Information Assurance & Regulatory Compliance

5 March 2018

Section 1

Overview

Toady's Lecture

Objectives

- Gain an understanding of Information Assurance (IA).
- Understand the relationship between IA and Regulatory Compliance.
- Gain an understanding of Information Security Management Systems (ISMSs).
- How to achieve and manage IA through use of an ISMS.

Required Reading

- Igli Tashi. 'Regulatory Compliance and Information Security Assurance'. In: *Availability, Reliability and Security, 2009. ARES '09. International Conference on*. Mar. 2009, pp. 670–674

Section 2

Information Assurance

Information Security

Definition

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (NIST).

- Awareness of technical issues
- Awareness of user issues
- Awareness of organisational issues

Securing Organisations

- Organisations are socio-technical systems.
- information is what the organisation does
  - business processes create and use information
  - information risks are intertwined
- Security will be hard!
  - technical, organisational, and human elements
  - constraints on budget, effort, and time
  - how to select controls
- Other forces:
  - Financial motives: Business plans and strategies.
  - Regulartory and Legislative compliance
  - Responsibility of Management.

Security also includes compliance

All affect Information Security to some degree:

- Laws
- Decrees
- Industry regulations
- Codes of Conduct
- Stakeholder Expectations
- Contracts/Agreements
- Best Practises
- Company specific Policies, Standards & Guidelines
- Regulations/Administrative Order's

Compliance is important

- Avoid breaches of any
  - law;
  - statutory, regulatory or contractual obligations; and
  - security requirements.
- Security Incidents cost:
  - money
  - reputation
- Compliance has advantages:
  - increase to reputation
  - monetary incentives i.e. tax breaks
- Stakeholders request that organisations comply with laws and regulations in a transparent manner.

Information Assurance

Definition

Information Assurance (IA) is the confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users [HMG05].

- Awareness of Information Security.
- Awareness of legislative and regulatory compliance
- Confidence in security solution.
- Responsibility of Senior Management
- Affects business strategy and planning.

Security as Risk Management

Doing Security $\equiv$ Risk Management

- Asset identification
- Risk identification
  - Identifying assets' vulnerabilities
  - Identifying relevant threats
- Risk treatment analysis
- Treating the risk

Information Security Management System

Definition

. . . that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (ISO 27001)

Management system includes:

- organizational structure
- policies
- planning activities
- responsibilities
- practices
- procedures
- processes and
- resources

Section 3

ISO 27000 Series

ISO 27000 Series

The Series

Best practice recommendations on information security management, risks and controls within the context of an overall ISMS

Published Standards

- 27000 Overview and vocabulary
- 27001 Requirements
- 27002 Code of practice for information security management
- 27003 Implementation guidance
- 27004 Measurement
- 27005 Risk management

ISO 27000 Controls

- Security Policy
- Organization of Information Security
- Asset Management
- Human resources security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

