Global Information Assurance Certification Paper

An approach to building an integrated information/information technology security management program and security architecture.

In partial fulfillment of the requirements of the Global Information Assurance Certification, Security Essentials Certification

GSEC Practical Assignment v 1.4b, Option 1

Andrew Hughes, June 2003

Table of Contents

Abstract

The requirement for formal Information and Information Technology Security Management Programs is becoming commonplace in government and private sector industries to meet regulatory or legislative requirements.

This paper presents an approach for operations-focused departments to build an effective security management program with integrated security operations, security architecture, risk management and security audit functions. Methods to integrate the security management program activities into the normal, pre-existing practices of the organization are discussed.

Introduction

Information systems departments with informal or ad hoc security practices are being challenged by increasing regulatory requirements to implement comprehensive security management programs.

The requirement for formal Information and Information Technology Security Management Programs is becoming more commonplace in the public and private sectors to meet regulatory or legislative requirements. (See appendix A)

Design and implementation of a formal security management program for an organization is a daunting task and at risk of poor uptake if not adequately integrated into the processes of the organization. Departments focused on security operations and day-to-day tasks are particularly susceptible to the risk that the daily operations tasks will consume all available time, thus stunting the development of improved process.

Objective

This paper presents an approach for operations-focused departments to build an effective security management program with integrated security operations, security architecture, risk management and security audit functions.

Definition of a new methodology or paradigm in information security is not the objective of this paper. Rather, a practical approach is described to integrate an organization's existing methodologies and approaches into a comprehensive, achievable program.

A proposed Security Management program structure is first described. The security program contains key functional areas for security management: security operations, security architecture, risk management and audit. The functional areas are not fully elaborated – it remains for the individual organization to develop each area to suit their specific requirements, or to use an established methodology.

The security program is structured in a way that allows momentum to be derived from existing functions and triggers. Key integration points or checkpoints are indicated. These checkpoints allow the security program to be tied into existing operational process, ensuring that the vitality of the program is maintained.

Proposed model for a Security Management Program

In this Security Management Program model, the functional elements of IT security management are assembled into four key areas: Risk Assessment, Security Architecture, Security Operations and Security Audit.

The security program is constructed with identified interfaces, triggers and information exchanges between the functional areas primarily to simplify interaction with the program.

Rationale for program structure

This arrangement of the security management program is deliberately structured to recognize strong security operations. It assumes that risk assessment, security architecture/standards and security audit are relatively weak in the organization.

Operations activities are used to drive out and build the security architecture by identifying small focus areas that require risk assessment. The approach described here allows the operations-oriented organization to define focus areas for security analysis and treatment, and to collect the work results into the Security Architecture for future use.

In the author's experience working with small to medium sized government organizations with limited resources, these types of organizations tend to focus on operational aspects of daily security management rather than on building the security architecture and risk assessment functions. Account management, patches and antivirus controls are top of mind and so receive the bulk of effort. The specification of secure standards and use of IT risk management process is rare.

As external triggers occur and the internal environment increases in complexity, the organizations consume more time reacting and struggle with conflicting standards and designs imposed from external sources.

Use of focus areas to drive artifact development

A powerful method of structuring security program activities is to define Focus Areas that require treatment.

A focus area has clearly defined boundaries and may consist of a technology, product, system or application. The work result or artifact set of focus area development will be policy, standards, practices and guidelines. These artifacts are then added to the architecture repository and the security operations procedures.

The focus area allows the security program to create the integrated artifact set that ties the risk assessment, security architecture and security operations areas together. It allows incremental creation of business-driven topics. It avoids building entire sets of artifact types, such as all standards or all security policies, all at once.

Identification of a focus area normally will be caused by a security program trigger.

For example, if the organization chooses to procure wireless personal digital assistant (PDA) devices such as BlackBerry PDAs for staff, a security program trigger would occur as part of normal infrastructure procurement.

A focus area that examines the use of wireless PDAs in the organization would be declared. Research, risk assessment, policy, standards, user guidelines and operations guides would be created and added to the security architecture repository and the security operations procedure set.

