Practical implementation of ISO 27001 / 27002

Security in Organizations
2011
Eric Verheul
Main literature for this lecture:

1. ISO 27001 and ISO 27002


3. [http://www.iso27001security.com](http://www.iso27001security.com)
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
Recap on information security

Recap

- Complicating factors in implementing Information Security (IS) are its multidisciplinary nature and constraints on budget, effort and getting management attention.
- ISO 27002 is a (long) list of 133 IS controls divided over 11 chapters originally dating from the nineties.
- Practice shows that ‘just’ implementing ISO 27002 is not the way to secure organizations because not all controls are equally relevant for all organizations.
- To address this ISO 27002 was supplemented with ISO 27001 which describes ‘security management’.
- Fundamental to ISO 27001 is that it considers IS as a continual improvement process and not as implementing a security product.
Outline

Theory
• Recap on information security
• **ISO 27001/27002 introduction**
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
<table>
<thead>
<tr>
<th>H</th>
<th>ISO 27002</th>
<th>NEN Vertaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Security Policy</td>
<td>Beveiligingsbeleid</td>
</tr>
<tr>
<td>6</td>
<td>Organization of Information Security</td>
<td>Beveiligingsorganisatie</td>
</tr>
<tr>
<td>7</td>
<td>Asset Management</td>
<td>Classificatie en beheer van bedrijfsmiddelen</td>
</tr>
<tr>
<td>8</td>
<td>Human resources security</td>
<td>Beveiligingseisen ten aanzien van personeel</td>
</tr>
<tr>
<td>9</td>
<td>Physical and Environmental Security</td>
<td>Fysieke beveiliging en beveiliging van de omgeving</td>
</tr>
<tr>
<td>10</td>
<td>Communications and Operations Management</td>
<td>Beheer van communicatie- en bedieningsprocessen</td>
</tr>
<tr>
<td>11</td>
<td>Access Control</td>
<td>Toegangsbeveiliging</td>
</tr>
<tr>
<td>12</td>
<td>Information Systems Acquisition, Development and Maintenance</td>
<td>Ontwikkeling en onderhoud van systemen</td>
</tr>
<tr>
<td>13</td>
<td>Information Security Incident Management</td>
<td>Incidentmanagement</td>
</tr>
<tr>
<td>14</td>
<td>Business Continuity Management</td>
<td>Continuïteitsmanagement</td>
</tr>
<tr>
<td>15</td>
<td>Compliance</td>
<td>Naleving</td>
</tr>
</tbody>
</table>
History of ISO 27002

- Motivation for ‘7799’: organizations can trust in each other’s information security
- UK Department of Trade and Industry's (DTI) publishes "Users Code of Practice" in 1989.
- To ensure meaningfulness a consortium of users formed (including Shell, BT) resulted in "A code of practice for information security management" PD 0003 in 1989.
- PD 0003 published as British standard BS 7799 in 1995
- Major revision of BS 7799 in 1999.
- Published as ISO 177799 standard in 1999, published with minor amendments in 2000.
- Major revision of ISO 17777 in 2005. ISO 17799 renamed to ISO 27002 in 2005, this is the current version.
History of ISO 27002

ISO 27001/27002 introduction
History of ISO 27002

• Current version BS7799 is ISO 27002:2008
  • contains 133 controls
  • previous version (2000) contained 125 controls
  • 9 deleted, 17 added
• Controls are supplemented with detailed further implementation guidelines.
• The transition from British standards (BS) to international standards (ISO) will further increase importance.
10.1.3 Segregation of duties

Control
Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.

Implementation guidance
Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent.
Critique in 1995:

- Insufficient guidelines on how to implement BS7799
- In effect BS7799 is a list of (133) controls and which controls should be selected and which not?
- Information security primarily deals with managing (residual) risks by choosing appropriate controls and that was not really part of the standard

As a response to earlier critique, BS7799 introduced 10 ‘Key Controls’: that were mandatory. But this did not address the critique satisfactorily.
Critique on BS7799

1. Security policy
   1.1. Information security policy ........................................ 17
   1.1.1. Information security policy document .......................... 17

2. Security organisation
   2.1. Information security infrastructure ................................. 19
   2.1.1. Management information security forum ........................ 19
   2.1.2. Information security co-ordination .............................. 20
   2.1.3. Allocation of information security responsibilities ......... 20
   2.1.4. Authorisation process for IT facilities ........................ 21
   2.1.5. Specialist information security advice .......................... 22
   2.1.6. Co-operation between organisations ............................ 22
   2.1.7. Independent review of information security ................... 23
7799 Key Controls

1. Information security policy document
2. Allocation of information security responsibilities
3. Information security education and training
4. Reporting of security incidents
5. Virus controls
6. Business continuity planning process
7. Control of proprietary software copying
8. Safeguarding of organizational records
9. Data protection
10. Compliance with security policy

Can you think of ‘Key Controls’ missing?
How to get organizations ‘secure’?