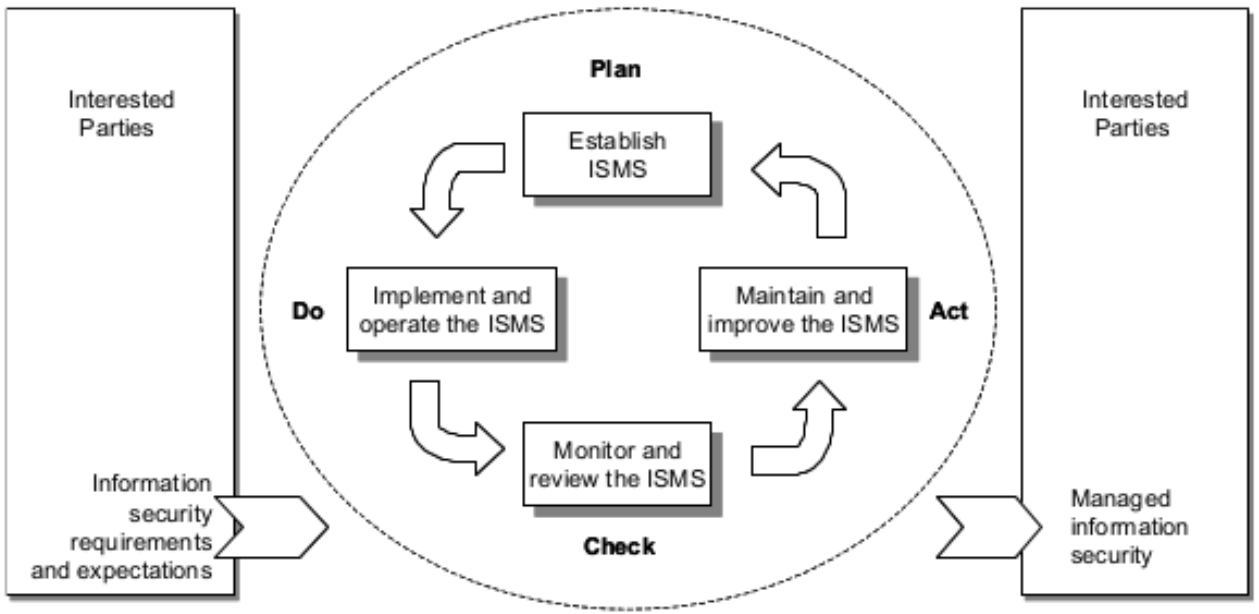
InfoSec according to ISO 27000

- Input
  - Risks to business process
  - Legal, regulatory, contractual and security requirements
- Process
  - Risk identification
  - Risk analysis
  - Risk treatment
- Output
  - Set of managed information security controls

ISMS according to ISO 27000

- Treat management as a cyclic business process
- Process is based on the Plan Do Check Act (PDCA) cycle
- Management involved at every cycle
- ISO 27001 describes the management process
- ISO 27002 contains list of controls
- ISO 27005 advice on risk management

