IT Governance: The benefits of an Information Security Management System

Katerina Cai, CISSP
Hewlett-Packard
Speaker Biography

• Solution architect in the HP European security consulting practice
• 5 years experience in PKI, smart cards, SSO and security IT governance domain
• Worked on BS 7799 certification project for HP managed services Europe
Agenda

- What is an Information Security Management System (ISMS)?
- The Ten ISO 17799 Control Domains
- Do’s and Don’ts
- Commercial tools available
- BS 7799 Certification
IT Governance

- Business Management + IT management
- Controlling the risk ≠ technological solutions
- Complex/detailed yet apply across industries
- control the formulation and implementation of IT strategy and guide it in the proper direction for the purpose of achieving competitive advantages for the corporation
Today’s Reality

So Many Corporate Assets, So Little Protection

Legal Liability
Espionage
Tarnished Reputation

Enterprise Resources

Customer
Other Vendors

Network

INTERNET
EXTRANET
INTRANET

Applications
Data

Server

Web, App, Data Servers
Storage Farm

Remote Worker
Office Workgroup

Branch Offices

Thief

Vandalism
What is an ISMS?

- Framework to manage the security risks within an organization

- Highlights
  - Security policy
  - Organizational setup for security personnel
  - Risk assessment and management methodology
  - Controls and how they are implemented
  - Regular review
  - Proper documentation
Plan-Do-Check-Act Process Model (PDCA)

- **Plan**
  - Establish ISMS Context & Risk Assessment
  - Design & Implement ISMS
  - Monitor & Review ISMS

- **Do**
  - Development, Maintenance & Improvement Cycle
  - Improve ISMS

- **Check**

- **Act**
  - Managed Information Security
  - Interested Parties

Interested Parties
- Information Security Requirements & Expectations
High Level Information Security Policy

• Who?
  – Who is issuing the policy and who must abide by it.

• Where?
  – Scope of the policy

• What?
  – Preserving the confidentiality, integrity and availability of information

• Why?
  – Business factors and nature of threats
Security Organization

• Appropriate personnel to manage security within the organization
• Information security manager
• Proper allocation of information security responsibility
• The management information security forum
  – If necessary cross-functional
  – Separate from operation and report directly to management
Asset List

- Assets that contribute to the fundamental business of the organization in scope

- Examples of asset include:
  - Information assets
  - Paper documents
  - Software assets
  - Physical assets
  - People
  - Company image and reputation
  - Services

- High level asset definition
  - i.e. group all routers together under heading routers

- Prioritize the assets with high, medium and low
Risk Assessment

• No one mandatory risk assessment methodology
• Choice of methodology depends on the organization
• Three questions for each major asset group in the asset list
  – Potential threats
  – Potential vulnerabilities
  – Current controls in place
• One of the most important and time consuming step
Risk Management

- No mandatory risk management methodology
- Choose one of the four approaches below for identified risks
  - Accept
  - Mitigate
  - Avoid
  - Transfer
- Must have management support and sign-off
What is an ISMS?

• Framework to manage the security risks within an organization

• Highlights
  – Security policy
  – Organizational setup for security personnel
  – Risk assessment and management methodology
  – Controls and how they are implemented
  – Regular review
  – Proper documentation
ISO17799 Control Domains

1) Security policy
2) Security organisation
3) Asset classification and control
4) Personnel security
5) Physical and environmental security
6) Communications and operations security
7) System access control
8) System development and maintenance
9) Business Continuity Planning (BCP)
10) Compliance
Security Policy

- Ensure support from management in securing an organization
  - Existence of a security policy
  - Regular review and update of policy
Security Organisation

• Management of information security within the organization
  – There should be adequate information security staff as well as proper procedures to approve information security procedures.

