhered to?
- Is the change management procedure being rigorously followed?
- In other words, are the *controls* working?

In summary, the objective of the Review Phase is to answer the following questions:

- How effective is the organization's information security management practice?
- Is the organization doing the right things?
- Have there been changes to the environment that could impact the organization's Risk Profile?
- Are the information security policies adequate? Are they comprehensive?
- How can the information security management practice be improved?

<u>Assessment Phase – Reprise</u>
The return to the Assessment Phase constitutes a second pass of the iterative process of information security management.

Re-visiting the Assessment Phase may be done as a consequence of specific outcomes of the Review Phase, or as an event in the natural course of information security management. Consequently, it may be a lengthy or summary assessment contingent on the outcome of the Review Phase.

Given the evolving nature of the information technology industry, the inherent insecurities of both the TCP-IP protocol, and weaknesses in current system development standards and methodologies, and in the ever-increasing numbers of threat vectors, it is safe to assume that a re-assessment of the organisation' information security posture will be necessary.

Conclusion

While the development and implementation of a formalized ISMP may appear to be a daunting undertaking, its importance to an organization cannot be overstated.

Furthermore, it is hoped that a number of simple countermeasures indicated herein and elsewhere will have served to remove some of the misperceptions of complexity.

Information security practices appear to have struck some chord of harmony within the information technology community – perhaps an acknowledgement of a common and interrelated plight. Consequently, and otherwise, vast amounts of knowledge and expertise are available in the public domain.

All that remains is the implementation of a pragmatic information security management practice.

List of References

[1] National Institute of Standards and Technology
URL: http://csrc.nist.gov

[2] Pipkin, Donald L.
2000
Information Security: Protecting the Global Enterprise
Prentice-Hall PTR
ISBN 0-13-017323-1

[3] International Standard ISO/IEC 17799, Information Security Management, Code of Practice for Information Security Management – Frequently Asked Questions
URL: http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf

[4] Australian Standard Handbook of Information Security Risk Management
URL: http://www.riskmanagement.com.au/

[5] Government of Canada, Communications Security Establishment Knowledge Centre
URL: http://www.cse-cst.gc.ca/en/knowledge_centre/publications/manuals/MG-2.html

[6] Editors: Harold F. Tipton / Micki Krause
2002
Information Security Management Handbook
Volume 3
4th Edition
Auerbach Publications
ISBN 0-8493-1127-6

[7] Benefits of Security Risk Analysis
URL: http://www.iso17799software.com/riskben.htm

[8] ISO 17799: What is it?
URL: http://www.iso17799software.com/what.htm

[9] Allen, Julia H.
2001
The CERT® Guide to System and Network Security Practices
Addison-Wesley
ISBN 0-201-73723-X

[10] Garfinkel, Simson / Spafford, Gene
1996
Practical UNIX & Internet Security
2nd Edition
O'Reilly & Associates, Inc
ISBN 1-56592-148-8

[11] United States General Accounting Office
URL: http://www.gao.gov/

[12] Tripwire, Inc.
URL: http://www.tripwiresecurity.com/

[13] SNORT Open Source IDS
URL: http://www.snort.org/

[14] ManHunt by Recourse Technologies
URL: http://www.recourse.com

[15] Network Security Library
URL: http://secinf.net/info/ids/nvh_ids/

[16] neuSECURE Threat Management & Security Operations Software by GuardedNet
URL: http://www.guarded.net/products/products.htm

[17] ePolicy Orchestrator by McAfee Security
URL: http://www.mcafeeb2b.com/products/epolicy/default-management-solution.asp

[18] CERT Co-ordination Centre: Responding to Intrusions
URL: http://www.cert.org/security-improvement/modules/m06.html

Information Resources

[19] Microsoft Windows 2000 Security Services
URL: http://www.microsoft.com/windows2000/technologies/security/default.asp

[20] National Security Agency – Security Recommendation Guides
URL: http://nsa2.www.conxion.com/

[21] Standards Australia Risk Management Portal
URL: http://www.riskmanagement.com.au/

[22] Electronic Privacy Information Centre (EPIC)
URL: http://www.epic.org/

[23] Federal Information Processing Standards Publications
URL: http://www.itl.nist.gov/fipspubs/

[24] Computer Virus Help (by Henri Delger)
URL: http://pages.prodigy.net/henri_delger/index.htm

[25] Symantec Security Response White Papers
URL: http://securityresponse.symantec.com/avcenter/whitepapers.html

[26] Norberg, Stefan
2001
Securing Windows NT/2000 Servers
1st Edition
O'Reilly & Associates, Inc
ISBN 1-56592-768-0