By defining and developing the focus area, the security program can deliver useful, on-demand results to the organization and rapid progress can be achieved.

Security Management Program overview

There are four major IT Security Services functions within the proposed IT Security Program: Architecture, Risk Assessment, Operations and Audit.

IT Security Architecture sets policy and standards that govern the implementation, activities and operations of IT resources and people. In this discussion paper, the architecture is considered to be the set of blueprints, design patterns and organizational rules or policies.

The security architecture is the repository of organizational knowledge about security technology as derived from the other security services functional areas. It looks at strategic directions and aligns the organization to security technologies. It is the interface to external stakeholder groups.

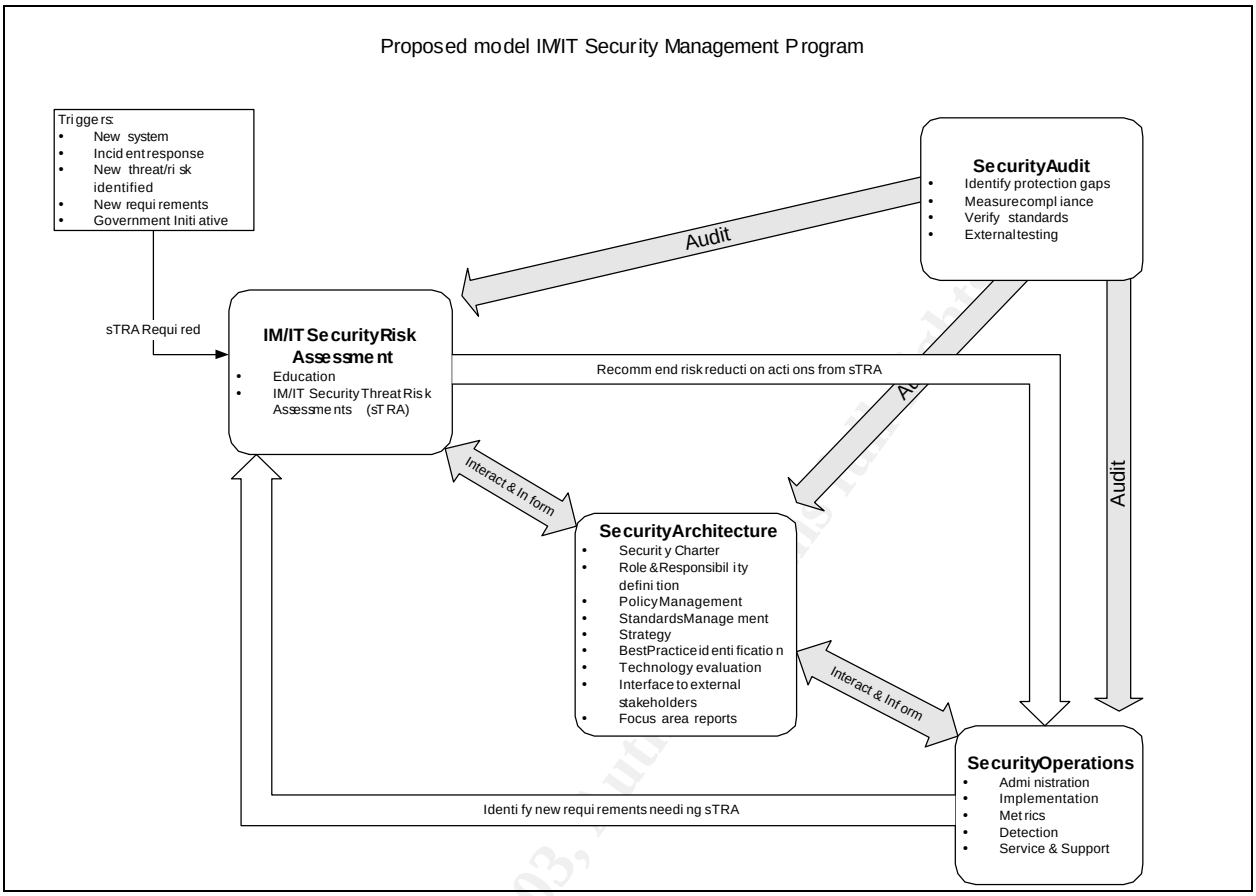
The **IT Security Risk Assessment** area assesses and manages IT security risk. It performs Threat-Risk Assessments to evaluate existing and proposed systems. It promotes good security practices to improve the effectiveness of Security Operations.

"Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions" (Stoneburner, p 4). By implementing a security risk management function, the organization gains awareness and control of IT security threats and risks. It is the key entry point into the security program.

IT Security Operations is concerned with security administration, implementation, detection, troubleshooting and metrics. Security Operations tends to be the most developed functional area due to daily necessity.

IT Security Audit tests the organization's environment for compliance to the policies, standards and practices set out by the Security Architecture. The Security Architecture is also audited for compliance to external requirements, regulations and legislation. The audit function may use internal, external or contracted resources.

The following diagram shows the interrelationships between the four functional areas.



IT Security Architecture

Description

IT Security Architecture defines policy and standards that govern the implementation of IT resources and actions of people. It looks at strategic directions and aligns the organization to security technologies. It is the interface to external stakeholder groups.

Key activities

The person managing the security architecture:

- Defines, maintains and improves the IT Security Management Program
- Defines the IT Security Program Charter (Scholtz, p. 15) which includes statement of Security Principles
- Defines roles and responsibilities for IT security management
- Manages security policy (create, update internal policy, cross-reference to external policy)
- Sets standards of security features and configurations

- Evaluates new technology
- Devises security strategies
- Identifies security best practices
- Assists the organization to define information and asset classifications
- Defines focus areas that require treatment by the security program

Key Artifacts

These key documents and artifacts are the result of the activities above. They are published within the organization to allow sponsors to see the results of the security services functions and to allow other groups within the organization to interact efficiently with security services. The artifacts form the reference body of knowledge that captures the organization's experience in IT security.

IT SECURITY PROGRAM CHARTER

A document that:

- Articulates the fundamental security principles at the organization. Generally accepted system security principles can be found in the NIST Special Publication SP800-14 (Swanson, 4-10)
- Identifies the stakeholders in IT Security
- Defines IT Security roles and responsibilities
- Identifies the key business drivers for IT Security

The Security Program Charter sets the stage for IT Security in the organization. All security functions will be built according to the principles and drivers outlined in the Charter.

SECURITY POLICY INDEX

The security policy index lists the relevant external policies and regulations that the organization must adhere to. This is especially significant where the organization is a division within a larger body – there are normally Federal, statewide, provincial or corporate policies that constrain local policy.

The policy index also shows locally developed security policy and acts as a reference for users, administrators and management.

SECURITY POLICIES

A document set that:

- Expresses the policy decisions surrounding use of Information and Information Technology at the organization

Policies are the formal statements or rules that govern the actions of workers who have access to the organization's information assets. Policy can serve to specify how to conform to legislation or inform workers of organizational requirements (Fraser, p 7-8).

Policy must be clear, able to be followed and enforceable. Clear policy violation consequences must be stated. (Fraser, p 8)

To ensure successful creation and adoption of policy, a stable, efficient approval process is required. Also, wide publication of policies through a user awareness program is essential.

TECHNOLOGY AND DESIGN STANDARDS, DESIGN PATTERNS

Document set that is used by the operations groups to implement and manage technology. The Standards documents are owned and stored in the Security Architecture repository.

The documents reflect the current practices of the operations groups and are intended to be practical, implementable reference documents.

Some common standard sets:

- Software/hardware manufacturer/version standards
- Product configuration standards
- Design patterns for specific technology implementations

INFORMATION CLASSIFICATION GUIDELINE

Consistent and accurate information classification is a cornerstone of the risk assessment process (Peltier, p 4-5).

BEST PRACTICES REPORTS

From time to time, best practices reports will be issued from the Security Architecture area. These reports describe the industry best practices concerning a specific topic area. They are adjusted to suit the organization's internal practices.

For example, best practices reports may be written for server/workstation patch handling, remote access and security incident response.

The concept is to define the organization's standard practices, keeping in mind industry best practice.