• Maintenance of the information security standard when outsourcing

• Control of information security when the organization is accessed by a third party
Asset Classification & Control

• Assets
  – Information assets
  – Paper documents
  – Software assets
  – Physical assets
  – People
  – Company image and reputation
  – Services

• Classifies them correctly in order to provide an adequate level of protection
• Necessary for the risk assessment
Personnel Security

- Security in job definition and resource assignment
- Appropriate information security training
- Appropriate handling and reporting of security incidents and malfunctions
  - Similar to ITSM incident management
Physical and Environmental Security

- Secure areas to prevent holes in physical perimeters
- Equipment security to prevent harm to an organization’s physical assets
- General controls related to physical security
  - Clear desk clear screen
  - Removal of property
Communications and Operations Security

• Operations
  – Correct and secure operation of the organization
  – System planning and acceptance to minimize the risk of systems failure
  – Protection against malicious software
  – Secure handling of media in order to avoid damage

• Communications
  – Network management
  – Exchanges of information and software in transit, electronically, etc

• Both
  • Maintaining availability and traceability of information, i.e. good housekeeping
System Access Control

- The existence of an access control policy
- User access management
- User responsibilities (password use and equipment)
- Network access control
  - Complementary to network control in previous section
- Operating system access control
- Application access control
- Monitoring system access and use
  - Ensure adequate logging
- Mobile computing and teleworking
  - Ensure correct authorization and authentication when working remotely
System Development & Maintenance

- Security requirements of systems
  - The business should specify security requirements along with other requirements

- Security in application systems
  - Avoid misuse or loss of user data

- Cryptographic controls in system development

- Security of information used in development
  - Protection of system test data
  - Access control to program source libraries

- Security in development and support processes
  - Change control procedures
  - Technical review of operating systems or software packages change
Business Continuity Planning (BCP)

- Organizations must have a process for creating, testing and updating the BCP
  - Analysis possible risks
  - Establish framework
  - Write plan
  - Test, maintain and reassess on a continuous basis
Compliance

• Compliance with legal requirements
  – Intellectual property laws, data protection and privacy laws, cryptographic regulations, etc

• Reviews of security policy and technical compliance
  – Making sure that the system is compliant with policy and industry standards

• Efficiency and effectiveness of the system audit
ISO17799 Control Domains

- Security policy
- Security organisation
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations security
- System access control
- System development and maintenance
- Business Continuity Planning (BCP)
- Compliance
Documentation and Audit

• Documentation
  – Consistent format
  – Accessible to relevant parties - online

• Audit
  – Third party is the best
  – Internal and self assessment also acceptable
Do’s

• Plan before doing
• Limit scope
  – define clearly the scope of the ISMS
• Get buy-in from all functions
  – an approach to implementing security that is consistent with the organisational culture
  – security policy, objectives and activities that reflect business objectives
• Educate and communicate
  – Effective marketing of security to all managers and employees
  – Distribute guidance on information security policy and standards to all employees and contractors
  – Provide appropriate training and education
Don’ts

• Design, document and then let it rot
• Let technology dictate
• Follow textbook
• Get stuck on details
• Manage every risk
  – Accept when cost of managing risk is higher than accepting it
Commercial tools

• CobiT
  – Control Objectives for Information and Related Technology

• COBRA
  – Contains Risk assessment and control compliance

• Octave
  – Operationally Critical Threat, Asset, and Vulnerability Evaluation

• ASSET (NIST)
  – Free, developed by government

• Documentation specific to ISO 17799
  – GMITS
  – PD 3000
BS 7799

- Derived from ISO 17799
- Specification for designing, documenting and implementing an ISMS – more important than controls
- Basis for certification
Case study - HP Managed Services EMEA

• Why obtain certification?
  – Customer demand
  – Reduce internal cost of managing security

• Advantages
  – Adapt ISMS as the security plan for all delivery centers
  – Incorporate BS 7799 requirements into performance measurements

• Difficulties
  – Fit already existing model into BS 7799 framework
  – Define a clear scope

• Future
  – Certify all delivery centers
Summary

- ISMS is a framework for managing RISK in enterprise (PDCA)
- Risk assessment & Risk Management
- Start small, plan before doing, and educate
- ISO 17799 Ten control domains
- BS 7799 Certification
Thank you

Katerina Cai
Hewlett-Packard
Bibliography

- IT Governance: Data Security & BS 7799/ISO 17799 by Alan Calder and Steve Watkins 2002
Backup slides