- Information security primarily deals with managing (residual) risks by choosing appropriate controls.
- With other risks (for instance financial, operational) these are positioned with the appropriate management, e.g., ‘Chief Financial Officer’, ‘Head of Treasury’.
- Information is typically created or used in things the organizations ‘does’, i.e., business processes such as sales, administration, HR. Risks related to ‘information’ are intertwined with these business process.
- Of course, there are more risks than information security risks that jeopardize business processes, think of financial risks or operational risks, safety risks. Typically the responsibility dealing with those risks is placed with a ‘manager’.
More risks in organizations

- **Environmental Risks**
  - Capital Availability
  - Regulatory, Political, and Legal
  - Financial Markets and Shareholder Relations

- **Process Risks**
  - Operations Risk
  - Empowerment Risk
  - Information Processing / Technology Risk
  - Integrity Risk
  - Financial Risk

- **Information for Decision Making**
  - Operational Risk
  - Financial Risk
  - Strategic Risk
How to get organizations ‘secure’?

• The responsibility for information security should also be placed at the manager level that is responsible for the business process.

• The responsibility for information security should *not* be placed at the ICT department as they typically do not know all characteristics of the business processes!

• The ‘security officer’ is *not* responsible for information security but making sure that other take their responsibility..
Dealing with ‘risks’ that (negatively) influence an organization is called Enterprise Risk Management (ERM). It is an essential part of Corporate Governance, i.e. the way an organization is ‘run’.

Information security is part of ERM

Information and Communication Technology (ICT) introduces more risks to organizations than information security risks.

Corporate Governance ≥ ICT Governance ≥ Information Security
Entrance of ISO 27001

- Based on the ideas of quality management systems (ISO 9001)
- Many such management systems exist, e.g.:
  - Quality management (ISO 9001)
  - Information Security management (ISO 27001)
  - Digital Certificate management (ETSI TS 101 456)
  - Environment management (ISO 14001)
  - Occupational Health & Safety management (BSI OHSAS 18001)
- As with all management systems also an organization’s ISO 27001 implementation can be formally certified (discussed in a later lecture in more detail)
Entrance of ISO 27001

- 1989: UK Department of Trade and Industry's (DTI) publishes "Users Code of Practice" (C)
- 1995: Code of Practice published as British standard BS 7799 (C)
- 1998: BS7799-2, guidance document on implementing BS7799 based on management system (M)
- 1999: BS 7799 published as ISO standard 17799 (C)
- 2005: ISO 17799 revised and renamed to ISO 27002 (C)
- 2005: updated version of BS7799-2 became ISO 27001 standard (M)
- The ISO 27001 normatively refers to ISO 27002, so effectively ISO 27001 consists of both:
  - ISO 27002: contains a comprehensive list of controls (C)
  - ISO 27001: process description to select & implement controls (M)
ISO 27001

- Key message of ISO 27001: information security is an improvement process (and not a product!)
- Management involvement explicitly stipulated
- ISO 27001 is based on a (simple!) Plan-Do-Check-Act cycle also known as the Deming cycle.
ISO 27001

Figure 1 — PDCA model applied to ISMS processes
ISO 27001

Management

Information Security Management System

Risks to Business processes
Legal, regulatory, contractual
(security) requirements

Organization level

(Managed) Information security controls

ISO 27002
ISO 27001 acceptance

- Het ‘Besluit voorschrift informatiebeveiliging rijksdienst 2007’ states the requirements that should be met by the Dutch central government on information security.
- Although the requirements do not state it directly, the explanation that accompanies the regulation (‘Memorie van toelichting’) refers to ISO 27001 as an example implementation.

VIR 2007 can be obtained from [http://wetten.overheid.nl](http://wetten.overheid.nl) by looking for ‘voorschrift informatiebeveiliging rijksdienst’
ISO 27001 acceptance