FOCUS AREA REPORTS

As focus areas are identified and declared, the focus area report presents the background and research results.

During focus area definition, the various elements required to support the focus area are listed. If there are policy, standards or guidelines already existing, the report lists them. If not, the report indicates that they must be developed.

The concept is to publish the focus area report to allow the organization to see the security treatments required for that focus area. This raises the visibility of both the focus area topic and the security management program.

Security Risk Assessment

Description

The IT Security Risk Assessment area assesses and makes recommendations to reduce IT security risk.

Risk analysis and management should be a core principle of IT Security at the organization. Risk analysis uses threat/vulnerability identification combined with likelihood and impact assessment to articulate the business risk.

The Security Risk Assessment area informs the Security Architecture of new vulnerabilities, threats and risks. This ensures that the Architecture evolves to meet new requirements.

In this model, the Security Risk Assessment area is responsible for the promotion of Security within the organization. This includes a user awareness program and guidance to developers for implementation of best practices.

It performs Threat-Risk Assessments to evaluate existing and proposed systems.

It promotes security practices that improve the effectiveness of Security Operations. By implementing a security risk assessment function, the organization gains awareness and control of IT security threats and risks.

The key tool that guides the interaction with applications and system owners is the Threat-Risk Assessment (TRA). The TRA contains a structured questionnaire that assists owners to articulate asset values, threats, vulnerabilities and impact. Many threat-risk assessment methodologies and guides exist. Examples include NIST Special Publication 800-30 (Stoneburner), Software Engineering Institute OCTAVE Framework (Alberts), Information Security Risk Analysis (Peltier), Government of Canada Communications Security Establishment Threat and Risk Assessment working guide (Communications Security Establishment).

Key activities

The key activities of the IT Security Risk assessment area:

- Development and customization of Security Threat-Risk Assessment guidelines
- IT Security threat-risk assessments
- Education and awareness program definition
- Security presentations to management and executive
- Promotion of best practices

Key artifacts

These key documents and artifacts are the result of the key activities above. They are published within the organization to allow business owners to see the results of the security services functions and to allow other groups within the organization to interact efficiently with security services.

IT SECURITY THREAT-RISK ASSESSMENT GUIDELINES

- Describes the standards, methods, templates and criteria to be used to assess security risks
- Many security risk assessment methodologies exist. The organization should adopt and customize a methodology suitable to the size and complexity requirements.

IT SECURITY THREAT-RISK ASSESSMENT REPORTS

For each significant IT system or information asset, regular Security Threat-Risk Assessments should be performed

SECURITY AWARENESS PROGRAM DESCRIPTION

- Describes the communications and training that make up the security awareness program
- Describes the documents and tools required to deliver training

RISK ASSESSMENT CONSULTING

- As required, the Risk Assessment area will consult with project teams, program areas and management on topics related to risk management.

Interface to other Security Program Functional Areas

The Security Risk Assessment area recommends changes to systems based on Security Threat-Risk Analysis (TRA). The approved recommendations are passed to Security Operations for implementation.

Risk Assessment receives change notification from Security Operations for any significant changes to the operating environment such as requests for new application deployments, requests for new infrastructure or major infrastructure change requests. If appropriate, Risk Assessment then performs a TRA.

External triggers can cause Security Risk Assessment actions. These include: identification of new threats, new external requirements and response to incidents.

Changes in the Security Architecture components will cause risk assessment to update user awareness messages and assessment criteria within the TRA.

Security Risk Assessment informs the Security Architect of the actions recommended to Security Operations, for potential modification of the Architecture.

Security Operations

Description

IT Security Operations is concerned with security administration, implementation, detection, troubleshooting and metrics.

Operations takes recommendations from the Risk Assessment function and implements them.

Key activities

Security Operations activities include:

- Access control administration
- Disaster recovery preparation
- Technology implementation
- Implementation of Risk Assessment recommendations
- Troubleshooting / Service & Support
- Incident detection and response
- Security metrics

Key artifacts

These key documents and artifacts are the result of the key activities above. They are published within the organization to allow business owners to see the results of the security services functions and to allow other groups within the organization to interact efficiently with security services.