Plan Do Check Act



ISO 27001

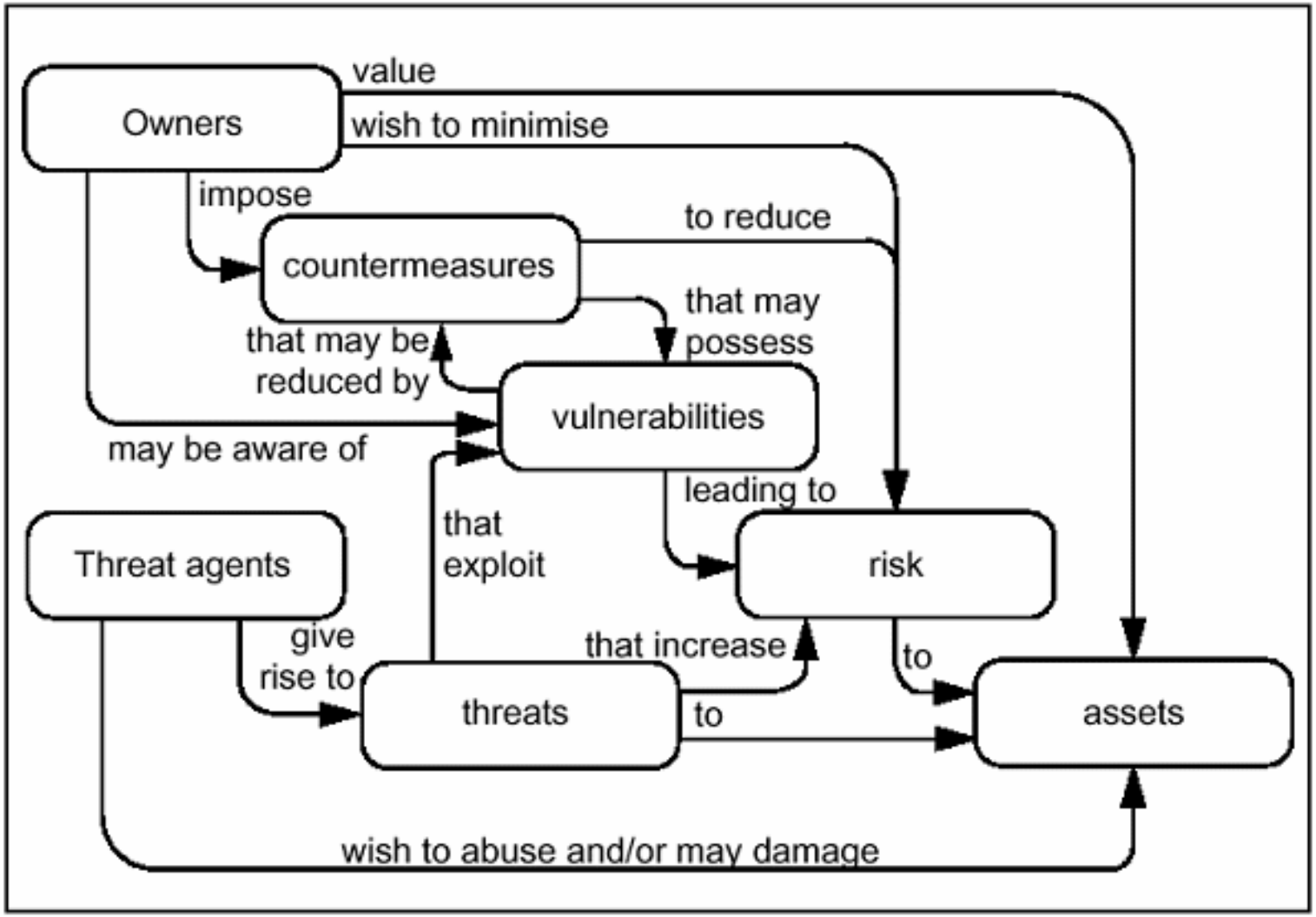
Plan Do Check Act: Detailed

- Plan
  - Define the ISMS:
    - InfoSec Policy, Scope, Asset Identification, Risk assessment approach, management process
  - select controls using risk assessment (ISO 27002)
  - decide control effectiveness measurement technique
- Do
  - Implement management processes
  - Implement selected controls
- Check
  - Internal review of management processes
  - Internal review of selected controls
- Act
  - Perform management review
  - Adjust ISMS

Section 4

Risk Assessment

Security in Context



http://www.bestinternetsecurity.net/wp-content/uploads/2008/08/risk-threats-vulnerabilities.gif

What are Asset?

Assets

Anything that has value to an organisation

Example asset Types:

- Information/Data
  - Matric Numbers, Financial data, Password Hashes, Logs...
- Business Processes
  - Enrolment, Hiring, Firing...
- Hardware
  - Servers, Security Tokens, ID Badges, Credit Cards...
- Software
  - Operating Systems, Office Software,
- Services
  - LTC, Moodle, YACRS
- Buildings
  - School of Computing, Boyd Orr
- People
  - Individuals, Committees
- ...

Asset Identification

All assets are valuable; but some assets are more valuable than others.

- Everything has the potential to be an asset.
- Assets can contain assets
  - Buildings contain things.
  - Computers contain information.
- Complex assets can be treated as a whole
  - Care about computer as a whole, and not constituent parts.
- Asset Identification can be dependent on scope of assessment.
  - Can be tricky to work out what assets to drop or skip details of.
  - Might need to perform own assessment for complex assets.

Threat Manifestation aka Risk

Risk

$$\text{Threat}(\textit{Asset}) + \text{Vulnerability}(\textit{Asset}) \equiv \text{Success}$$

Threat

- Circumstances that have potential to cause loss or harm to the asset
- Threats can be accidental, deliberate, or environmental in origin

Vulnerability

- Weakness that can be exploited within a system
- Vulnerabilities can be accidental, deliberate, or environmental in nature