Number of Certificates Per Country

<table>
<thead>
<tr>
<th>Country</th>
<th>Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan</td>
<td>3862</td>
</tr>
<tr>
<td>India</td>
<td>526</td>
</tr>
<tr>
<td>China</td>
<td>492</td>
</tr>
<tr>
<td>UK</td>
<td>477</td>
</tr>
<tr>
<td>Taiwan</td>
<td>431</td>
</tr>
<tr>
<td>Germany</td>
<td>174</td>
</tr>
<tr>
<td>Korea</td>
<td>106</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>103</td>
</tr>
<tr>
<td>USA</td>
<td>101</td>
</tr>
<tr>
<td>Spain</td>
<td>75</td>
</tr>
<tr>
<td>Hungary</td>
<td>68</td>
</tr>
<tr>
<td>Italy</td>
<td>68</td>
</tr>
<tr>
<td>Poland</td>
<td>58</td>
</tr>
<tr>
<td>Malaysia</td>
<td>55</td>
</tr>
<tr>
<td>Ireland</td>
<td>42</td>
</tr>
<tr>
<td>Thailand</td>
<td>41</td>
</tr>
<tr>
<td>Austria</td>
<td>39</td>
</tr>
<tr>
<td>Romania</td>
<td>35</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>32</td>
</tr>
<tr>
<td>Greece</td>
<td>30</td>
</tr>
<tr>
<td>Australia</td>
<td>29</td>
</tr>
<tr>
<td>Singapore</td>
<td>29</td>
</tr>
<tr>
<td>Mexico</td>
<td>27</td>
</tr>
<tr>
<td>France</td>
<td>26</td>
</tr>
<tr>
<td>Turkey</td>
<td>24</td>
</tr>
<tr>
<td>Brazil</td>
<td>23</td>
</tr>
<tr>
<td>Slovakia</td>
<td>23</td>
</tr>
<tr>
<td>UAE</td>
<td>20</td>
</tr>
<tr>
<td>Slovenia</td>
<td>19</td>
</tr>
<tr>
<td>Macau</td>
<td>18</td>
</tr>
<tr>
<td>Croatia</td>
<td>17</td>
</tr>
<tr>
<td>Netherlands</td>
<td>16</td>
</tr>
<tr>
<td>Philippines</td>
<td>15</td>
</tr>
<tr>
<td>Iran</td>
<td>14</td>
</tr>
<tr>
<td>Pakistan</td>
<td>14</td>
</tr>
<tr>
<td>Vietnam</td>
<td>14</td>
</tr>
<tr>
<td>Iceland</td>
<td>13</td>
</tr>
<tr>
<td>Indonesia</td>
<td>13</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>13</td>
</tr>
<tr>
<td>Colombia</td>
<td>11</td>
</tr>
<tr>
<td>Kuwait</td>
<td>11</td>
</tr>
<tr>
<td>Norway</td>
<td>10</td>
</tr>
<tr>
<td>Portugal</td>
<td>10</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>10</td>
</tr>
<tr>
<td>Sweden</td>
<td>10</td>
</tr>
<tr>
<td>Canada</td>
<td>9</td>
</tr>
<tr>
<td>Switzerland</td>
<td>9</td>
</tr>
<tr>
<td>Bahrain</td>
<td>8</td>
</tr>
<tr>
<td>Egypt</td>
<td>5</td>
</tr>
<tr>
<td>Oman</td>
<td>5</td>
</tr>
<tr>
<td>Peru</td>
<td>5</td>
</tr>
<tr>
<td>South Africa</td>
<td>5</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>5</td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>4</td>
</tr>
<tr>
<td>Lithuania</td>
<td>4</td>
</tr>
<tr>
<td>Morocco</td>
<td>4</td>
</tr>
<tr>
<td>Chile</td>
<td>3</td>
</tr>
<tr>
<td>Gibraltar</td>
<td>3</td>
</tr>
</tbody>
</table>

Total: 7346
ISO 27001 acceptance

Source: www.iso27001certificates.com

June 2009

Radboud Universiteit Nijmegen
Digital Security Group
Future of the ISO 27000 series

• ISO/IEC 27000 Fundamentals and vocabulary, 2009
• ISO/IEC 27001 ISMS - Requirements (revised BS 7799 Part 2:2005), 2005
• ISO/IEC 27003 ISMS implementation guidance, 2010
• ISO/IEC 27004 Information security management measurement, 2009
• ISO/IEC 27005 Information security risk management, 2008
• ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems, 2007
• ISO/IEC 27007 Guidelines for information security management systems auditing, under development
• ISO/IEC 27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002, 2008
Variants on ISO 2700* for medical sector

- In the Netherlands a variant on ISO 27002 is developed specifically for the medical sector:
  - NEN 7510: Medische informatica - Informatiebeveiliging in de zorg – Algemeen
  - NEN 7511-1 Medische informatica - Informatiebeveiliging in de zorg - Toetsbaar voorschrift bij NEN 7510 voor complexe organisaties
  - NEN 7511-2 Medische informatica - Informatiebeveiliging in de zorg - Toetsbaar voorschrift bij NEN 7510 voor samenwerkingsverbanden
  - NEN 7511-3 Medische informatica - Informatiebeveiliging in de zorg - Toetsbaar voorschrift bij NEN 7510 voor solopraktijken
  - NEN 7512: Medische informatica Informatiebeveiliging in de zorg – Vertrouwensbasisvoor gegevensuitwisseling
Variants on ISO 2700* for medical sector

• There also exists an ISO standard (27799) variant on the ISO 27001 for the medical sector ‘Health informatics - Information security management in health using ISO/IEC 27002.

• ISO 27799 is giving a new direction to ISO 27001; in essence it does supplements ISO 27001 management system with minimal security controls to be taken from ISO 27002, i.e. irrespective of the organization’s risk assessment. In fact the ISO 27799 distinguishes ISO 27002 controls that shall implemented and that should be implemented.

• Controls that shall be implemented include: confidentiality agreements, addressing security in third part agreements, Information security awareness, education and training, removal of access rights and disposal of media.