DELIVERY OF SERVICES

The primary function of Operations is service delivery. The outcomes are the configured systems or accounts rather than reports or documents.

OPERATIONS GUIDES AND DOCUMENTATION

These documents are used by technical and administration staff to ensure consistent application of policies, standards and practices.

- Detailed documentation on procedures
- Detailed configuration and installation documentation
- Operations guides for systems

IMPLEMENTATION AND CHANGE MANAGEMENT DOCUMENTATION

- Change and implementation plans

INCIDENT REPORTS

- Details of specific security incidents and actions taken in response

METRICS REPORT

- Report of volumes of detected security events

Interface to other Security Program Functional Areas

The Security Operations group receives security risk reduction recommendations from the Security Risk Assessment group for implementation.

The Security Operations group identifies new technologies or systems and alerts the Risk Assessment group of substantial changes to the environment. The Risk

Assessment group then decides whether to conduct a Security Threat-Risk Assessment.

Security Operations is responsible for ensuring that any standards, policies and practices defined by the Security Architect are implemented and administered efficiently and correctly.

Security Operations informs the Security Architect of changes to the operating environment to allow the architect to update the Security Architecture as needed.

Security Audit

Description

Security Audit tests the organization's environment for compliance to the policies, standards and practices set out by the Security Architecture. The Security Architecture is also audited for compliance to external requirements. The audit function may use internal, external or contracted resources.

The Audit function is more stringent than the basic verification and compliance activities within the other functional areas. Reports are produced that identify implementation or design gaps in the other functional areas.

Missing or inappropriately implemented security controls are identified.

The Audit team also assesses control gaps in the controls applied to system administrators and operators.

Audit is a key tool to ensure that controls are implemented effectively.

Key activities

Security Audit activities include:

- Process audits
- Implementation audits
- Standards audit

Key Artifacts

These key documents and artifacts are the result of the key activities above.

AUDIT REPORTS

Reports that identify the system under review, the standards used to measure against and gaps between implemented configuration and standard configuration.

Interface to other Security Program Functional Areas

Formal audits should be performed regularly on a defined schedule or in response to regulatory or legislative requirements.

Integration points for Security Management Program

To ensure the vitality and momentum of the security management program, key integration points are indicated. These integration points should be triggers within other existing processes in the organization. When a trigger is encountered, the appropriate Security Management Program activity should occur.

The table shows the key activities of the security management program listed in the previous sections and what might trigger them. It is not a complete listing, but should serve to illustrate the integration points.

Key Activity	Program area	Possible triggers
Define focus area for treatment	Architecture	- New focus area being developed by the organization. E.G. if wireless PDA's are being introduced to the organization for the first time, a focus area would be defined.
Manage security policies	Architecture	- Part of the focus area development workflow – new focus area requires policy to govern new activities
Set security configuration standards	Architecture	- Part of the focus area development workflow - Operations planning for implementation of new technology
New technology evaluation	Architecture	- Procurement process informs Security Management Program of new technology purchase requirement
Perform IT threat and risk assessment	Risk Assessment	- Part of the focus area development workflow - Response to a security incident - New product implementation - Major changes to the operating environment - New external requirements - SDLC process reaches the appropriate point for risk assessment trigger

Implement new security controls	Operations	- Risk assessment report recommendations for improvements
Security Audit	Audit	- Regulatory requirement to perform regular audits

Examples of common business processes that trigger Security Management Program activity are: package procurement, package development, package implementation, project management office activities, data sharing agreements/interactions, incident handling, operational process improvement (from metrics trending) and regulatory/legislative compliance activity.

The majority of these triggers enter the Security Management Program cycle at the Risk Assessment function. For example:

- As a part of package evaluation and selection, the package should be assessed to determine that it fits the organization's risk acceptance measures.
- A required step in application development projects should be to conduct risk assessment early in the design/development phases, with followup assessments during implementation and operation phases. (Stoneburner, p. 5)
- Changes to regulations or legislation may trigger a high-level compliance study to discover where the organization needs to spend effort to come into compliance

The proposed approach to build the integrated program

Now that a Security Management Program structure has been proposed, the challenge of building and implementing it remains.

