TJTSM51 Information Security Management

Professor: Mikko Siponen, Ph.D., D.Soc.Sc.
Course assistant Mr. Hemin Jiang
(<hemin.jiang@jyu.fi>)

Structure

- Introduction to the course
- Introduction and conceptual foundation
- Information security in different disciplines
- Secure system design methods
- Information security standards
- Risk Assessment and IT investment
- Information security policies

2

INTRODUCTION TO THE COURSE

3

Purpose

To provide knowledge about:

- The information security field, its basic concepts and principles
- Techniques and methods for managing information security in organizations
- Key empirical research findings

4

The Key aim of the course

- The course "TJTSM51 Information Security Management" focuses on providing know-how that is required to manage organizations' information security functions. The perspective of the course is therefore that of information security manager of the company, or respective consulting or expert tasks.

5

Related Courses

- ITKST40 Society and Information Security, Department of Mathematical Information Technology
- ITKST46 Cyber security management, Department of Computer Science and Information Systems and Department of Mathematical Information Technology

6

Contact Persons

- Professor Mikko Siponen, Head of Department
  - Email: mikko.t.siponen@jyu.fi
  - Office Hours:
    - Monday, 1 hour before the lecture by Siponen.
    - Wednesday, 1 hour after the lecture by Siponen.
- Mr. Hemin Jiang
- Email: Jiang Hemin hemin.jiang@jyu.fi
- Office Hours:
    - Monday and Wednesday, 1 h after the lecture

7

Schedule of Lectures 1/2

- Ma 19.1. 14:15-16:00: Prof. Siponen, introduction, allocation of case exercises, the Conceptual Foundation, and Information security in different disciplines
- Ke 21.1. 12:15-14:00: Prof. Siponen: Secure system design methods.
- Ma 26.1. 14:15-16:00: Prof. Siponen: Information security standards
- Ke 28.1. 12:15-14:00 Alain Tambe: Social engineering and Phishing
- Ma 2.2. 14:15-16:00 Alain Tambe: indentity theft
- Ke 4.2. 12:15-14:00: Case exercise on Information security policies + research on the topic (Siponen).
- Ma 9.2. 14:15-16:00 Case exercises on employees' compliance with information security policies + research on on the topic (Siponen)
- Ke 11.2. 12:15-14:00: Password Psychology: memory, behaviour, and security by Naomi Woods
- Ke 18.2. 12:15-14:00 case exercises on personal use of Internet + research on the topic (Jiang+Siponen).

8

Schedule of Lectures 2/2

- Ma 23.2. 14:15-16:00: Dr. Tsohou: Information Security Risk Management
- Ke 25.2. 12:15-14:00 Dr. Tsohou: Business Continuity Management
- Friday 27.2. Dr. Tsohou - TBA
- Ma 2.3. 14:15-16:00: Dr. Tshou Personal Data Protection
- Ke 4.3. 12:15-14:00 Case exercises on information security investments + lectures on the topic by prof. Siponen.
- Ma 9.3. 14:15-16:00: Senior Inspector of Nuclear power plants in Finland, Timo Wiander, Physical Security.
- Ke 11.3. Optional, if needed for case exercises

9

How to Pass a Course

- **Course has traditional lectures** (there are not mandatory, but they might help you to pass the course)
- Background material can be obtained from information security management books:
  - E.g., Management of Information Security, Michael Whitman and H Mattord.
  - Such books however are not enough for passing the course with the excellent grades.
  - They lack “evidence-based” approach.

10

How to Pass a Course

- **Mandatory case exercises on four categories**:
- 1) Non-work related use of Internet, 2) Investment, 3) Training and 4) policies, Clean desk and encryption
- Students need to select and solve one in each area (so 4 case examples altogether).
- Case exercises can be done in individually or in groups.
- They need to be returned to course assistant 2 days before the deadline in a power point –format (you do not have to use power point; you can use any software you want). Send the file in .pdf format to course assistant (hemin.jiang@jyu.fi).