• Currently NEN 7510 is being revised in this direction.
Legal status of NEN 7510

- Since the June 1, 2008, the Dutch law on the usage of the Dutch social security number (BSN) in the health sector is enacted.
- By this law, it is mandatory for the health sector to use the BSN number from 1 June 2009 forward. Article 2 of the law states that care providers need to be compliant with the NEN 7510 standard on information security.
- This year (2010), care providers are being audited against this standard. The Dutch Health Care Inspectorate (Inspectie voor de gezondheidszorg) is monitoring this.
Developed by the National Institute of Standards and Technology (NIST) under the Federal Information Security Management Act (FISMA)
Variants on ISO 2700* by BSI

- The Bundesamt für Sicherheit in der Informationstechnik (BSI) is a German federal office that is the central IT security service provider for the German government.
• Analyzing the differences and similarities between the ISO 27000, NIST and BSI schemes would be an interesting research project.
• The IT-Grundschutz contains very detailed security configurations of a large variety of systems. For instance; what would a sensible thing to do in the security configuration of an answering machine?
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
ISO 27001 clauses

• ISO 27001 consists of about 94 requirements (depending on how you count) that contain some redundancy
• ISO 27001 clause 4.2.1g) ‘normatively’ refers to the ISO 27002 control objectives and controls as a minimum.
• Some overlap in ISO 27001 with ISO 27002:
  • Requirements on IS policy (Ch. 5)
  • Asset management (Ch. 7)
  • Awareness programs (part Ch. 8)
  • Security incident management (Ch. 13)
ISO 27001

- **Plan:**
  - define ISMS
    - Information security policy
    - Scope
    - Determine assets (‘anything that has value to the organization’)
    - Approach to risk assessment
    - Management processes
    - select controls using risk assessment [↩ISO 27002]
    - decide how to ‘measure’ effectiveness of selected controls
- **Do:**
  - Implement management processes
  - Implement selected controls
- **Check:**
  - Internal review of management processes
  - Internal review of selected controls
- **Act:**
  - Perform management review (e.g. based on security incidents, ‘effective measurements’)
  - Adjust ISMS
4. Information security management system
4.1 General requirements
4.2 Establishing and managing the ISMS
4.2.1 Establish the ISMS (‘plan’)

- Document scope and boundaries
- Document ISMS policy
- Identify the assets
- Develop and document risk assessment methodology
- Conduct risk assessment on the assets
- Select controls for the treatment of risk
- Management approval of residual risks
- Implement and operate ISMS
- Prepare Statement of Applicability
Attention points

1. ISO 27001 (4.2.1 j)) requires the formulation of a Statement of Applicability that includes:
   - the control objectives and controls selected as part of the risk assessment and the reasons for their selection;
   - the control objectives and controls currently implemented and
   - the exclusion of any control objectives and controls in ISO 27002 and the justification for their exclusion.
The ISO 27001 clauses

The clauses

4.2.2 Implement and operate the ISMS (‘do’)
  • Formulate Risk Treatment Plan
  • Implement selected controls
  • Document how to measure the effectiveness of selected controls
  • Implement training and awareness programs
  • Implement ISMS
  • Implement response to security incidents

4.2.3 Monitor and review the ISMS (‘check’)
  • Regular reviews / internal audits of ISMS effectiveness
  • Measurement effectiveness of controls
  • Review risk assessments at planned intervals

4.2.4 Maintain and improve the ISMS (‘act’)
  • Implement the identified improvements
<table>
<thead>
<tr>
<th>The ISO 27001 clauses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The clauses</strong></td>
</tr>
<tr>
<td>4.3 Documentation requirements</td>
</tr>
<tr>
<td>4.3.1 General</td>
</tr>
<tr>
<td>4.3.2 Control of documents</td>
</tr>
<tr>
<td>4.3.3 Control of records</td>
</tr>
<tr>
<td>5 Management responsibility</td>
</tr>
<tr>
<td>5.1 Management commitment</td>
</tr>
<tr>
<td>• Management shall provide evidence of its commitment</td>
</tr>
<tr>
<td>5.2 Resource management</td>
</tr>
<tr>
<td>5.2.1 Provision of resources</td>
</tr>
<tr>
<td>• The organization shall determine and provide the resources needed</td>
</tr>
<tr>
<td>5.2.2 Training, awareness and competence</td>
</tr>
<tr>
<td>6 Internal ISMS audits ('check')</td>
</tr>
</tbody>
</table>
7 Management review of the ISMS (‘act’)

7.1 General
• Management shall review the organization’s ISMS at planned intervals (at least once a year)

7.2 Review input
• Take into account feedback from interested parties, internal audits, effectiveness measurements, security incidents

7.3 Review output
• The output from the management review shall include any decisions and actions

8 ISMS improvement

8.1 Continual improvement
• The organization shall continually improve the effectiveness of the ISMS

8.2 Corrective action
1. ISO 27001 (4.2.1) requires the formulation of a Statement of Applicability that includes:

- the control objectives and controls selected as part of the risk assessment and the reasons for their selection;
- the control objectives and controls currently implemented and the exclusion of any control objectives and controls in ISO 27002 and the justification for their exclusion.

2. ISO 27001 (4.2.2d) requires measurement of the effectiveness of the selected controls or groups of controls and a specification of the control objectives and controls selected as part of the risk assessment.