There are many approaches to building parts of or entire security management programs (Fraser, Treasury Board of Canada Secretariat, Scholtz) . Not surprisingly, they tend to share similar steps: 1) gain business sponsorship, 2) define the requirements, 3) plan the implementation, 4) execute the plan, starting with an overall threat risk assessment.

The proposed approach is designed to ensure that there are sufficient triggers to maintain a source of momentum.

This is done by:

- Establishing the security program framework first
- Performing the overall threat risk assessment to define an overall list of focus areas
- Developing each focus area in turn
- Watching for triggers that would cause new focus areas to be defined
- Delivering the focus areas in priority order as defined by the business

The approach

There are two key phases during security program development: 1) initiation and 2) execution.

The initiation phase is used to confirm the business requirements and form the framework that will hold the artifacts and activities of the security management program. It defines the key interfaces within the security program and to other business processes.

The execution phase builds the knowledge and artifact repository in the security architecture. As triggers or requests for security service occur (primarily for risk assessment), focus areas are defined and policy, standards, risk assessment, guidelines and user awareness activities may occur.

Initiation phase

START WITH THE CLEARLY DEFINED BUSINESS NEED

Although the IT security community is convinced of the intrinsic value of security management, unless there is a specific tangible benefit to the organization, it will be difficult to gain support.

Triggers such as regulatory/legislative requirements, security breach or an external security audit can provide the initial push to create a security management program (ISO/IEC 17799:2000, p. ix).

IDENTIFY AND RECRUIT A BUSINESS SPONSOR

Management sponsorship for development of a formalized program is crucial for long term program viability. Typically, the chief information officer or chief financial officer has the largest stake in an effective security management program. Work with the business sponsor to develop a business case, using risk management principles.

CHARTER THE PROGRAM

Define a Security Program Charter for the organization that sets out the security principles, management sponsorship, roles, responsibilities, approval process and business drivers for the Security Management program (Scholtz, p. 15).

This document should be brief and serve as a central reference against which all the security management programs are compared.

DEFINE AN INITIAL IMPLEMENTATION PLAN

To establish the Security Management program, some initial work must be done to form the framework. Items such as the Security Program Charter, security program description, communications plan, risk assessment methods, policy index and functional area interaction points must be defined first.

Create an implementation plan for the framework with early, achievable goals. Plan to iterate through versions of the framework elements, refining over time.

If it has not been done already, use a high-level threat-risk assessment to determine which areas are most important for the organization to focus on.

COMMUNICATE AND MARKET THE SECURITY MANAGEMENT PROGRAM

Publicize the services and artifacts of the Security Management Program. Some of the artifacts listed in the program definition section are intended to be reference guides for operators, developers and business area owners.

Establish the points where organizational processes must interact with the security management program. For example, prior to production implementation of a product, a security threat risk assessment is mandatory.

Establish the points where organizational processes can optionally interact with the security management program. For example, during software development projects, the project manager should request security assessments at appropriate phases. In any case, prior to production implementation, a final security assessment is mandatory.

Parts of the organization that are required to pass the security assessment phase will learn quickly that it is in the organization's best interest to involve the security management program as early as possible in their business cycle.

Execution phase

WATCH FOR TRIGGERS

Watch for security program triggers and engage new focus area as early as possible. Triggers such as new development projects or procurement process will greatly benefit by early interaction with the risk assessment and security architecture areas.

DEVELOP AND DESCRIBE FOCUS AREAS

The focus area is the central object of attention in the proposed security management program structure. Focus areas are identified by various triggers such as security breaches, results of risk assessment or procurement activity.

Focus areas permit quick delivery of results as they are required by the organization.

COMMUNICATE AND MARKET THE SECURITY MANAGEMENT PROGRAM

Communications is key. Continue to publicize the services and artifacts of the program to ensure that the services are sought at the correct times by the organization.

As new focus areas are developed, policy, standards, risk assessments and guidelines will be written. Creating awareness of these new program deliverables within the organization will maximize their benefit.

Critical success factors

The following are critical success factors for implementation of a successful security management program.