11

Case Exercises 1/2

- **Mandatory case exercises on four categories**:

- At each time, students are prepared to present their case exercises, so that there are 4-6 presentations at each time.
- If you are not prepared to present (you are not present in the class, then you solve one extra case exercise for each time you are not present).

12

Case Exercises 2/2

- In the lectures associated with the case exercises, we discuss about the case exercises, and also outline what could be the responses to the case exercises in the light of the research findings.
- In terms of case exercises, there are two learning experiences:
  - One if when you do the case exercise
  - Another one is when you learn how you case exercise solutions could be improved.
- The case exercises are situations which I have been faced as a consultant type of role. These are examples of a real problems that consultants or information security manager face.
- Exams consists of the same case exercises, or case exercises which are based on the case exercises took by the students.

13

Case exercises: Non-work use of computers at work

- Case 1: information security manager contacts you that her company has a malware problem coming from the visit of non work related use of Internet. How you would address this problem?
- Case 2: information security manager contacts you that company has a malware problem coming from employees' surfing from the adults site. The information security manager has tried to move with the problem, but did not get management' approval. The information security manager has some evidence that a top level manager surf the adult sites. How to solve this problem?

14

Case exercises: Non compliance in general

- Case 3: information security manager contacts you that no one in her company complies with the infosecurity policies? She ask you as a consultant to solve the problem. How you would solve it. What are the steps?

- Case 4: information security manager contacts you that employees' do not use an email encryption software, in the situation where law would require them to do so. The encryption software requires pressing one extra button. One group of employees' claim that this is too much. Another group of employees claim that their contacts outside of the company cannot open it or they complain that they do not want to open the encrypted message.

15

Case exercises: Policies

- Case 5: Develop password procedures for organizations that has 100 different systems. Users use 1 to 30 systems. All systems contain at least sensitive system.

- Case 6: you are asked to develop information security procedures for companies. How would you do it. Describe the overall approach or process.

16

Case exercises: training

- Case 7: Organization has a number of systems that require difficult to guess password. The employees have hard time in developing these and write passwords down. Information security manager ask you as a consultant to provide a training sessions to employees so that they can develop a number of hard-to-guess passwords. Give the training in the class.

- Case 8: prepare a campaign for 10 000 employees to change their passwords for hard to guess passwords. What is the message to convince the employees to change their passwords.

17

Case 9: Organizations has in use the following multiple choice online training that is mandatry for employees

A) ”Passwords must have must be 8 characters including 1 uppercase letter, 1 ..”;

(B) ”Passwords must have must be 10 characters including 1 uppercase letter, 1… ”

(C) ”Passwords must have must be 12 characters including 1 uppercase letter, 1… ”

18

18

CASE 9 continue

- The online training package can be passed when the employees get 90% of the answers right (of the multiple choice questions).
- In the company, there is 98% coverage of the training, so 98% of the employees have took it and passed. This is good to show to the management and ISO auditors, who want to see that all the people have taken the training.
- So things are good in paper. However, it has been realized in reality no one cannot recall the online training, and they do not follow any security procedures.
- How you would solve this problem? How would you approach it?

19

Case exercises: clean desk policy

- Case 10: information security manager contacts you as a consultant to solve the following problem that the employees do not comply with the clean desk policy of the company. The company has 400 people in the same building and they have hot desks. How you would solve the problem?
- Case 11: you are an information security manager. Employees do not follow the company clean desk policy and leave confidential material to their tables. You need to design a campaign to make employees to comply with the policy. Budget is 0 €.

20

Case exercises: investment

- Case 12: datawarehouse. You are asked to lead a team by a Fortuna 50 company to search for a place for datawarehouse of the company. You need to come up with the requirements and find top 3 ideal locations for the datawarehouse.
- Case 13: There is no email encryption software available in the company. Confidential information and social security numbers are send out in email (without encryption) every now and then. It seems to be illegal. Security manager has selected an email encryption software that he thinks is easy to use. It is also among the cheapest, and price is per user. Security manager has tried to persuade the management to invest in the software by claiming that people break the law, but management does not go for it. After all, all these emails are send without an encryption and management see no problems so far. How you get the investment accepted and use?