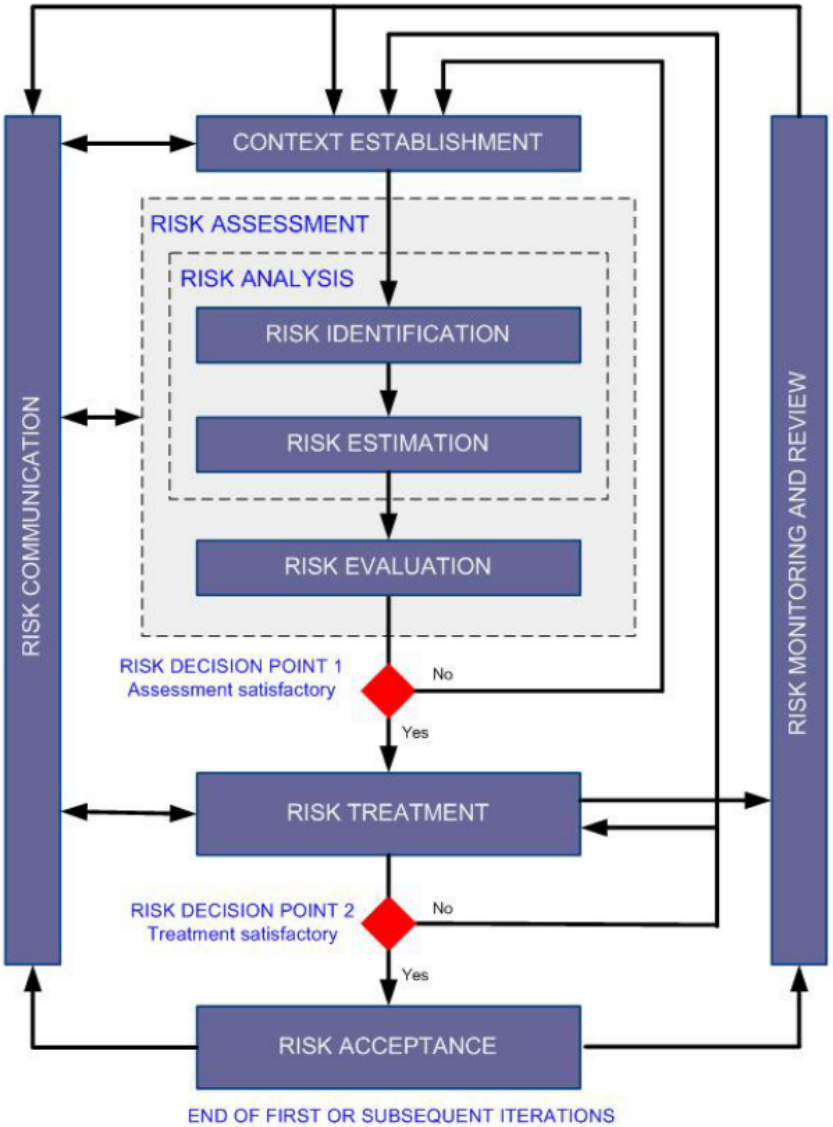
ISO Threat Types

- Physical damage
  - fire, water, dust
- Natural events
  - weather, volcanic activity
- Loss of essential services
  - loss of power
- Disturbance due to radiation
  - electromagnetic, thermal
- Compromise of information
  - Eavesdropping, Remote Spying
- Technical failures
  - equipment or software malfunction
- Unauthorised Actions
  - illegal processing of data, using pirated software
- Compromise of functions
  - Abuse of rights, Denial of Actions

Where can Vulnerabilities Occur?

- Hardware
  - environmental damage, wear and tear
- Software
  - well-known flaws, insufficient testing
- Network
  - single point of failure, unprotected comm lines
- Personnel
  - lack of personnel, insufficient training
- Site
  - located in flood plain, unstable power grid
- Organisational
  - lack of continuity plans, lack of email usage policy

Risk Assessment Process



Risk Assessment Process

1. Context establishment
   - Determine legal requirements, scope and boundaries, and dependencies
2. Risk assessment
   - Identify assets, threats, vulnerabilities
3. Risk estimation/evaluation
   - Risk = impact (1–5) $\times$ liklihood (1–5)
   - Prioritise Risks
4. Risk treatment
   - Accept, Avoid, Transfer, or Treat
   - Treatment reduces risk
5. Risk acceptance
   - re-evaluate risk
   - management acceptance
6. Documentation/communication
7. Risk monitoring

Doing Risk Assessments

- Often Performed as a workshop exercise
- Provide example lists to generate discussion
- Methodology should be used to generate discussion
- Provide experts from business and technical aspects
- Keep it grounded; but also interesting
- Take existing incidents, audits, assessments into account
- Manage process using spreadsheets...

