Security Management in Practice

Contact

- Dr. Phil Legg
- Phil.Legg@uwe.ac.uk
- Room 2Q17

(Typically available Mondays, Tuesdays, Wednesdays, but please book via e-mail 24 hours ahead).

Module Delivery and Assessment

- Delivery:
  - – One hour lecture session
  - – Two hour workshop session
    - Research-based activities (individual and group) to support course content and further learning.
- Assessment:
  - – Project-based assessment:
    - Report (75%) and Presentation (25%)

Learning Outcomes

Understand the significance of ISO and other standards in the specification of a Information Security Management System

Analyse the range of real world security issues that face commercial organisations and Institutes

Evaluate the significance of security laws and regulations

Propose an ISMS for a real organisation, using recognised methods and to an internationally recognised standard

Reflect on the process of specifying an ISMS, justifying methods used and /or proposing alternatives

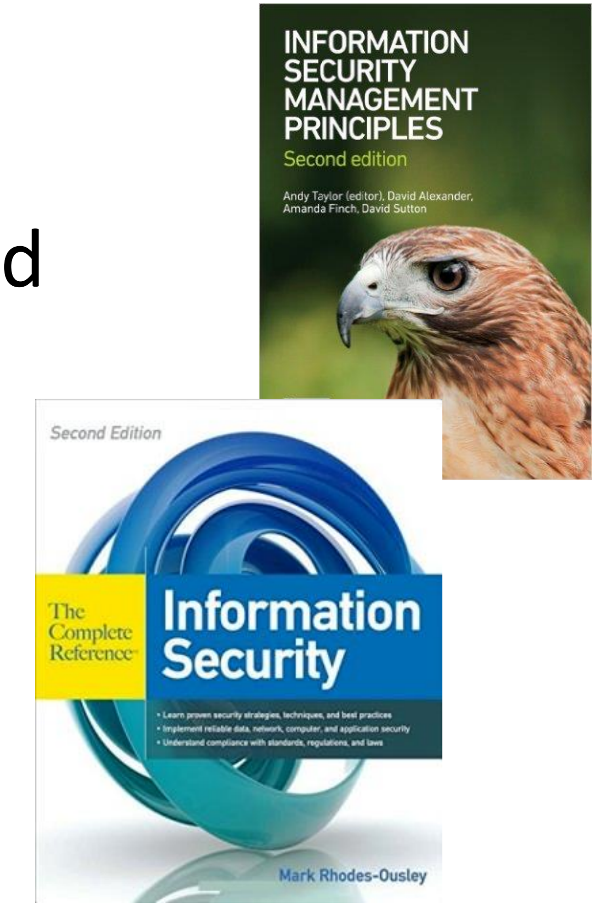
Module Schedule

1. Introduction
2. Information Risk Analysis, Threats and Vulnerabilities
3. Information Security Management Systems (ISMS)
4. Case Study: UWE Information Security Team
5. ISMS Controls
6. Legislation
7. Security Standards and Procedure
8. Procedural and People Security
9. Technical Security Controls
10. Physical and Environmental Security
11. Business Continuity, Disaster Recovery, Module Overview

Presentation sessions take place during Assessment Period 2

Recommended Text

- Information Security Management Principles. (Second edition), Andy Taylor, David Alexander, Amada Finch, David Sutton.
- Information Security: The Complete Reference (Second Edition), Mark Rhodes-Ousley.


INFORMATION SECURITY MANAGEMENT PRINCIPLES
Second edition
Andy Taylor (editor), David Alexander, Amanda Finch, David Sutton
Second Edition
The Complete Reference
Information Security
• Learn proven security strategies, techniques, and best practices
• Implement reliable data, network, computer, and application security
• Understand compliance with standards, regulations, and laws
Mark Rhodes-Ousley

Introduction to Security Management

Introduction

What is Security, and why is it important?

How can we effectively manage Security?

What is Security Management?

What is it that we are trying to secure?

What is Security?

- Security is not a single aspect
  - – Security is a process.
- Three D’s of security:
  - – Defense
  - – Detection
  - – Deterrence

Why is Security important?

- Personal and organisational security:
  - Protection of property (tangible security).
    - Hardware systems, assets, products, buildings.
  - Protection of information (intangible security).
    - Knowledge, data, intellectual property.

What is Security Management?

- Need to allow access only when authorized and necessary.
- Need to prevent access when unauthorized.
- How do we ensure that this is actually the case?

Information Technology Governance

- Guidelines for effective, efficient and acceptable use of information and communication technology within their organisation.
  - Strategic planning for IT in line with the vision and mission of the organisation
  - Oversight and monitoring of all IT-activity.
  - An IT decision-making model.

