Advances in International Information Security Standards

Mr. Dale Johnstone
Principal Consultant
Risk Management & Compliance
PCCW Limited

Chairman ISMS
International User Group
Hong Kong & Macau Chapter

Member ISO
Information Security Committee
JTC 1 / SC 27 / WG 1

Principal Consultant
Risk Management & Compliance
PCCW Limited
Agenda

• In the Beginning
• Move to ISO
• Evolution within ISO
• What to Expect (2005)
• Financial Sector
• ISMS Road Map (Future)
In the Beginning
In the Beginning

BS 7799-1 Published as a UK Standard
In the Beginning

Need for an Information Security Management System Identified

BS7799-2 - Published
In the Beginning

BS7799-1 Updated to be Non-UK Centric & Republished
Move to ISO
Growing International Interest – BS7799-1 sent to ISO International Standard Committee
BS7799-2 – Updated & Reissued to align with ISO 9000 PDCA Model / ISO 17799 Controls
Evolution within ISO
<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2000</td>
<td>ISO 17799 Published – 75.4% Approval Vote</td>
</tr>
<tr>
<td>April 2001</td>
<td>Due to Close Vote – Irregular Step taken to Immediately Commence Review</td>
</tr>
<tr>
<td>October 2001</td>
<td>150 Pages of Comments Received</td>
</tr>
<tr>
<td>April 2002</td>
<td>100 Pages of Comments Received</td>
</tr>
<tr>
<td>October 2002</td>
<td>162 Pages of Comments Received</td>
</tr>
<tr>
<td>April 2003</td>
<td>210 Pages of Comments Received</td>
</tr>
<tr>
<td>October 2003</td>
<td>202 Pages of Comments Received</td>
</tr>
<tr>
<td>October 2004</td>
<td>64 Pages of Comments Received</td>
</tr>
<tr>
<td>Date</td>
<td>Event</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>October 2002</td>
<td>Call for Interest – Justification Study</td>
</tr>
<tr>
<td>April 2003</td>
<td>Study Period Commenced – BS7799-2 Submitted</td>
</tr>
<tr>
<td>October 2003</td>
<td>44 Pages of Comments Received</td>
</tr>
<tr>
<td>April 2004</td>
<td>40 Pages of Comments Received</td>
</tr>
<tr>
<td>October 2004</td>
<td>New Work Item Proposal Commenced</td>
</tr>
<tr>
<td></td>
<td>63 Pages of Comments Received</td>
</tr>
<tr>
<td>April 2005</td>
<td>61 Pages of Comments Received Approval Received to Proceed to FCD</td>
</tr>
</tbody>
</table>
What to Expect (2005)
ISO 17799

100% Approval Vote Received

Off to Publishers
What to Expect (2005)

ISO 17799

May/June

100% Approval Vote Received

Off to Publishers

BS 7799-2

November/December

??% Approval Vote Received

Off to Publishers
What to Expect (2005)

ISO 17799

May/June
100% Approval Vote Received
Off to Publishers

ISO 27001

November/December
??% Approval Vote Received
Off to Publishers
ISMS Road Map (Future)
• Code of practice for information security management
  – ISO 17799
  – 2007 = ISO 27002?

Has obtained unanimous approval from all countries throughout the world involved in ISO Information Security Committee

Maintaining the greatest influence over all information security management standards
ISMS Road Map (Future)

• ISMS – Requirements (BS7799-2)

Has obtained majority support to proceed to final drafting stage

To better enable companies demonstrate compliance with legislative requirements ISO 27001 certification is expected to grow significantly in 2006/2007
Setting up and managing an ISMS requires the same approach as for any other management system.

Observing a continuous cycle designed to ensure organizational best practices are documented, reinforced & improved over time.
ISMS Road Map (Future)

- **ISMS – Measurements & Metrics (in-progress)**

  Define implementation objectives, effectiveness & efficiency criteria, tracking & measuring evolution, assist in benchmarking tools

  Analyse information in objective manner, based on facts/real values

  Use analytical information as a means to improve ISMS

  As part of continuous improvement using metrics & measurements to allow an objective comparison of achieved information security:

  1. Over a period of time;
  2. between different parts of an organisation; and/or
  3. between organisations.
<table>
<thead>
<tr>
<th>ISMS Road Map (Future)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Code of practice for information security management</td>
</tr>
<tr>
<td>• ISMS – Requirements (in-progress)</td>
</tr>
<tr>
<td>• ISMS – Implementation Guidelines (in-progress)</td>
</tr>
<tr>
<td>• ISMS – Measurements &amp; Metrics (in-progress)</td>
</tr>
<tr>
<td>• ISMS – Concepts &amp; Models (Under consideration)</td>
</tr>
<tr>
<td>• ISMS – Fundamentals and vocabulary (Conceptual)</td>
</tr>
<tr>
<td>• ISMS – Monitoring &amp; Review (Conceptual)</td>
</tr>
<tr>
<td>• ISMS – Auditing (Conceptual)</td>
</tr>
</tbody>
</table>
ISO 17799 (2005)
11 Security Categories (Chapters)