21

Selection of the Case exercises

- Send you selection to course assistant:
- hemin.jiang@jyu.fi
- He will send you the reading list that give you different hints in solving the problem. The reading list may not provide direct solutions to solve the problems.
- Beside that you can search Computer & Security –journal or search by using Google Scholar. Use JYU VPN in order to get access to Computers & Security, and much wider access through Google Scholars.

22

Evaluation of the course

- The evaluation will be based on the final exams
- The case exercises must be done (4 for each person).
- The exams is on about the lectures in the course + case exercise.

23

INTRODUCTION AND CONCEPTUAL FOUNDATION

24

Society is reliant on IT

- Modern society is increasingly reliant on information processing and global networks
- Economy is reliant on information and information processing
- Several services are directly or indirectly relying on IT (e.g. hotels, hospitals, telecommunications, marketing,
- e-commerce)
- In such a society, security is a vital and a growing concern

25

The value of Information in the Information Age

- Information is valuable to the people that it belongs, to the people that use it and the people that wish to get it
- However, collecting, creating, and maintaining information brings cost
- Certain aspects determine the value of information:

26

Information security problems are increasing

27

Definitions

- **Asset**:
- **Value**:
- **Threat**:
- **Vulnerability**:

28

Definitions

- **Owner**:
- **Authorization**:

29

The Term Information Security…

- …is often confused with the concepts of:
  - Safety
  - Insurance
  - Assurance

30

Information Security

Means e.g., at organizational context that Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

31

Information Security

- The preservation of **confidentiality**, **integrity** and **availability** of information
- Additional properties that can be involved are authenticity, accountability, non-repudiation, and reliability.

32

Confidentiality

33

Integrity

34

Availability

35

Additional information security properties

- **Authenticity**:
- **Accountability**:
- **Non-repudiation**:
- **Reliability**:

36

Information Security Management at organizations

- Information security management refers to the structured process of implementing and managing information security in an organisation.
- Information security management is composed by a series of sequential actions that aim at protecting information and information systems' assets with ultimate purpose to ensure business continuity of the organisation.

37

Examples of Assets

- Physical Assets:
  - Hardware
  - Printers
  - Communication facilities
  - Buildings, etc.
- Data
- Software
- Intangible Assets:
  - Reputation
  - Image
  - Competitive Advantage, etc.

38

Categories and Examples of Threats

- Natural Threats
  - Earthquake
  - Flooding
  - Fire, etc.
- Threats from Technical Problems
  - Technical Failure of Server or a Workstation
  - Technical Failure of Network Distribution Component
  - Power Failure, etc.
- Human Threats
  - Accidental: Users' Errors, Software/Hardware Maintenance Error,
  - Intentional: Misuse of System Resources, Masquerading of User Identity, Unauthorized Use of an Application

39

Categories and Examples of Vulnerabilities

- Hardware-related Vulnerabilities
- Software-related Vulnerabilities

40

Categories and Examples of Vulnerabilities

- Network-related Vulnerabilities
- Personnel-related Vulnerabilities
- Location/Buildings-related Vulnerabilities

41

Categories and Examples of Impacts

- Legal Obligations
  - Civil suit or criminal offence resulting in damages/ penalty of (e.g., 2,000$ or less)
  - Regulatory opligations

42

Categories and Examples of Impacts

- Commercial and Economic Interests
- Financial Loss/Disruption to Activities
- Loss of trust/reputation

43

…Back to the Definitions

- **Risk**:
- **Safeguard** (also, **Control** or **Countermeasure**):

44

…Back to the Definitions

- **Policy**:
- **Procedure**:
- **Residual risk**: the risk remaining after implementing safeguards

45

Relationship between Security Concepts

- safeguards (S)
- Risks (R)
- Assets (A)
- Threat (T)