3. ISO 27001 (4.3.1) requires that the selected controls can be linked back to results of the risk assessment.

Attention points
## Measurement examples

<table>
<thead>
<tr>
<th>H</th>
<th>ISO 27002</th>
<th>Measurement example</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Security Policy</td>
<td>% of people that are aware of it</td>
</tr>
<tr>
<td>6</td>
<td>Organization of Information Security</td>
<td># incidents w.r.t. responsibility allocation</td>
</tr>
<tr>
<td>7</td>
<td>Asset Management</td>
<td>% of system components in CMDB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% of systems w. allocated responsibility</td>
</tr>
<tr>
<td>8</td>
<td>Human resources security</td>
<td># of staff violations</td>
</tr>
<tr>
<td>9</td>
<td>Physical and Environmental Security</td>
<td>% of staff wearing badges</td>
</tr>
<tr>
<td></td>
<td></td>
<td># of unattended visitors.</td>
</tr>
<tr>
<td>10</td>
<td>Communications and Operations Management</td>
<td># of unsuccessful backups</td>
</tr>
<tr>
<td></td>
<td></td>
<td># lost backup media</td>
</tr>
<tr>
<td></td>
<td></td>
<td># successful virus attacks</td>
</tr>
<tr>
<td>11</td>
<td>Access Control</td>
<td>% of easily guessed passwords</td>
</tr>
<tr>
<td>12</td>
<td>Information Systems Acquisition, Development and Maintenance</td>
<td># new systems without risk assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td># security incidents with new systems</td>
</tr>
<tr>
<td>13</td>
<td>Information Security Incident Management</td>
<td>% of security incidents reported</td>
</tr>
<tr>
<td></td>
<td></td>
<td># of repeated security incidents</td>
</tr>
<tr>
<td>14</td>
<td>Business Continuity Management</td>
<td># of downtime incidents not consistent with service level agreements</td>
</tr>
<tr>
<td>15</td>
<td>Compliance</td>
<td># of complaints</td>
</tr>
</tbody>
</table>
ISO 27001 challenges

• Finding the right balance between the (theoretical) standard and pragmatism.
• The avoidance of just creating a lot of paperwork
• Actually getting your organization more ‘secure’ in a practical sense as a result of ISO 27001 implementation.

.. and of course the intrinsic challenges:
• Multidisciplinary nature (technical, organizational, human)
• Constraints on budget and effort
• Constraints on attention
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• **Determining the ISMS ‘scope’**
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
Determine the scope

- Relevant clause from ISO 27001 is 4.2.1a): ‘Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope’.
Determine the scope

- If an organization, say A, has outsourced its IT to another company, say B, this does not mean that the information security of the outsourced systems is the sole responsibility of B.
- From an ISO 27001 perspective, and in fact from any reasonable perspective, A stays responsible for the information security of the outsourced systems.
- This means that A should conduct a risk assessment resulting in security controls and impose those on B in a Service Level Agreement (SLA).
- If B itself is ISO 27001 compliant then this might be sufficient, otherwise A should also somehow monitor B’s compliance with the SLA.
• It is tempting for organizations to choose a narrow scope. For instance for organization B that provides outsourcing services then it is tempting to let the ISO 27001 scope only consist of the outsourcing department itself and not the other departments of B such HR, facilities, finance.

• The drawback of this is that all other departments of organization B that provide security relevant services (HR, Facilities) to the outsourcing department, become formally ‘external’ to the outsourcing department. This means that the outsourcing department needs to make formal requirements with the other departments on security and to monitor compliance.
Outline

Theory

• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001

• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
ISO/IEC 27002

0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4. Conduct information security risk assessment
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
6. Develop ISMS implementation program
7. ISMS implementation program
8. Information Security Management System
9. ISMS operational artifacts
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
14. Party on!

Inventory

PDCA cycle (one of many)

ISO/IEC 27001

Key
- Activity
- Database
- Document or output
- ISO/IEC standard

Source: http://www.iso27001security.com
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• **Choice #1: clustering assets in information systems**
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
‘Identify the assets’

- Perhaps surprising, this is rather hard in practice.
- Organizations often do not even have a clear understanding of their ‘information systems’ or ‘applications’, let alone of the residing ‘components’.
- This also implies that the responsibility for information security of the information systems is often not properly allocated.
- ISO 27001/27002 do not define the notion ‘information system’, so we use a definition from Wikipedia: ‘a system of people, data records and activities that process the data and information in an organization, and it includes the organization's manual and automated processes’.
‘Identify the assets’

• An information system is closely aligned with a business process for which a line manager is responsible.

• Although ISO 27001 does not explicitly mandates it, any reasonable sized organization should have a clear inventory of their information systems and allocated information security responsibilities for them to line management.

• In an ISO 27001 implementation it is a reasonable choice to use the information system inventory as the asset clustering.

