

**Risk Management MN220:
Seminar 7: IT Risk**



SHERIDAN COLLEGE

PERTH | WESTERN AUSTRALIA

Information security risk management

- Introduction
- History
- Information technology
- Information security
- Risks, threats and vulnerabilities
- History of the Internet
- Information security risk management
- Standards (**AS/NZS ISO/IEC 27001:2013, COBIT**)
- Information security management system (ISMS)
- Case study

New threats in Organisational information Security

<https://www.youtube.com/watch?v=nMBFgwb-4h4>

Risk that sometimes occur!



History

- IT systems were standalone
- Risk assessments focused on technical vulnerabilities
- IT risk assessment was the domain of IT professionals
- IT systems have become interconnected
- The Internet has connected the world increasing the vulnerabilities in information security

Information technology

1980's PC - IBM 286-10Mhz, 5MB RAM

1990's Internet connection - 4.4 Kbps dialup connection

2000's PC - Pentium- 3Ghz, 4-16 Gigabit RAM

2000's Internet connection - 2 Mbps asynchronous broadband

National Broadband Network (NBN)

Information security

- Information is available on numerous computer systems
- Information is distributed widely
- Many people have access to more information
- Privacy is now a greater issue (with respect to electronic records)
- The legal framework has changed

What is information?

*“Information is an **asset** which, like other important assets, has **value** to an organisation and consequently **needs to be suitably protected.**” ¹*

- 1 AS/NZS ISO/IEC 17799:2006 Information technology – Security techniques –Code of practice for information security management.

What is information security?

*“Preservation of **confidentiality**, **integrity** and **availability** of information; in addition, other properties, such as **authenticity**, **accountability**, **non-repudiation**, and **reliability** can also be involved.” 2*

- 2 AS/NZS ISO/IEC 17799:2006 Information technology –Security techniques –Code of practice for information security management.

Enterprise information security

Biggest Information Security Breaches

- <http://www.csoonline.com/article/2130877/data-protectionhe-15-worst-data-security-breaches-/data-protection/the-15-worst-data-security-breaches-of-the-21st-century.html>

EIM- Enterprise Information Management

- <https://www.youtube.com/watch?v=2YnMu3hiGfQ>
- https://www.youtube.com/watch?v=13wV_Qq8YCo
- <https://www.youtube.com/watch?v=9eQuEEKtjHs>

Preservation of information

Confidentiality:

- To ensure information is available to only those with authorisation to access it

Integrity:

- To ensure information and information processing systems remain accurate and complete

Availability:

- To ensure information is available to those with authorisation as and when they require it

Risks, threats, and vulnerabilities³

Risk:

- “Combination of the probability of an event and its consequence.”

Threat:

- “A potential cause of an unwanted incident, which may result in harm to a system or organization.”

Vulnerability:

- “A weakness of an asset or group of assets that can be exploited by one or more threats.”

• 3 AS/NZS ISO/IEC 17799:2006 Information technology –Security techniques –Code of practice for information security management.

Threat types

Natural and accidental threats:

- Non-intentional threats (accidents);
- Earthquakes, fires, floods, lightening.

Malicious threats:

- Intentional threats caused by people, organisations, governments.

Malicious threat agents⁴

Malicious threat agents have the following characteristics:

- Capability
- Motivation
- Catalysts
- Access
- Inhibitors
- Amplifiers

⁴ Jones. A., Ashenden. D., Risk management for computer security

Motivation

Motivation to carry out a threat may arise due to one or a number of the following:

- Personal gain or ambition
- Political interests
- Religious belief
- Power
- Revenge
- Curiosity
- Terrorism

Capability

For threats to be carried out requires capability:

- *A computer hacker needs to have knowledge and skill*
- *The theft of a person's identity requires knowledge and skill*

Therefore threat assessments need to take into consideration the **capabilities** of the **suspected perpetrators**.

Opportunity

For threats to be carried out the opportunity must exist for the attack to take place:

- Open doors;
- **Unattended** systems and computers;
- Easy **electronic access** to information and systems; and
- Weak security systems.

Catalyst

A catalyst is required to cause a threat agent to select a target:

- Disaffected employee;
- Past employee;
- Supplier losing a contract;
- Sub-contractors;
- Change in technology.

Inhibitors

Inhibitors may affect the target or the threat agent:

- Security policy;
- Security systems;
- Physical barriers to the source of information;
- Fear of being caught (threat agent).