Information Security Concepts

Information Security (IS).
Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. *(ISO 27001)*

Information Assurance (IA).
The confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users. *(UK Cabinet Office)*

Information Security Principles

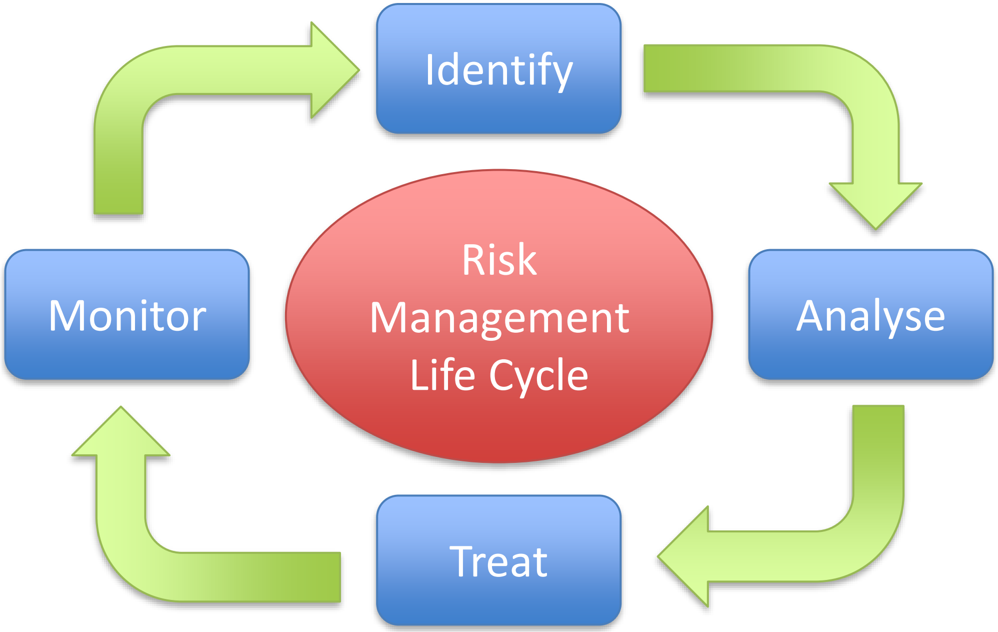
Confidentiality.
The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Integrity.
The property of safeguarding the accuracy and completeness of assets.

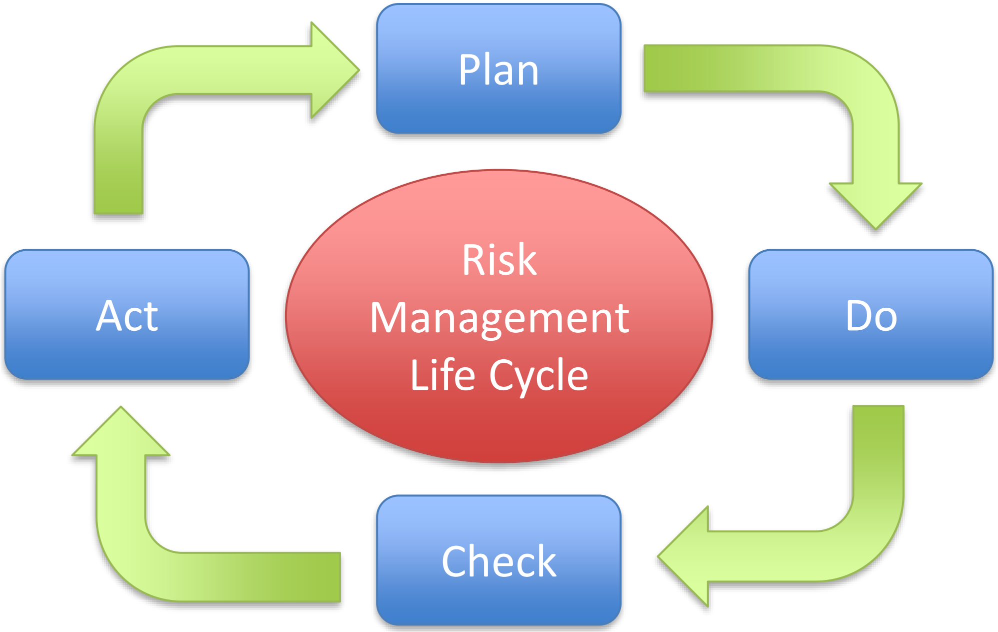
Availability.
The property of being accessible and usable upon demand by an authorised entity.

Asset.
Anything that has value to the organisation, its business operations and its continuity.

Managing Security = Managing Risk



PDCA (Plan-Do-Check-Act)



Information Security Principles

Threat.
A potential cause of an incident that may result in harm to a system or organisation.

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

Risk.
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

Impact.
The result of an information security incident, caused by a threat, which affects assets.

Information Security Challenges

The effect of the rapidly changing business environment.

Balancing cost and impact of security with the reduction in risk.

Security as an enabler of progress by reducing the cost of the loss, corruption, non-availability or unauthorised release of information.

The role of information security in combating hi-tech (and other) crime.

Quiz

What are the three D's of information security?

Defense

Detection

Deterrence

Quiz

What is the CIA model of information security?

Confidentiality

Integrity

Availability

Recap

- What is security and how do we manage this?
- Managing security is about managing risk.
- IT governance – an organisational decision-making model.
- Information security models (PDCA) and key concepts

Stuxnet cyber attack

- Watch: "Cracking Stuxnet, a 21st-century cyber weapon" (TED Talk)
- Read: "The Real Story of Stuxnet" (IEEE Spectrum)

How was the attack executed?
How could this have been mitigated?

What were the motivations behind Stuxnet?
What are other possible motivations for attack?

What are the implications of Stuxnet today?
Zero-day exploits?
Critical Infrastructure?
IoT?

Research and discuss the Stuxnet attack.
Think about the implications of this on today's society and cyber security concerns.
Feedback and discuss challenges as a group.