• Why is making the ICT department responsible for the information security of all information systems not a good idea?
Choice #1: clustering assets in information systems

Systems and allocating responsibilities

Disjoint information systems

- Department #1
  - Manager #1
  - Business Process #1
  - Information System #1

- Department #2
  - Manager #2
  - Business Process #2
  - Information System #2

- Department #3
  - Manager #3
  - Business Process #2
  - Information System #3

Uncommon but easy
Allocating responsibilities

Information systems using common resources

Choice #1: clustering assets in information systems
Allocating responsibilities

Interconnected information systems

Department #1
Manager #1
Business Process #1
Information System #1

Department #2
Manager #2
Business Process #2
Information System #2

Department #3
Manager #3
Business Process #2
Information System #3

Choice #1: clustering assets in information systems

Occurs and difficult
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• **Choice #2: using the ‘combined approach’ for risk assessment**
• Baseline selection
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
BIAs & RATs

- By using a high level risk analysis (Business Impact Analysis or BIA) decide what the organization’s critical information systems are.
- An information system is called critical when one of its CIA characteristics is ‘High’ otherwise it is non-critical.
BIAs & RATs

- Non-critical information systems solely rely on ‘baselines’ for their information security, i.e. minimal sets of security controls.
- Baselines also apply to the critical information systems but in addition a detailed level risk analysis (Risk Assessment and Treatment or RAT) is conducted, leading to possible controls additional to the baselines.
- This is reminiscent to the ‘key control’ setup of the old BS7799, it is also the direction taken in ISO 27799.

Critical systems

Billing  CRM  Telephone  ERP  Document management  Email  Treasury  

Baseline security
BIAs & RATs

- Non-critical information systems solely rely on ‘baselines’ for their information security, i.e. minimal sets of security controls.
- Baselines also apply to the critical information systems, in addition a detailed level risk analysis (Risk Assessment and Treatment or RAT) is conducted, leading to possible controls additional to the baselines.
- This is reminiscent to the ‘key control’ setup of the old BS7799, it is also the direction taken in ISO 27799.

We will discuss risk assessments in the next lecture.
BIAs & RATs

Choice #2: using the 'combined approach' for risk assessment
Choice #2: using the ‘combined approach’ for risk assessment

**BIAs & RATs**

1. **Information System inventory**
2. **Allocation of ownership**
3. **Conducting Business Impact Analyse (BIA)**
4. **Conducting Risk Assessment and Treatment (RAT)**

- **Baseline security**
- **Critical systems**
  - Billing
  - CRM
  - Telephone
  - ERP
  - Document management
  - Email
  - Treasury
  - ....

- **Continuous**
- **Review e.g. every 2 years**
- **E.g. every 2 years**

Radboud Universiteit Nijmegen
Digital Security group
### Example BIA questions & Answers for patient record system

Choice #2: using the 'combined approach' for risk assessment

<table>
<thead>
<tr>
<th>Criteria related to Confidentiality</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Example BIA questions & Answers for patient record system

## Confidentiality: Organizational impact when information in the system is compromised

<table>
<thead>
<tr>
<th>Question</th>
<th>Impact</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy sensitivity of data</td>
<td>None</td>
<td>Standard registry (e.g., memberships)</td>
</tr>
<tr>
<td>Financial loss as result of information disclosure</td>
<td>&lt; 2,5k</td>
<td>2,5k -- 50k</td>
</tr>
<tr>
<td>Possible fraud as a result of information disclosure</td>
<td>&lt; 2,5k</td>
<td>2,5k -- 50k</td>
</tr>
<tr>
<td>Reputation loss as a result of information disclosure</td>
<td>No negative publicity</td>
<td>Local negative publicity</td>
</tr>
<tr>
<td>Liability issues as a result of information disclosure</td>
<td>None</td>
<td>Limited</td>
</tr>
<tr>
<td>To what extent can information disclosure lead to injuries</td>
<td>None</td>
<td>Serious injuries</td>
</tr>
</tbody>
</table>

**Result**

- Low
- Medium
- High

Choice #2: using the 'combined approach' for risk assessment
Example BIA questions & Answers for patient record system

**Integrity:** Organizational impact when information is incorrect

<table>
<thead>
<tr>
<th>Question</th>
<th>Impact</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial loss as result of unintentional changes in information</td>
<td>&lt; 2,5k, 2,5k -- 50k, &gt; 50k</td>
<td></td>
</tr>
<tr>
<td>Financial loss as result of intentional changes in information (fraud)</td>
<td>&lt; 2,5k, 2,5k -- 50k, &gt; 50k</td>
<td></td>
</tr>
<tr>
<td>Reputation loss as a result of incorrect information</td>
<td>No negative publicity, Local negative publicity, National negative publicity</td>
<td></td>
</tr>
<tr>
<td>Liability issues as a result of incorrect information</td>
<td>None, Limited, High</td>
<td></td>
</tr>
<tr>
<td>Possible wrong management decisions as a result of incorrect information</td>
<td>None, Limited, High</td>
<td></td>
</tr>
<tr>
<td>Safety dangers as a result of incorrect information</td>
<td>None, Serious injuries, Loss of life</td>
<td>PATIENT DATA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Result</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
</table>
**Example BIA questions & Answers for patient record system**