46

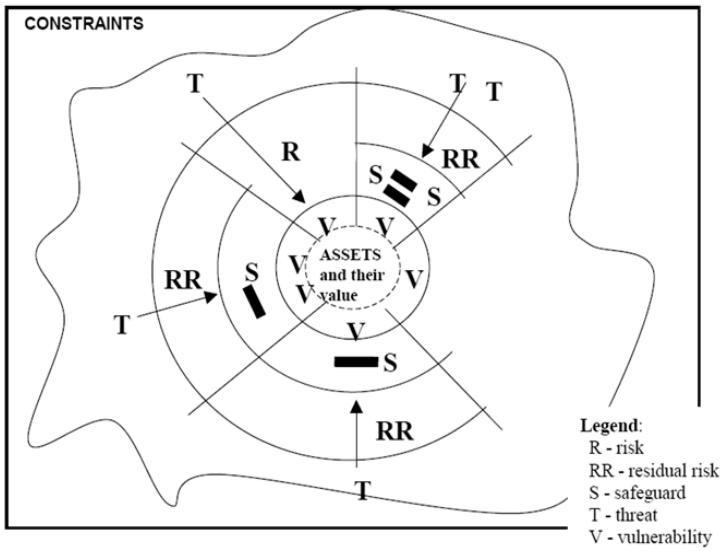


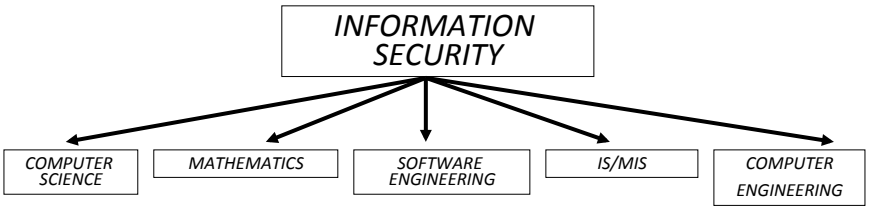
Figure 1 – Security element relationships

ISO/IEC 13335-1:2004

47

INFORMATION SECURITY IN DIFFERENT DISCIPLINES

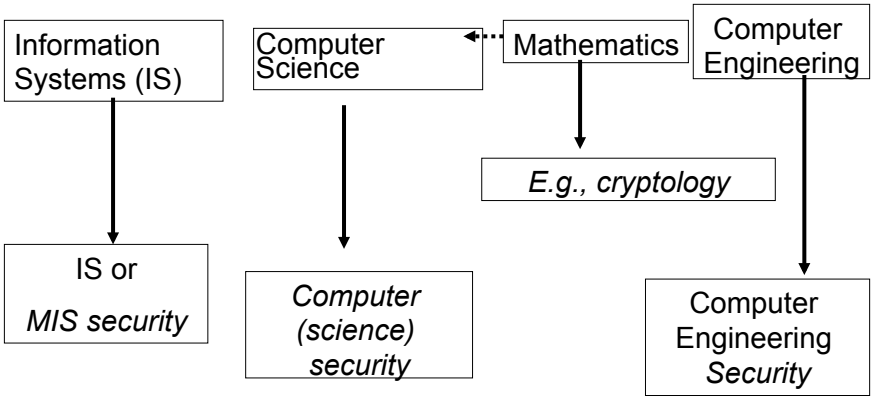
48



- Role of theory and evidence vs. "common-sense" understanding of the reality.
- The latter is often flawed, cf., history of science and evidence-based medicine.