Vulnerabilities

Operating systems:

- Identified by “code crackers”
- Manufacturers issue “patches”

Software applications:

- “Easter eggs”

Connectivity and dependence:

- The Internet

History of the Internet

1967 - First packet switched network developed in UK

1969 - ARPANET deployed in USA

1970 - First email system developed

1972 - FTP (File Transfer Protocol) developed

1991 - World Wide Web developed by Sir Tim Berners-Lee and Robert Cailliau.

Downside of the Internet

- Hacking
- Denial of service (DOS) attacks
- Intellectual property theft
- Spying
- Industrial espionage
- Terrorism
- **Phishing** (to obtain confidential information from Internet users, by sending e-mails appearing to be from a legitimate organisation)
- Fraud
- Cyber stalking

AS/NZS ISO/IEC 27002:2006. Information technology – Security techniques – Code of practice for information security management

- 1 Scope
- 2 Terms and definitions
- 3 Structure of Standard
- 4 Risk assessment and treatment
- 5 Security policy
- 6 Organization of information security
- 7 Asset management
- 8 Human resource management

AS/NZS ISO/IEC 27002:2006

- 9 Physical and environmental security
- 10 Communications and operations management
- 11 Access control
- 12 Information systems acquisition, development and maintenance
- 13 Information security incident management
- 14 Business continuity management
- 15 Compliance

Information security risks

- Identify assets;
- Information assets;
- Paper documents;
- Software assets;
- Physical assets;
- Marketing assets;
- Services.

IT SECURITY RISK ASSESSMENT

Part 2- <https://www.youtube.com/watch?v=rrbX0cWqE6E>

Part 3- <https://www.youtube.com/watch?v=CaC83WG3zUo>

Threats and vulnerabilities

Identify threats to the business:

- Hackers
- Competitors
- Terrorists
- Identify vulnerabilities: *identifying*, quantifying, and prioritizing (or ranking) the *vulnerabilities* in a system
- Operating systems
- Software
- Business processes

Risk assessment and risk management

Similar process to AS/NZS ISO 31000

- What can go wrong, where, by whom ??

Control framework provided in AS/NZS
ISO/IEC27002:2006

133 controls across 11 areas within the framework

Conduct risk assessment, risk treatment, communicate and consult, monitor and review.

Developing the Information Security Management System (ISMS)

Based on *PDCA* model of ISO 9001, Quality management

Plan (**establish** the ISMS)

Do (**implement and operate** the ISMS)

Check (**monitor and review** the ISMS)

Act (**maintain and improve** the ISMS)

ISO27001- Information Security Management System (Framework)

<https://www.youtube.com/watch?v=tuAYS5fRnpk>

(OECD Guidelines /Principles for ISMS)

- Awareness
- Responsibility
- Response
- Risk Assessment
- Security design and implementation
- Security Management
- Reassessment

IMPT: See Annex B of ISO27001 for mapping to PDCA

(Australian Privacy Act 1988)

- Australian Privacy Principle 1 — Open and transparent management of personal information
- Australian Privacy Principle 2 — Anonymity and pseudonymity
- Australian Privacy Principle 3 — Collection of solicited personal information
- Australian Privacy Principle 4 — Dealing with unsolicited personal information
- Australian Privacy Principle 5 — Notification of the collection of personal information
- Australian Privacy Principle 6 — Use or disclosure of personal information
- Australian Privacy Principle 7 — Direct marketing
- Australian Privacy Principle 8 — Cross-border disclosure of personal information
- Australian Privacy Principle 9 — Adoption, use or disclosure of government related identifiers
- Australian Privacy Principle 10 — Quality of personal information
- Australian Privacy Principle 11 — Security of personal information
- Australian Privacy Principle 12 — Access to personal information
- Australian Privacy Principle 13 — Correction of personal information

