ISO ISMS Standards

Ted Humphreys

Charted Fellow of BCS (CITP), CISM and Convenor of ISO/IEC JTC1/SC27 WG1
ISO/IEC JTC 1/SC27 and WG1

SC 27
Chair Dr Walter Fumy
Vice-chair Dr Marijke de Soete
Secretariat Krystyna Passia

WG1
Security management standards
Convenor
Ted Humphreys

WG2
Security techniques
Convenor
Prof. Kenji Naemura

WG3
Security evaluation
Convenor
Mats Ohlin
WG1 Areas of Work

- Information security management systems (ISMS)
- Information security best practice
- Risk management
- Metrics and measurements
- Implementation guidance
- IDS
- Information security incident handling
- IT network security
- TTP services
- DR services
ISO 27000 ISMS Series

- Fundamentals and vocabulary
- ISMS requirements
- ISMS measurement
- ISMS implementation guidelines
- ISMS Risk Management
- ISM
- 17799 (from April 2007)

Published
Work in progress
Proposed new project

27000 Family
• ISO/IEC 27001 (revised version of BS 7799 Part 2:2002)

• **Publication date 15\textsuperscript{th} Oct. 2005**

• BS 7799 Part 2:2002 has now been withdrawn

• Can be used as the basis for ISMS Certification (as was BS 7799 Part 2:2002) as it designed using the same PDCA model as ISO 9001 (QMS), ISO 14001 (EMS) and ISO 22000 (FSMS) – see document SC27 N4784 for more details
• Highlights and features
  – Risk management approach
    • risk assessment
    • risk treatment
    • management decision making
  – Continuous improvement model
  – Measures of effectiveness
  – Auditable specification (internal and external ISMS auditing)
ISO 27002 (ISO/IEC 17799)

- Code of Practice for information security management
- The revised version of ISO/IEC 17799 was published on the 15th June 2005
  - Asset management, mobile code, vulnerability management, human resources, incident handling, external services together with other revision topics...
- From April 2007 ISO/IEC 17799 is expected to be renumbered as 27002
ISO 27002 (ISO/IEC 17799)

- 2005 revision highlights
  - Improvements made to cover the new risks and treats, ways of doing business, networking arrangements and technologies that have emerged over the last 5 years
  - Greater use of external services
  - Service delivery management
  - Improvements in asset management, human resources security and incident handling management
  - Vulnerability management (including patch management)
  - Mobile code threats
  - Wireless and new mobile technologies
Objective to provide implementation guidance to support the ISMS requirements standard 27001
- Detailed advice and on help regarding the PDCA processes
- ISMS Scope and policy
- Identification of assets
- Monitoring and review
- Continuous improvement
Objective to develop an Information security management measurements standard aimed at addressing how to measure the **EFFECTIVENESS** of ISMS implementations (processes and controls)

- *Performance targets, benchmarking …*
  - *What to measure, How to measure and When to measure*
- *Awareness, incident handling, audit trail analysis, application and use of procedures, access control effectiveness …*

- At 2nd working draft level
Evolution of ISO 133335 into ISO 27005

Guidelines for the management of IT security (GMITS)
- GMITS Part 1 (concepts & models)
- GMITS Part 2 (policy & planning)
- GMITS Part 3 (risk assessment)
- GMITS Part 4 (selection of controls)
- GMITS Part 5 (network management)

Management of ICT security (MICTS)
- MICTS Part 1
- MICTS Part 2

IT network security Part 1
ISO 27005 (ISMS risk management)

- ISMS Risk Management
  - MICTS-2 has been renumbered as 27005
  - Its title has been changed to information security risk management
ISO 27000 ISMS Family of standards

27001 ISMS requirements

27002 (17799 from April 2007) Code of practice for information security management

27000 ISMS Fundamentals and vocabulary

ISO 27003 ISMS implementation guidelines

ISO 27004 Information security management measurements

ISO 27005 ISMS Risk Management

Supports, adds value, contributes and gives advice on 27001 requirements and their implementation
SC27 Liaisons

- Telecoms
- ITU-T & ETSI
- WC1
- ISSA
- ISSEA
- TC65
- TC68
- TC215
- Banking
- Healthcare
- Information Security
- Safety
ITU-T Liaison with SC27 WG1

- ISMS Standards
  - ISO 27001, ISO 27002 (ISO 17799) ...
  - X.1051 ISMS Telecoms requirements
- IT Network Security
- Incident Handling
- ITU-T X.841|ISO/IEC 15816:2002 - Security information objects for access control
- ITU-T X.843|ISO/IEC 15945:2002 - Specification of TTP services to support the application of digital signatures
Current work plans and projects