36 Control Objectives (Level 2 Headings)

133 Controls (Level 3 Headings)
3 Security policy
3.1 Information security policy
Objective: To provide management direction and support for information security.
Management should set a clear policy direction and demonstrate support for, and commitment to,
information security through the issue and maintenance of an information security policy across the
organization.

3.1.1 Information security policy document
A policy document should be approved by management, published and communicated, as appropriate, to
all employees. It should state management commitment and set out the organization’s approach to
managing information security. As a minimum, the following guidance should be included:
a) a definition of information security, its overall objectives and scope and the importance of security
as an enabling mechanism for information sharing (see introduction);
b) a statement of management intent, supporting the goals and principles of information security;
c) a brief explanation of the security policies, principles, standards and compliance requirements of
particular importance to the organization, for example:
1) compliance with legislative and contractual requirements;
2) security education requirements;
3) prevention and detection of viruses and other malicious software;
4) business continuity management;
5) consequences of security policy violations;
d) a definition of general and specific responsibilities for information security management, including
reporting security incidents;
e) references to documentation which may support the policy, e.g. more detailed security policies and
procedures for specific information systems or security rules users should comply with.

This policy should be communicated throughout the organization to users in a form that is relevant,
accessible and understandable to the intended reader.
5 Security policy

5.1 Information security policy

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

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

5.1.1 Information security policy document

Control

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

Implementation guidance

The information security policy document should state management commitment and set out the organization’s approach to managing information security. The policy document should contain statements concerning:

a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);

b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:

1) compliance with legislative, regulatory, and contractual requirements;

2) security education, training, and awareness requirements;

3) business continuity management;

4) consequences of information security policy violations;

5) a definition of general and specific responsibilities for information security management, including reporting information security incidents;

6) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

This information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

Other information

The information security policy might be a part of a general policy document. If the information security policy is distributed outside the organisation, care should be taken not to disclose sensitive information. Further information can be found in the ISO/IEC IS 13335-1:2004.
## Clause 5.1

<table>
<thead>
<tr>
<th></th>
<th>2000</th>
<th>2005</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paragraphs</td>
<td>19</td>
<td>23</td>
<td>21.05</td>
</tr>
<tr>
<td>Lines</td>
<td>36</td>
<td>51</td>
<td>41.67</td>
</tr>
<tr>
<td>Words</td>
<td>251</td>
<td>343</td>
<td>36.65</td>
</tr>
<tr>
<td>Characters</td>
<td>1592</td>
<td>2202</td>
<td>38.32</td>
</tr>
<tr>
<td>Characters +spaces</td>
<td>1824</td>
<td>2528</td>
<td>38.60</td>
</tr>
</tbody>
</table>
5 Security policy

5.1 Information security policy

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

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

5.1.1 Information security policy document

Control

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

Implementation guidance

The information security policy document should state management commitment and set out the organization’s approach to managing information security. The policy document should contain statements concerning:

a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);

b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:

1) compliance with legislative, regulatory, and contractual requirements;
2) security education, training, and awareness requirements;
3) business continuity management;
4) consequences of information security policy violations;

e) a definition of general and specific responsibilities for information security management, including reporting information security incidents;

f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

This information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

Other information

The information security policy might be a part of a general policy document. If the information security policy is distributed outside the organisation, care should be taken not to disclose sensitive information. Further information can be found in the ISO/IEC IS 13335-1:2004.
5        Chapter Title (Security Category)
  5.1     Control Objective
  5.1.1   Control

Defines specific control statement to satisfy control objective

**Implementation guidance**

Provides more detailed information supporting implementation of the control and meeting the control objective. Some guidance may not be suitable therefore other ways of implementing control may be more appropriate

**Other information**

Provides further information to be considered, for example legal considerations and references to other standards
Control Objectives (Level 2)

ISO 17799 2005

INFORMATION SECURITY POLICY (1)

SECURITY POLICY
Control Objectives (Level 2)

ISO 17799 2005

ORGANISING INFORMATION SECURITY

INTERNAL ORGANIZATION (2)

EXTERNAL PARTIES (3)
ISO 17799
2005

Responsibility for Assets (4)
Information Classification (5)
Control Objectives (Level 2)