- Frequent and effective communications with all stakeholders
- Management support and commitment
- Production of *usable* assessments, guidelines and standards
- Focus on delivery of services rather than controlling the activities of the organization
- Integration with non-security activities like procurement or application development projects to raise awareness and maintain momentum
- Leverage existing security activities such as Operations to maintain momentum for building other areas such as risk assessment and architecture

Conclusion

As regulation and legislation become more common for security and privacy of information, more organizations will be required to implement security programs and plans. The proposed approach described in this research paper has identified simple methods of integrating security management program steps into normal, pre-existing practices, thus gaining and keeping security program vitality and momentum.

List of References

Alberts, Christopher and Audrey Dorofee. “An Introduction to the OCTAVE[SM] Method.” 30 January 2001. URL: http://www.cert.org/octave/methodintro.html (7 June 2003)

Fraser, B. “RFC 2196: Site Security Handbook”. September 1997. URL: http://www.ietf.org/rfc/rfc2196.txt?number=2196 (7 June 2003)

Communications Security Establishment, Government of Canada. “Threat and Risk Assessment working guide”. October 1999. URL: http://www.cse.dnd.ca/en/documents/knowledge_centre/government_publications/itsg/ITSG-04e.pdf (7 June 2003)

Treasury Board Secretariat, Government of Canada. “Government Security Policy.” 1 February 2002. URL: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg1_e.asp (7 June 2003)

Treasury Board Secretariat, Government of Canada. “Information Technology Security Standard.” 1 June 1995. URL: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp (7 June 2003)

ISO/IEC 17799:2000 “Information technology – code of practice for information security management”. Geneva: ISO, 2000.

Ministry of Finance, Province of British Columbia. “Core Policy Manual Chapter 15.” URL: http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/15_Security.htm (7 June 2003)

Office of Management and Budget. “Management of Federal Information Resources.” Circular A-130 Transmittal Memorandum #4. 28 November 2000. URL: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html (7 June 2003)

Peltier, Thomas R. *Information Security Risk Analysis*. Boca Raton: CRC Press LLC. 2001.

Scholtz, Tom. “Making Information Security Policy Effective.” 19 July 2002. URL: http://www.metasecuritygroup.com/library/whitepapers/MakingInformationSecurityPolicyEffective-METASecurityGroupInformationSecurityPolicyFramework.pdf (7 June 2003)

Stoneburner, Gary, Alice Goguen and Alexis Feringa. “Risk Management Guide for Information Technology Systems.” NIST Special Publication 800-30. October 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (7 June 2003)

Swanson, Marianne, and Barbara Guttman. “Generally Accepted Principles and Practices for Securing Information Technology Systems.” NIST Special Publication 800-14. September 1996. URL: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf (7 June 2003)

Weil, Steven. “HIPPA Consensus Research Project.” The SANS Institute. URL: http://www.sans.org/projects/hipaa.php (7 June 2003)

Worthen, Ben. “How to Meet Tomorrow’s Privacy Rules Today.” CIO Magazine. 1 November 2002. URL: http://www.cio.com/archive/110102/rules.html (7 June 2003)

Appendices

Appendix A

The table shows sources of further information regarding government or industry regulations or legislation for establishing information security management programs. Most requirements are related to the protection of privacy and the control frameworks needed to provide adequate protection.

Organization/Industry	Example regulations, requirements or summaries
US Government	▪ http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html ("Management of Federal Information Resources", Office of Management and Budget Circular A-130) ▪ http://csrc.nist.gov/policies ("Federal Requirements", Computer Security Resource Center, NIST)
US Healthcare	▪ http://www.sans.org/projects/hipaa.php (Weil, "HIPAA Consensus Research Project")
Various, including: US healthcare, US Financial Services Industry, US Public sector	▪ http://www.cio.com/archive/110102/rules.html (Worthen, "How to Meet Tomorrow's Privacy Rules Today")
Government of British Columbia	▪ http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/15_Security.htm (Ministry of Finance, Core Policy Manual Chapter 15)
Government of Canada	▪ http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg1_e.asp (Government Security Policy, Section 10.1)