Future requirements & priorities

Future plans

Links & relationships within SC27 and through liaison and collaboration

WG1 Road Map
INTERNATIONAL CERTIFICATION
Business Sectors

Argentina, Australia, Austria, Bahrain, China, Germany, Greece, Hong Kong, India, Italy, Japan, Korea, Kuwait, Norway, Romania, Singapore, Spain, UK

Telecoms 27%

Australia, Brazil, Canada, Hungary, Italy, Japan, UK, USA

Finance 20%

Germany, Japan, Korea, Spain, Sweden, Taiwan, UK, USA

Manufacturing 10%

Argentina, Australia, Austria, Bahrain, China, Germany, Greece, Hong Kong, India, Italy, Japan, Korea, Kuwait, Norway, Romania, Singapore, Spain, UK

Utilities 4%

Australia, China, Japan, Korea, Mexico, Poland, Taiwan, UK

3rd Party Services 17%

Germany, Japan, Korea, Netherlands, Singapore, UK, USA

Government 7%

China, Japan, Korea, Mexico, Poland, Taiwan, UK

IT Industry 15%

France, Germany, Italy, Japan, Korea, Taiwan, UK, USA

World Market Sectors
<table>
<thead>
<tr>
<th>Country</th>
<th>ISMS</th>
<th>Country</th>
<th>ISMS</th>
<th>Country</th>
<th>ISMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan</td>
<td>1190</td>
<td>Czech Republic</td>
<td>6</td>
<td>Bahrain</td>
<td>1</td>
</tr>
<tr>
<td>UK</td>
<td>219</td>
<td>Brazil</td>
<td>5</td>
<td>Chile</td>
<td>1</td>
</tr>
<tr>
<td>India</td>
<td>139</td>
<td>Greece</td>
<td>5</td>
<td>Egypt</td>
<td>1</td>
</tr>
<tr>
<td>Taiwan</td>
<td>69</td>
<td>Spain</td>
<td>5</td>
<td>France</td>
<td>1</td>
</tr>
<tr>
<td>Germany</td>
<td>51</td>
<td>Turkey</td>
<td>5</td>
<td>Lebanon</td>
<td>1</td>
</tr>
<tr>
<td>Italy</td>
<td>41</td>
<td>Croatia</td>
<td>4</td>
<td>Lithuania</td>
<td>1</td>
</tr>
<tr>
<td>Korea</td>
<td>35</td>
<td>Iceland</td>
<td>4</td>
<td>Luxemburg</td>
<td>1</td>
</tr>
<tr>
<td>USA</td>
<td>31</td>
<td>Philippines</td>
<td>4</td>
<td>Macau</td>
<td>1</td>
</tr>
<tr>
<td>Hungary</td>
<td>24</td>
<td>Saudi Arabia</td>
<td>4</td>
<td>Macedonia</td>
<td>1</td>
</tr>
<tr>
<td>Netherlands</td>
<td>22</td>
<td>Argentina</td>
<td>3</td>
<td>Morocco</td>
<td>1</td>
</tr>
<tr>
<td>China</td>
<td>21</td>
<td>Kuwait</td>
<td>3</td>
<td>New Zealand</td>
<td>1</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>20</td>
<td>Mexico</td>
<td>3</td>
<td>Qatar</td>
<td>1</td>
</tr>
<tr>
<td>Australia</td>
<td>18</td>
<td>UAE</td>
<td>3</td>
<td>Romania</td>
<td>1</td>
</tr>
<tr>
<td>Finland</td>
<td>15</td>
<td>Belgium</td>
<td>2</td>
<td>Russian Federation</td>
<td>1</td>
</tr>
<tr>
<td>Switzerland</td>
<td>13</td>
<td>Canada</td>
<td>2</td>
<td>Slovenia</td>
<td>1</td>
</tr>
<tr>
<td>Ireland</td>
<td>11</td>
<td>Colombia</td>
<td>2</td>
<td>Thailand</td>
<td>1</td>
</tr>
<tr>
<td>Norway</td>
<td>11</td>
<td>Denmark</td>
<td>2</td>
<td>Serbia and Montenegro</td>
<td>1</td>
</tr>
<tr>
<td>Singapore</td>
<td>11</td>
<td>Isle of Man</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Austria</td>
<td>9</td>
<td>Malaysia</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poland</td>
<td>7</td>
<td>Slovak Republic</td>
<td>2</td>
<td>Relatve Total</td>
<td>2063</td>
</tr>
<tr>
<td>Sweden</td>
<td>7</td>
<td>South Africa</td>
<td>2</td>
<td>Absolute Total</td>
<td>2050</td>
</tr>
</tbody>
</table>
Thank you for listening