ISO 17799 2005

PRIOR TO EMPLOYMENT (6)

DURING EMPLOYMENT (7)

TERMINATION OR CHANGE OF EMPLOYMENT (8)
Control Objectives (Level 2)

ISO 17799 2005

- PHYSICAL & ENVIRONMENT SECURITY
- SECURE AREAS (9)
- EQUIPMENT SECURITY (10)
Control Objectives (Level 2)

ISO 17799 2005

- OPERATIONAL PROCEDURES AND RESPONSIBILITIES (11)
- THIRD PARTY SERVICE DELIVERY MANAGEMENT (12)
- SYSTEM PLANNING AND ACCEPTANCE (13)
- PROTECTION AGAINST MALICIOUS AND MOBILE CODE (14)
- BACK-UP (15)
- NETWORK SECURITY MANAGEMENT (16)
- MEDIA HANDLING (17)
- EXCHANGE OF INFORMATION (18)
- ELECTRONIC COMMERCE SERVICES (19)
- MONITORING (20)

COMMUNICATION & OPERATIONS MANAGEMENT
Control Objectives (Level 2)

ISO 17799 2005

1. BUSINESS REQUIREMENT FOR ACCESS CONTROL (21)
2. USER ACCESS MANAGEMENT (22)
3. USER RESPONSIBILITIES (23)
4. NETWORK ACCESS CONTROL (24)
5. OPERATING SYSTEM ACCESS CONTROL (25)
6. APPLICATION & INFORMATION ACCESS CONTROL (26)
7. MOBILE COMPUTING AND TELEWORKING (27)
Control Objectives (Level 2)

ISO 17799 2005

- Security Requirements of Information Systems (28)
- Correct Processing in Applications (29)
- Cryptographic Controls (30)
- Security of System Files (31)
- Security in Development and Support Processes (32)
- Technical Vulnerability Management (33)
ISO 17799 2005

REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES (34)

MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS (35)
Control Objectives (Level 2)

ISO 17799 2005

BUSINESS CONTINUITY MANAGEMENT

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT (36)
ISO 17799 2005

COMPLIANCE WITH LEGAL REQUIREMENTS (37)

COMPLIANCE WITH SECURITY POLICIES AND STANDARDS AND TECHNICAL COMPLIANCE (38)

INFORMATION SYSTEMS AUDIT CONSIDERATIONS (39)
# ISO 17799: 2005 (Summary)

<table>
<thead>
<tr>
<th>Clause</th>
<th>Security Category</th>
<th>Objectives</th>
<th>Controls</th>
<th>v2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Scope</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Terms and Definitions</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Structure of the Standard</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>Risk Assessment and Treatment</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>Security Policy</td>
<td>1</td>
<td>2</td>
<td>1 – 2</td>
</tr>
<tr>
<td>6</td>
<td>Organising Information Security</td>
<td>2</td>
<td>11</td>
<td>3 – 10</td>
</tr>
<tr>
<td>7</td>
<td>Asset Management</td>
<td>2</td>
<td>5</td>
<td>2 – 3</td>
</tr>
<tr>
<td>8</td>
<td>Human Resources Security</td>
<td>3</td>
<td>9</td>
<td>3 – 10</td>
</tr>
<tr>
<td>9</td>
<td>Physical and environmental Security</td>
<td>2</td>
<td>13</td>
<td>3 – 13</td>
</tr>
<tr>
<td>10</td>
<td>Communications and Operations Management</td>
<td>10</td>
<td>32</td>
<td>7 – 24</td>
</tr>
<tr>
<td>11</td>
<td>Access Control</td>
<td>7</td>
<td>25</td>
<td>8 – 31</td>
</tr>
<tr>
<td>12</td>
<td>Information Systems Acquisition, Development and Maintenance</td>
<td>6</td>
<td>16</td>
<td>5 – 18</td>
</tr>
<tr>
<td>13</td>
<td>Information Security Incident Management</td>
<td>2</td>
<td>5</td>
<td>0 – 0</td>
</tr>
<tr>
<td>14</td>
<td>Business Continuity Management</td>
<td>1</td>
<td>5</td>
<td>1 – 5</td>
</tr>
<tr>
<td>15</td>
<td>Compliance</td>
<td>3</td>
<td>10</td>
<td>3 – 11</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>39{36}</strong></td>
<td><strong>133{127}</strong></td>
<td><strong>+3 / +6</strong></td>
</tr>
</tbody>
</table>
Advances in International Information Security Standards

Mr. Dale Johnstone

dale.johnstone@pccw.com