49

Information Security Research

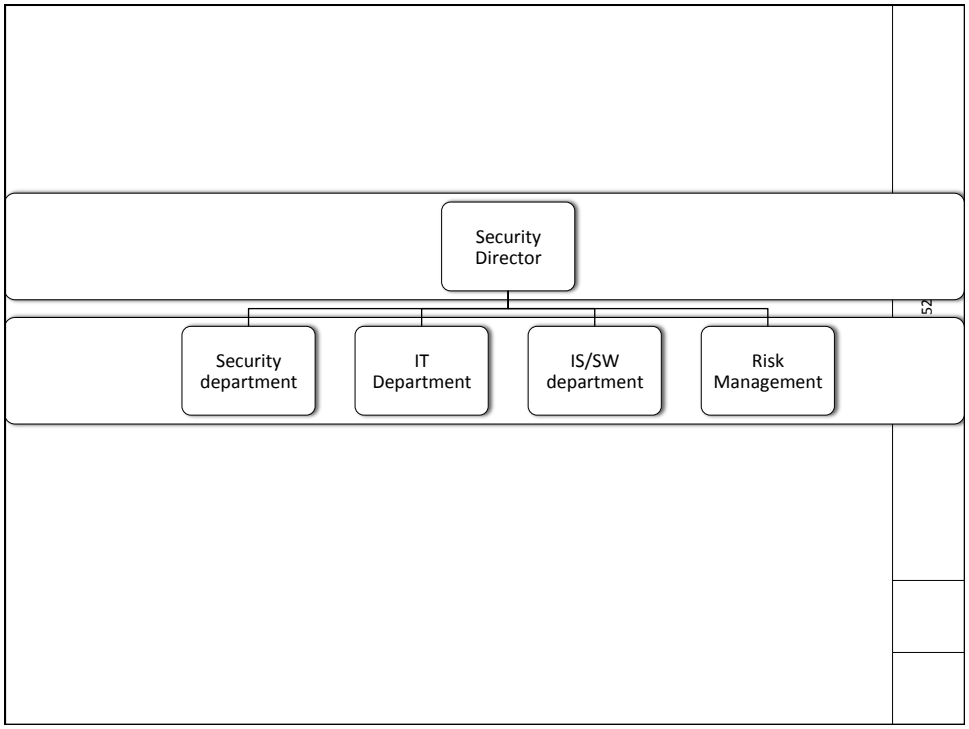


50

Positions in Industry

- Security Director
- Information Security Director
- Information Security Manager
- Information Security Consultant
- Chief Information Security Officer
- Senior Information Security Expert
- Information Security Expert
- Secure system developers

51

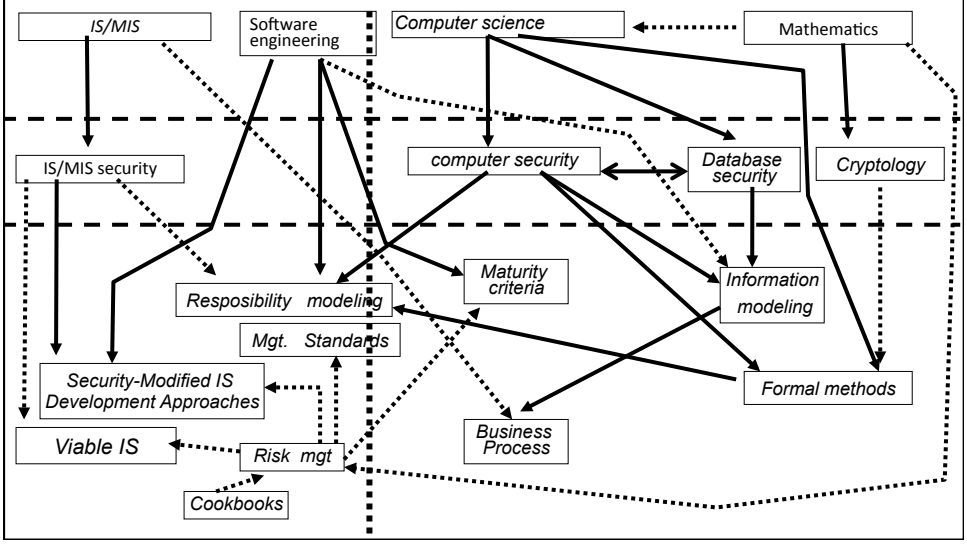


52

SECURE SYSTEM DESIGN METHODS

53

Origins of the different approaches for designing secure systems



Why we need secure systems design methods or methods for security management?