### Availability: Organizational impact when the system is unavailable

<table>
<thead>
<tr>
<th>Question</th>
<th>Duration</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable downtime before substantial financial loss (&gt; 50k) occurs</td>
<td>&gt; 1 day</td>
<td>&lt; 1 day  &lt; 4 hours</td>
</tr>
<tr>
<td>How long is manual processing as an alternative feasible</td>
<td>&gt; 1 day</td>
<td>&lt; 1 day  &lt; 4 hours</td>
</tr>
<tr>
<td>After what downtime are important management decisions no longer possible</td>
<td>&gt; 1 day</td>
<td>&lt; 1 day  &lt; 4 hours</td>
</tr>
<tr>
<td>After what downtime is the reputation of the organization in danger</td>
<td>&gt; 1 day</td>
<td>&lt; 1 day  &lt; 4 hours</td>
</tr>
<tr>
<td>After what downtime external requirements are no longer met</td>
<td>&gt; 1 day</td>
<td>&lt; 1 day  &lt; 4 hours</td>
</tr>
<tr>
<td>How many employees can not work when the system is unavailable</td>
<td>1%</td>
<td>10%</td>
</tr>
<tr>
<td>To what extent can unavailability lead to injuries</td>
<td>None</td>
<td>Serious injuries</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• **Baseline selection**
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
Baselines

- Selecting ‘appropriate’ ISO 27002 controls and underlying guidelines
- Clustering them in into procedures and handbooks
- ISO 27002 is technology neutral, so adopting technical baselines (e.g., on Windows, Linux, Cisco) is important too from a pragmatic perspective
- Finding the right balance between cost and effectiveness in selecting baselines is challenging.

1. Information security policy
2. ISMS handbook
3. ISMS reporting forms
4. Security organization, tasks and responsibilities
5. HR security procedures
6. Security instructions external parties
7. Handbook ICT administration
8. Handbook physical security
9. Employee security instructions
10. IS awareness, education and training program
11. Management security instructions
12. Technical baselines infrastructural security
13. Access policy
14. Security incident and vulnerability procedure
15. Privacy regulations
16. Specific IS requirements for primary suppliers
Technical baseline examples

Solutions for Security and Compliance

Version 2.0

Source: www.microsoft.com


Router Security Guidance Activity of the Systems and Network Attack Center (SNAC)

Author: Neal Ziring
23 May 2005
Version: 1.0

National Security Agency
9800 Savage Rd, Suite 6704
Ft. Meade, MD 20755-6704

SNAC.Guides@nsa.gov

Source: www.nsa.gov
<table>
<thead>
<tr>
<th>Who</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior management</td>
<td>Providing resources, management review (Act)</td>
</tr>
<tr>
<td>Security officer</td>
<td>Steering, guidance, monitoring (day to day) Operating ISMS</td>
</tr>
<tr>
<td>Project organization</td>
<td>Steering, drafting ISMS handbook, procedures/baselines (Plan)</td>
</tr>
<tr>
<td>Security committee</td>
<td>Approval, monitoring (Plan/Check/Act)</td>
</tr>
<tr>
<td>Business / process owner</td>
<td>Conducting risk analyses (Plan)</td>
</tr>
<tr>
<td>ICT department</td>
<td>Implementing ICT controls (Do)</td>
</tr>
<tr>
<td>Facility management</td>
<td>Implementing physical controls (Do)</td>
</tr>
<tr>
<td>Human Resource</td>
<td>Implementing HR controls (Do)</td>
</tr>
<tr>
<td>Purchasing department</td>
<td>Imposing security on external parties (Do)</td>
</tr>
<tr>
<td>Legal department</td>
<td>Legal compliance (e.g., privacy)</td>
</tr>
<tr>
<td>Internal audit department</td>
<td>Conducting audits (Check)</td>
</tr>
<tr>
<td>External auditors</td>
<td>Conducting audits (Check)</td>
</tr>
</tbody>
</table>
Determination of baselines (research)

• It would be interesting to draft (and motivate) different baselines for various types of organizations.
• The challenge is to make the baselines realistic; writing ideal baselines is trivial but those will not get implemented…
An organization can go through all the ISO 27002 controls and guidelines and determine which one would like to adopt.

But suppose that the total cost is too much?

For instance, the total cost would be 1 million Euro, while the organization only wants to spend 250 kEuro?

<table>
<thead>
<tr>
<th>Possible baseline controls</th>
<th>Cost (kEURO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1 Information security policy document</td>
<td>20</td>
</tr>
<tr>
<td>5.1.2 Review of the information security policy</td>
<td>10</td>
</tr>
<tr>
<td>6.1.1 Management commitment to information security</td>
<td>1</td>
</tr>
<tr>
<td>6.1.2 Information security coordination</td>
<td>4</td>
</tr>
<tr>
<td>6.1.3 Allocation of information security responsibilities</td>
<td>1</td>
</tr>
<tr>
<td>6.1.4 Authorization process for information processing facilities</td>
<td>4</td>
</tr>
<tr>
<td>6.1.5 Confidentiality agreements</td>
<td>14</td>
</tr>
<tr>
<td>6.1.6 Contact with authorities</td>
<td>1</td>
</tr>
<tr>
<td>6.1.8 Independent review of information security</td>
<td>25</td>
</tr>
<tr>
<td>6.2.1 Identification of risks related to external parties</td>
<td>5</td>
</tr>
<tr>
<td>6.2.3 Addressing security in third party agreements</td>
<td>13</td>
</tr>
<tr>
<td>7.1.1 Inventory of assets</td>
<td>50</td>
</tr>
<tr>
<td>7.1.2 Ownership of assets</td>
<td>2</td>
</tr>
<tr>
<td>7.1.3 Acceptable use of assets</td>
<td>2</td>
</tr>
<tr>
<td>TOTAL</td>
<td>1000</td>
</tr>
</tbody>
</table>
Determination of baselines (research)

