ISO-2700x Implementation & Audit
Training Summary

ISO/IEC 27000

• Management System: a system to establish and achieve policy and objectives.
• Process: a set of interrelated or interacting activities which transforms inputs into outputs.
• Policy: an organization's overall intention and direction as formally expressed by management
• Record: document stating results achieved or providing evidence of activities performed
ISO/IEC 27001 & ISO/IEC 27002

ISO/IEC 27001
Requirements for “Information Security Management Systems”

ISO/IEC 27002
Code of Practice for Information Security Management

ISO-27001

0 – Introduction
1 – Scope
2 – Normative references (related standards)
3 – Terms and definitions
4 – Information security management system
5 – Management responsibility
6 – Internal ISMS audits
7 – Management review of the ISMS
8 – ISMS Improvement
Annex A – Control objectives and controls
Other Annexes
Bibliography
Five mandatory requirements

• Section 4 – Information Security management System
  • 4.1 General requirements
    “The Organization shall establish, implement, operate, monitor, review and improve a documented ISMS within the context of the organization’s overall business activities and risks it faces. For the purposes of this standard the process used is based on PDCA model…”
  • 4.2 Establishing and maintaining and ISMS
    • 4.2.1 Establish
    • 4.2.2 Implement & operate
    • 4.2.3 Monitor & review
    • 4.2.4 Maintain & improve
  • 4.3 Documentation Requirements

ISO-27001:2005 Structure

• Section 5 - Management Responsibility
  • Management Commitment
  • Resource Management
• Section 6 – Internal ISMS Audits
• Section 7 - Management Review of the ISMS
  • Review Input
  • Review Output
• Section 8 - ISMS Improvement
  • Continual Improvement
  • Corrective Action
  • Preventive Action
ISO-27001:2005 Structure

Annex A Management Controls
A.5 Security Policy
A.6 Organization of Information Security
A.7 Asset Management
A.8 Human Resources Security
A.9 Physical and Environment Security
A.10 Communication and Operations Management
A.11 Access Control
A.12 Information Systems acquisition, development & maintenance
A.13 Information Security Incident management
A.14 Business Continuity Management
A.15 Compliance

Deming Cycle for IS

**Plan:** Establish the ISMS
Scope - Policy - Risk Assessment - Controls

**Do:** Implement and operate the ISMS
Risk Treatment Plan - Training & Awareness

**Check:** Monitor and Reviews the ISMS
Monitor - ISMS audits - ISMS Reviews

**Act:** Maintain and Improve the ISMS
Continual Improvements
4.2.1 Establish the ISMS

- Define the scope and boundaries of the ISMS …
- Define an ISMS policy …

c) Define a systematic approach to **risk assessment** …method, risk acceptance criteria, …
d) Identify the risks …assets, threats, vulnerabilities,…
e) Assess the risks …impact, likelihood,…
f) Identify and evaluate options for the treatment of risks …controls, accept risks, avoid, transfer,…
g) Select control objectives and controls for the treatment of risks …from Annex A…
h) Management approval of residual risks
i) Management authorization to implement and operate the ISMS
j) Prepare Statement of Applicability
ISO/IEC 27005: Info Sec Risk Mgt.

- ESTABLISH CONTEXT
- RISK ASSESSMENT
  - RISK ANALYSIS
  - RISK IDENTIFICATION
  - RISK ESTIMATION
  - RISK EVALUATION
- RISK TREATMENT
  - RISK AVOIDANCE
  - RISK TRANSFER
  - RISK REDUCTION
  - RISK ACCEPTANCE
- RISK COMMUNICATION
- RISK MONITORING AND REVIEW
- RISK ACCEPTANCE

Risk Assessment / Mgt methods

- AUSTRIAN IT SECURITY HANDBOOK
- CRAMM
- DUTCH A&K ANALYSIS
- EBIOS
- ISF METHODS FOR RISK ASSESSMENT AND RISK MANAGEMENT
- ISO/IEC IS 13335-2 (ISO/IEC IS 27005)
- ISO/IEC IS 17799:2005
- IT-GRUNDSCHUTZ (IT BASELINE PROTECTION MANUAL)
- MARION
- MEHARI
- OCTAVE V2.0 (AND OCTAVE-S V1.0 FOR SMALL AND MEDIUM BUSINESSES)
- SP800-30 (NIST)
**Risk management Tools**

- CALLIO
- CASIS
- COBRA
- COUNTERMEASURES
- CRAMM
- EBIOS
- GSTOOL
- ISAMM
- OCTAVE
- PROTEUS
- RA2
- RISKWATCH

**References**

Articles & presentations:
- ENISA ad hoc working group on risk assessment and risk management, *Inventory of risk assessment and risk management methods*
- GAO, *Information Security Risk Assessment: Learning from Leading Organizations*
- NIST, *Sp800-30, Risk Management Guide for Information Technology Systems*
- ISO/IEC 27001; ISO/IEC 17799

- [www.enisa.europa.eu/rmra](http://www.enisa.europa.eu/rmra)
- [www.gao.gov](http://www.gao.gov)
- [www.nist.gov](http://www.nist.gov)
- [www.iso.ch; www.nen.nl](http://www.iso.ch; www.nen.nl)
Question

“Is implementation of control X.x.x (27001 Annex A) mandatory?”