- Vendors offer a range of technical protection solutions;
- Employing any security techniques requires careful and systematic planning;
- It is unwise to start building a house or an airplane, for example, by buying wood or metal just because vendors widely advertise these items;

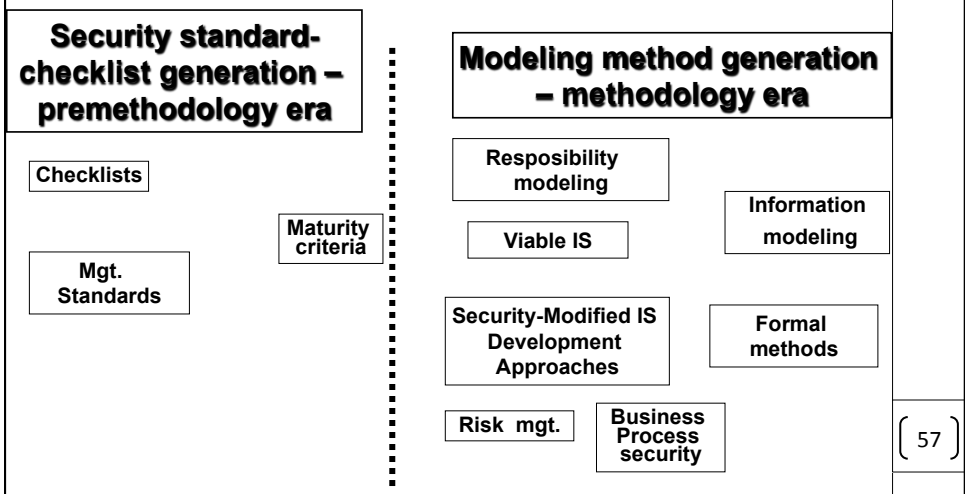
55

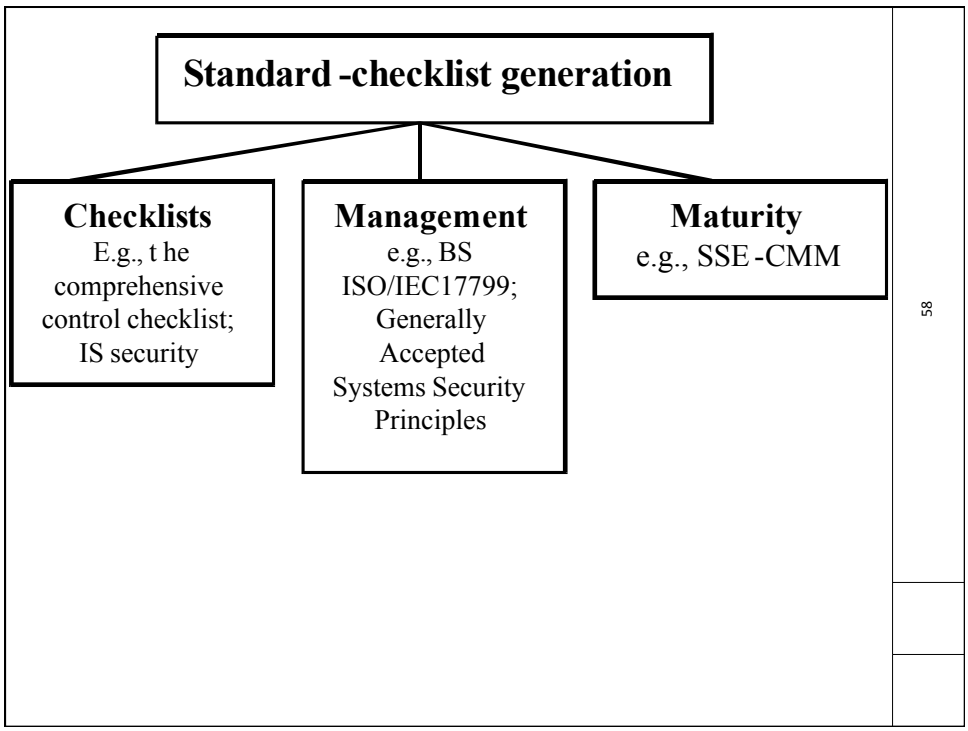
Careful planning required

- you'd never start building without first considering what design provides a *safe* house or plane, and what requirements the house or plane should meet.
- This idea also applies to securing information systems: Careful planning ensures the implementation of optimal and proper IS controls.
- Therefore secure-systems planning are needed.