- Try to associate to each of the selected controls a measure of ‘mitigation efficiency’, i.e., the extent it reduces generic risks.
- Find a subset of the selected controls with maximum efficiency that cost less than 250 kEuro (in mathematical terms a knapsack problem).
- Problem: how to determine ‘mitigation efficiency’?

### Possible baseline controls

<table>
<thead>
<tr>
<th>Control Description</th>
<th>Cost (KEURO)</th>
<th>Mitigation efficiency (0-5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1 Information security policy document</td>
<td>20</td>
<td>5</td>
</tr>
<tr>
<td>5.1.2 Review of the information security policy</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>6.1.1 Management commitment to information security</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.2 Information security coordination</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6.1.3 Allocation of information security responsibilities</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.4 Authorization process for information processing facilities</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>6.1.5 Confidentiality agreements</td>
<td>14</td>
<td>4</td>
</tr>
<tr>
<td>6.1.6 Contact with authorities</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>6.1.8 Independent review of information security</td>
<td>25</td>
<td>2</td>
</tr>
<tr>
<td>6.2.1 Identification of risks related to external parties</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6.2.3 Addressing security in third party agreements</td>
<td>13</td>
<td>5</td>
</tr>
<tr>
<td>7.1.1 Inventory of assets</td>
<td>50</td>
<td>3</td>
</tr>
<tr>
<td>7.1.2 Ownership of assets</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>7.1.3 Acceptable use of assets</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>1000</strong></td>
<td></td>
</tr>
</tbody>
</table>
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• **Typical topics in an ISMS management review**
• High level description of implementation project

• Recap
• Assignment & study for next week
Topics in management review (input)

1. Results of control effectiveness measurements
2. Results of independent security reviews (e.g., accountants)
3. Results of internal security reviews
4. Feedback and complaints of interested parties (e.g., clients)
5. Changes effecting information security (e.g., organization, contractual or legal conditions)
6. Status of corrective actions (results of earlier reviews)
7. Results of information security programs (including status of conducted risk assessments)
8. Reported information security incidents and trends
9. Recommendations done by the authorities
10. Information security trends in general
Possible management review actions (output)

1. Revision of information security policies
2. Revision of the information security framework (including risk assessment and -treatment methodology)
3. Revision of budget and / or responsibilities
4. Initiation of new information security programs
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• Typical topics in an ISMS management review
• **High level description of implementation project**

• Recap
• Assignment & study for next week
Example of implementation project

High level description of implementation project

![Diagram of implementation project process]

- **ISMS Organisation**
  - Design IS process (handbook)
  - Security Officer Appointment
  - Security Organization setup
  - Implementing IS Process (handbook)

- **Basic controls**
  - ISO 27002
  - Determining Relevant controls
  - Design and build of controls
  - Control Implementation

- **IT system Controls**
  - Asset inventory (IT systems)
  - Sanity check & responsibility allocation
  - Impact analysis (BIA)
  - Risk Analysis (RAT)

- **PROJECT**
  - Project plan + Cost / Profit analysis

**FASE**
- FASE I
- FASE II
- FASE III

Radboud Universiteit Nijmegen
Digital Security group
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
Recap on information security

Recap

• ISO 27001 describes a ‘security management system’, a methodology to select and maintain security controls (from ISO 27002) based on risk assessments. This system is called Information Security Management System (ISMS)
• Fundamental to ISO 27001 is that it considers IS as a continual improvement process and not as a product
• The ISMS scope is an important decision
• This process is known as the PDCA cycle, risk assessment is the engine within this cycle
• ISO 27001 leaves room for various implementations, getting a more secure organization instead of a ‘paper tiger’ is an attention point
• An organization’s ISO 27001 implementation can be formally certified
• We have seen an implementation based on the ‘combined approach’ based on assets clustered in information systems
Outline

Theory
• Recap on information security
• ISO 27001/27002 introduction
• The ISO 27001 clauses
• Determining the ISMS ‘scope’
• The ISO 27001 implementation process based on iso27k forum

An example implementation of ISO 27001
• Choice #1: clustering assets in information systems
• Choice #2: using the ‘combined approach’ for risk assessment
• Baseline selection
• Typical topics in an ISMS management review
• High level description of implementation project

• Recap
• Assignment & study for next week
Assignment & study for next week

• In the practicum you can start working on the assignment of writing an information security policy in the sense of ISO 27002.
• Study for next week:
  • The ISO 27005 standard
  • The NIST Special Publication 800-30: ‘Risk management Guide for Information Technology Systems’ (see the SIO website).