Section 5

Compliance and ISO 27002

ISO 27002: Code of Practise

Section 15 Deals with Compliance:

- 15.1: Compliance with legal requirements
- 15.2: Compliance with security policies and standards, and technical compliance
- 15.3: Information systems audit considerations

Legal Requirements

Objectives

To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements.

Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).

Legal Requirements

List of Controls

- Identification of Applicable Legislation
- Intellectual Property Rights
- Protection of Organisational Records
- Data Protection and Privacy of Personal Information
- Prevention of Misuse of Information Processing Facilities
- Regulation of Cryptographic Controls

Legal Requirements—Not Exhaustive!

95/46/EC Data Protection Directive Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

99/93/EC Electronic Signature Directive on the legal recognition and regulatory framework for eSignatures.

2001/29/EC Copyright Directive Directive on the harmonisation of certain aspects of copyright and related rights in the information society

2002/58/EC Data Retention Directive Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector.

2006/24/EC E-Privacy Directive Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

Compliance with Policies and Standards

Objectives

To ensure compliance of systems with organizational security policies and standards.

The security of information systems should be regularly reviewed.

Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls.

Compliance with Policies and Standards

List of Controls

Compliance with security policies and standards

- ISO/IEC 9K Quality Management Systems
- ISO/IEC 27K Information Security Management
- ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation
- COBIT Control Objectives for Information and Related Technology

Technical compliance checking

- Check systems for compliance with implementation standards
- Penetration testing
- Vulnerability assessment

Information systems audit considerations

Objectives

To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

There should be controls to safeguard operational systems and audit tools during information systems audits.

Protection is also required to safeguard the integrity and prevent misuse of audit tools.

Information systems audit considerations

List of Controls

Information systems audit controls

- Planned in advanced
- Minimal disruption
- Independent Auditing: PwC, KPMG, Deloitte, Cap-Gemini

Protection of information systems audit tools

- Source of information Leakage
- Tool access should be restricted
- Protection of audit process artifacts
- Third parties need oversight.

Section 6

Summary

In Conclusion

- Information Assurance is:
  - Risk Management
  - Defining policies and implementing controls
  - Compliance with legislation, regulation, and standards
  - Ensuring compliance
- ISMSs are used to establish, implement, operate, monitor, review, maintain and improve IA confidence.
- Provide a PDCA cycle to do so.
- `ISO 27K` Series provides a set of best practices for achieving and managing Information Assurance.

  ISO 27001 Provides security management

  ISO 27002 Provides security controls

Recommended Reading

- S. Haddad et al. 'Operational Security Assurance Evaluation in Open Infrastructures'. In: *Risk and Security of Internet and Systems (CRiSIS), 2011 6th International Conference on*. Sept. 2011, pp. 1–6
- Bilge Karabacak and Ibrahim Sogukpinar. 'A Quantitative Method for ISO 17799 Gap Analysis'. In: *Computers & Security* 25.6 (May 2006), pp. 413–419. ISSN: 0167-4048
- Sigurjon Thor Arnason and Keith D. Willett. 'Implementing an Information Security Management System: Plan-Do-Check-Act'. In: *How to Achieve 27001 Certification: An Example of Applied Compliance Management*. 2007, pp. 97–162
- HMG. *Risk Management and Accreditation of Information Systems*. English. Online. Centre for the Protection of National Infrastructure (CPNI), Aug. 2005

If you are really bored...

- CCRA. *Common Criteria for Information Technology Security Evaluation*. English. Common Criteria Recognition Arrangement (CCRA) Management Committe. 2012. URL: http://www.commoncriteriaportal.org/
- European Commission. *European Commission on Data Protection*. English. European Commission. 2012. URL: http://ec.europa.eu/justice/data-protection/ (visited on 20/11/2012)
- European Commission. *European Union Directives*. English. European Commission. 2012. URL: http://eur-lex.europa.eu/ (visited on 20/11/2012)