56

Alternative approaches for designing secure systems





INFORMATION SECURITY STANDARDS

59

The concept of standardisation

- Assuring desirable common characteristics of products and services
- Facilitating trade
- Diffusing technological progress and innovation
- Enabling consumers' trust
- Facilitating common problems' solution

60

Standards: meaning and classification

Standards can be:

- ✓de facto → concerning "fact" or practice
- ✓de jure → concerning law

61

Certification and Accreditation

Certification

- ❑Audit, verification and written certification
- ❑Issuing Certificate
- ❑Given by an independent third party with recognized ability
- ❑Compliance with the requirements of a standard

Accreditation

- ❑Affirmation by a recognized accreditation body
- ❑Issued to Accreditation Bodies
- ❑Recognizes the ability of the Body to provide certification to an organization with sufficiency and impartiality

62

The 27000 series on Information Security Management Systems

ISO/IEC 27000:2009	Overview and vocabulary
ISO/IEC 27001:2005	Requirements
ISO/IEC 27002:2013	Code of practice for information security management
ISO/IEC 27003:2010	Implementation guidance
ISO/IEC 27004:2009	Measurement
ISO/IEC 27005:2008	Information security risk management
ISO/IEC 27006:2007	Requirements for bodies providing audit and certification
ISO/IEC 27007: 2011	Guidelines for ISMS auditing
ISO/IEC 27011:2008	Guidelines for telecommunications organizations based on ISO/IEC 27002

63

ISO/IEC 27001: 2005

- Specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented **Information Systems Management System (ISMS)** within the context of the organization's overall business risks.
- A **management system** is a framework of policies, procedures, guidelines and associated resources to achieve the objectives of the organization
- **ISMS** is a part of the overall management system based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

64

ISO/IEC 27001: 2005

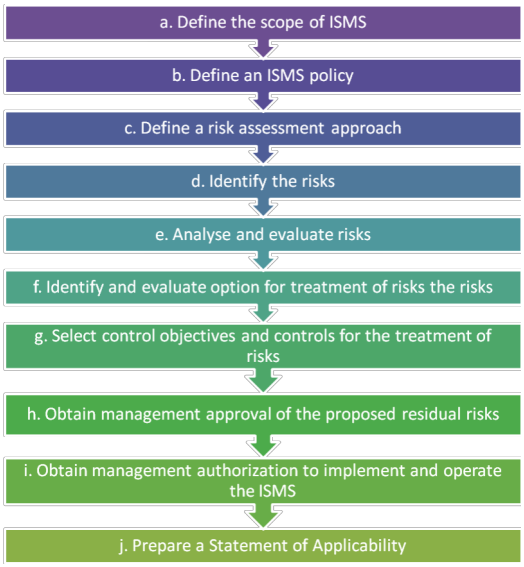
- Contains requirements for the implementation of security controls customized to the needs of individual organizations or parts of them.
- Contains requirements in a structure of:
  - 11 control clauses that include
  - 39 control objectives
  - 133 controls

65

The PDCA model of ISO/IEC 27001

66

PLAN: Establish the ISMS



67

Annex A - Control objectives and controls

1. Security Policy
2. Organizing Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

68

Annex A - Control objectives and controls: Examples (1)

A5: Security Policy

Objective: *To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations*

A5.1: Information security policy document

Control: *An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.*

69

Annex A - Control objectives and controls: Examples (2)

A6: Organization of information security

A6.1: Internal organization

Objective: *To manage information security within the organization*

A6.2 External parties

- Objective: *To maintain the security of the organization ' s information and information processing facilities that are accessed, processed, communicated to, or managed by external parties*

A6.1.3: Allocation of information security responsibilities

Control: *All information security responsibilities shall be clearly defined*

A6.2.2: Addressing security when dealing with customers

Control: *All identified security requirements shall be addressed before giving customers access to the organization ' s information or assets*

70

Annex A - Control objectives and controls: Examples (3)

A.11 Access control

A.11.2 User access management

Objective: *To ensure authorized user access and to prevent unauthorized access to information systems*

A11.2 User responsibilities

- Objective: *To prevent unauthorized user access, and compromise or theft of information and information processing facilities*

A11.2.3: User password management

Control: *The allocation of passwords shall be controlled through a formal management process*

A11.2.1: Password use

Control: *Users shall be required to follow good security practices in the selection and use of passwords*

71

ISO/IEC 27002: 2013

- Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.
- Provides general guidance on the commonly accepted goals of information security management
- Contains a comprehensive list of approved procedures and information security controls.
- Classification of controls in eleven categories

72

ISO/IEC 27002: 2013

The standard may serve as:

- A practical guideline for developing effective security management practices.
- A basis for the understanding of the requirements contained in ISO/IEC 27001: 2005.