Answer (1)

1. Yes, you need X because it is a basic security control that everyone needs. You’d be silly/negligent/risking the farm not to have it.
2. No, X is not needed because we don’t have it, therefore we consider it neither good practice nor best practice nor recommended.
3. That depends - I’m a consultant with lots of letters after my name but you’d have to pay me $$$ to answer your question.
4. No, X is unnecessary because it is more costly than the incidents it prevents. Unless we are really unlucky anyway. Do ya feel lucky, punk?
5. You tell me: have you assessed the information security risks and identified a troubling risk that control X might mitigate? Have you decided that it would be better to implement X than some other risk treatment (avoid the risk, transfer the risk, accept the risk)? Is X the most cost-effective control in this situation? Does X adequately mitigate the risk and, ideally, others too yet without making the situation worse through additional complexity, procurement/management costs or whatever? Is X feasible?
6. Yes because NIST/COBIT/SOX/a little bird says so.
7. Yes.
8. No.
9. Yes because it is “mandatory”, according to [insert favorite authority figure here].
10. No because it is “optional” and/or was not explicitly listed in black and white as absolutely mandatory by [insert favorite authority figure here too].
**Answer (2)**

11. Yes because it's the law [in country Y].
12. Only if your policies, plans, strategies, technical architecture, or internal standards say so.
13. Yes if there is a positive ROSI [Return On Security Investment], no if the ROSI is negative or if someone has seeded "reasonable doubt" or if there is something sexier on management's agenda this afternoon.
14. Yes, absolutely - I am a vendor selling X. X is all you need. X is better than sliced bread. I'd sell both my kidneys to buy X ...
15. Yes because we will get a bad audit report and/or grief from HQ if we do not have X.
16. Not necessarily now but it will definitely be required in the future. Trust me.
17. No because we cannot afford it at the moment.
18. No because if you have it, then we have to have it too, else we will appear behind the times and that is BAD.
19. Yes because we have it and you are Behind The Times.
20. Do you even have to ask? Doh!

---

**Key Controls**

<table>
<thead>
<tr>
<th>Controls Considered Essential from a Legislative Point of View</th>
<th>Controls Considered to be Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1.4 Data protection and privacy of personal information</td>
<td>5.1.1 Information security policy document</td>
</tr>
<tr>
<td>15.1.3 Protection of organizational records</td>
<td>6.1.3 Allocation of information security responsibilities</td>
</tr>
<tr>
<td>15.1.2 Intellectual property rights</td>
<td>8.2.2 Information security awareness, education, and training</td>
</tr>
<tr>
<td></td>
<td>12.2 Correct processing in applications</td>
</tr>
<tr>
<td></td>
<td>12.6 Technical vulnerability management</td>
</tr>
<tr>
<td></td>
<td>14 Business continuity management</td>
</tr>
<tr>
<td></td>
<td>13.2 Management of information security incidents and improvements</td>
</tr>
</tbody>
</table>
Top-10 security issues (random order)

1. (Management) Commitment
2. Clear Desk Policy
3. Risk assessment and Risk management
4. HR Security (joiners, during employment, leavers)
5. Security Incident Management
7. Internal Audits (Compliance)
8. (Physical) Access Control (People - Process - Technology)
9. Asset management and classification
10. Information systems and Mobile devices

Internal Audits

- An audit (process - criteria - evidence)
- The Auditor (is only human)
- The Audit Programme
- Audit Activities
  - initiating the audit
  - on-site activities
  - reporting
  - completing the audit & audit follow-up
Please…

• Course Questionnaire
• Thank you for your attendance
• **These were 5 fantastic days!**
• Good luck with your further activities in the world of **Information Security**
• Have a safe trip home and a nice weekend
• Any future questions, comments, suggestions, … to …

---

**Info**

Information-Security-Governance.com
IT Audits - Security Consulting - Training

Aart Bitter RE
**IT Auditor**

T:  +31 (599) 648 052
M:  +31 (6) 573 11 593
E:  Aart.Bitter@planet.nl
W:  www.information-security-governance.com