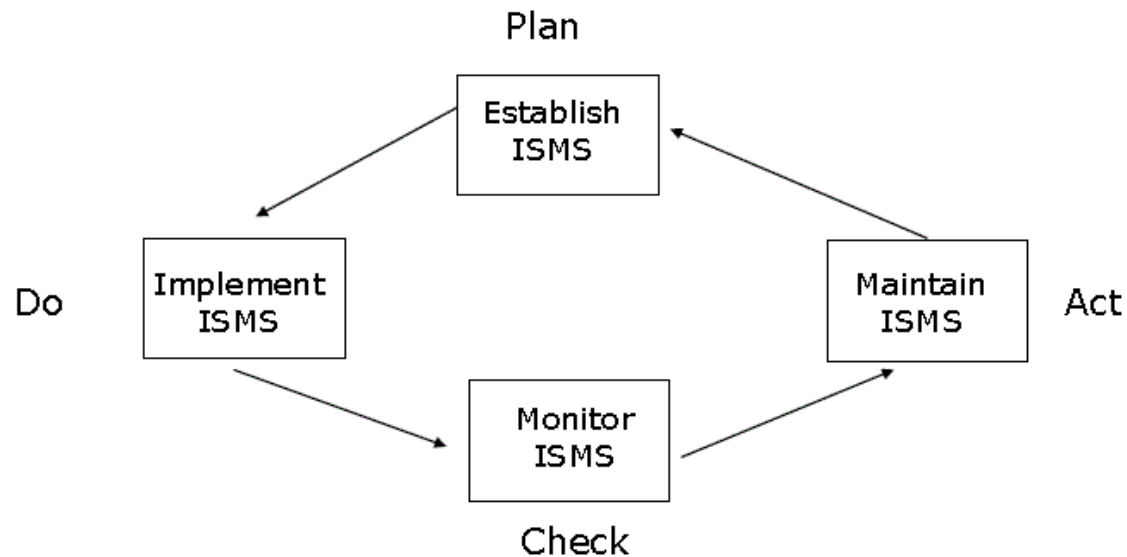


Develop the ISMS 55AS/NZS

DISCOVERERS WELCOME



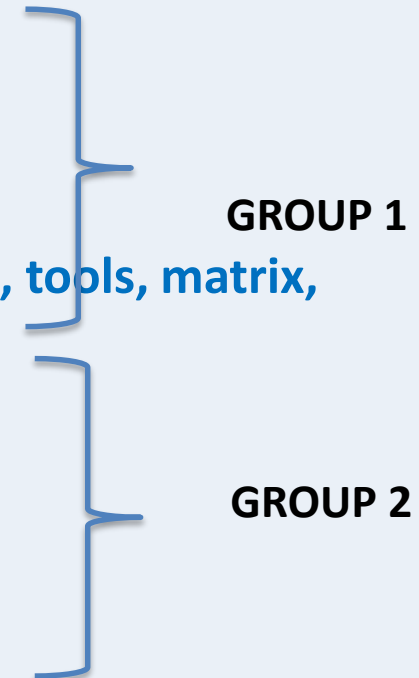
Develop the ISMS⁵



⁵AS/NZS ISO/IEC 27001:2006 Information technology – Security techniques – Information security management systems – Requirements

Choice Point Case study:

Structure of the RMP – just a guide⁴

- Introduction/Executive Summary
 - Definitions or glossary of terms (terminology used in the RMP)
 - Objectives (of risk management plan)
 - Risk management policy
 - **Interrelationship with strategic planning**
 - **Interrelationship with corporate governance**
 - **Organization and responsibilities/ accountability**
 - **Communication and consultation**
 - **Risk management framework (context, stakeholders, tools, matrix, criteria)**
 - **Risk management processes (methodology)**
- 
- GROUP 1**
- GROUP 2**

Structure of the RMP – cont'd

In the Appendix

- **Risk register** (Top 5 Risks only – 1 representative to brainstorm)
 - **Risk profile**
 - **Risk appetite and tolerance**
 - **Risk treatment plans**
 - **Monitor and review**
 - **Risk management programme**
 - **Performance measurement of the plan**
 - **Risk management implementation plan**
 - Appendices (sub reports)
- GROUP 3**
- GROUP 4**

STUDENT ARTICLE REVIEW

Choice Point Case study- Lecturer to discuss questions below with students

- What has happened? (the **event**)
- What was the root **cause**? (contributing factors)
- What could have been done to prevent it? (controls)
- How could the IMS managers better managed IM security breaches? (project managers and work executors)
- What were the risks and outcomes for the Public/clients, the company , internal stakeholders and staff? (take different perspectives and contexts)

Summary

- Information technology;
- Information security;
- Risks, threats and vulnerabilities;
- History of the Internet;
- Information security risk management;
- Standards (AS/NZS ISO/IEC 27001, COBIT); and
- Information security management system (ISMS).