73

ISO/IEC 27002: 2013 Example of Guidelines

A6.1.3: Allocation of information security responsibilities

Control: *All information security responsibilities shall be clearly defined*

Implementation guidance:

- the assets and information security processes should be identified and defined
- the entity responsible for each asset or information security process should be assigned and the details of this responsibility should be documented
- authorization levels should be defined and documented
- the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments
- coordination and oversight of information security aspects of supplier relationships should be identified and documented

74

Other Security Standards and Guidelines

- Risk Assessment
  - National Institute of Standards and Technology (NIST) SP 800-30 R1: 2012
- Security Governance
  - Information Security Forum (ISF),Standard of Good Practice: 2007
  - Information Systems Security Association (ISSA), GAISP Generally Accepted Information Security Practices: 2004
  - OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002

75

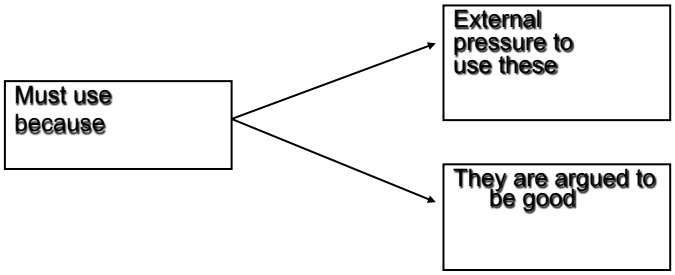
Other Security Standards and Guidelines

- Business Continuity
  - British Standards, BS 25999 series
- Information Security Incident Management
  - NIST SP 800-61, Computer Security Incident Handling Guide: 2004
- Information Security Evaluation
  - ISM3 Information Security Management Maturity Model: 2009
- Malicious Code
  - NIST SP 800 -83, Guide to Malware Incident Prevention and Handling: 2005

76

Security Standard generation

- Often even mgt. standards drive secure systems design and information security management



77

They are argued to be good

- "*can…*[the] *code of practice for information security management (BS7799-1:1999) be ignored? Well if your organization is looking for trouble in the future, I suppose the answer to this question is 'yes'*". (Pounder 1999 p. 311)
- "*...the best method of the ISP* [Information Security Policy] *development is to concentrate on the baseline approach* [i.e., to implement widely used controls] *and to implement as much as possible the security standards described* [such as BS 7799]" (Janczewski 2000 p. 96, quoted in Baskerville & Siponen 2002).
- "[…] *senior management's performance is judged by how well the organization performs in terms of internationally accepted codes of IS* [IS=Information Security] *practice* [such as BS7799]." (Eloff & von Solms 2000b p. 698).

78

Standard-Checklist generation: a common assumption

- List available means of protection (techniques, practices, processes, goals) that all organizations should implement or meet.
- assume that it is possible to find generic or universal sets of IS security procedures, techniques and practices that minimize information security risks.

79

An example of an IS security checklist

List of principles	Yes (x), no (-)
1. Do you have a firewall in your organization?	x
2. Do you use encrypted communication?	-
3. Are remote access connections encrypted?	x

80

An example of an IS security standard

List of principles
1. Use firewall in your organization
2. use encrypted communication
3. Use encrypted remote access connections

81

And a security maturity criteria…

Maturity level	IS security practices	Yes (X) / No (-)
1.	Do you have a firewall in your organization?	X
	…	-
2	Do you use encrypted communication?	-
….	…	-
5.	Are remote access connections encrypted?	X

82