BS 7799–2
Inception to Certification

Dale Johnstone
Chair – BS7799 User Group (Hong Kong)
Member - Australian Standards IT/12/4
Member – ISO/IEC JTC1 SC27
Principal Security Consultant
Risk Management & Compliance

5 December 2002
dale.johnstone@pcsw.com

---

**Agenda**

- What is BS7799?
- History of BS7799-1
- History of ISO/IEC 17799
- History of BS7799-2
- Current Status
- Future
- International User Group
- Roadmap to Certification
- Benefits
WHAT IS BS7799?

• Aim
  – Build on a Common Basis for Organisational Security Standards Development
  – Enhance Security Management Practice
  – Increase Confidence and Trust in Inter-Organisational Dealings

• Defines
  – Desired Best Practice Methods for Controlling (Protecting) Information
    (a) Confidentiality  (b) Integrity &  (c) Availability

• Consists of Two Parts
  – Part 1 – Code of Practice for Information Security Management
    • Represents Best Practice Guidance Based in Practical Industry Experience
  – Part 2 – Specification for Information Security Management Systems
    • Forms the Basis by Which Compliance Certification Can be Performed Against a Management Systems Standard
HISTORY OF BS7799
PART 1

Early 1990s
- Industry Need Determined for Best Practice Controls
- To Support Business & Government in the Implementation & Enhancement of Information Security
- Department of Trade and Industry (UK) established a Working Group Comprising Experienced Information Security Managers
- Information Security Management Code of Practice Produced

1992
- Published as an Industry Code of Practice (September)
  - Provided a Structured Framework for an Organisation to Examine & Improve the Security of their IT Systems Environment
- Originally published as a BSI-DISC publication
- Forms the Basis of British Standard 7799
History of BS7799 (Part 1)

- **1995**
  - BDD/2 Committee Revises Code suitable for publication
  - BS7799 Published as a UK Standard

- **1996 - 1997**
  - Need to increase level of confidence in BS7799 identified
  - Industry called for a means of certifying against the Code
  - Steering Committee Formed
    - UK Accreditation Service (UKAS)
    - International Register of Certified Auditors (IRCA)
    - Department of Trade & Industry (DTI)

- **1998 (April)**
  - UK ISMS Certification Scheme Launched

- **1999**
  - Revised and updated
  - New Controls Added:
    - E-commerce
    - Mobile Computing
    - Third Party Arrangements
  - UK Specific References Removed
  - Overall General Improvements Made
  - Second Edition Published (BS 7799-1:1999)
History of BS7799 (Part 1)

• Many Countries Adopted BS7799 for Domestic Use:
  - Australia
  - Brazil
  - Czech Republic
  - Canada
  - Denmark
  - Germany
  - Iceland
  - India
  - Ireland
  - Japan
  - Korea
  - Malaysia
  - Netherlands
  - Norway
  - Poland
  - Singapore
  - South Africa
  - Sweden
  - Switzerland
  - Taiwan
  - UAE
  - UK

• BS 7799 Translated Into Many Different Languages:
  - Danish
  - Chinese
  - Dutch
  - English
  - Finish
  - French
  - German
  - Icelandic
  - Japanese
  - Korean
  - Norwegian
  - Polish
  - Portuguese
  - Swedish
  - Finnish

HISTORY OF ISO/IEC 17799
History of ISO 17799

- **April 2000**
  - Given Strong International Interest - BDD/2 Recommended BS7799-1 be submitted to ISO for Development as an International Standard
  - BSI Submitted BS7799-1 to ISO using a 'Fast Track' Procedure
    - Allows International Standard to Be Published in 12 months

- **October 2000**
  - International Standard ISO/IEC 17799 Was Approved

- **December 2000**
  - International Standard ISO/IEC 17799:2000 Published
  - Some Minor Editorial Amendments

---

History of ISO 17799

- **April 2001**
  - ISO/IEC JTC1 SC27 'IT Security Techniques' Committee Assigned Responsibility for Maintenance & Further Development
  - Call for Revision Comments Issued

- **October 2001**
  - Revision Commenced by ISO Committee
  - 151 Pages of Comments Received

- **October 2002**
  - Revision Continues by ISO Committee
  - 666 Comments Spread Across 170 Pages Received
ISO 17799 Structure

- 10 Detailed Control Clauses
  1. Security Policy
  2. Security Organization
  3. Asset Classification & Control
  4. Personnel Security
  5. Physical & Environmental Security
  6. Communications & Operations Management
  7. Access Control Security
  8. System Development & Maintenance
  10. Compliance

ISO 17799 Topics

HISTORY OF BS7799
PART 2

1998
- Process for Establishing an Information Security Management System Identified
  - Developed by BDD/2
  - Published as BS 7799-2:1998
- BS 7799-2:1998 Specifies Controls to Be Implemented
  - According to Security, Legal and Business Requirements
- Specification Can be Used to:
  - Conduct Internal Audits to the Standard
  - Enable Third Party Certification to the Standard

1999
- Published as BS 7799-2:1999
  - Alignment of Controls With BS7799-1
History of BS7799 (Part 2)

- **Late 2001**
  - Revision of Standard Commenced

- **Main Drivers of Revision**
  - Harmonise with other Management System Standards
    - ISO 9001 & 14001
    - Assist with Integration and Operation of Organisation’s Management Systems
    - Facilitate Combined Third Party Audits
  - Need for Continual Improvement Processes
  - Corporate Governance
  - Information Security Assurance
  - Implementation of the new 2002 OECD Principles
    - Security of Information Systems and Networks

History of BS7799 (Part 2)

- **January – September 2002**
  - Draft for Public Comment Issued
  - BSI Committee BDD2 & International User Group
  - Finalised & Revised Version Completed

- **Contributors**
  - Australia
  - Brazil
  - Germany
  - Hong Kong
  - Ireland
  - Japan
  - Korea
  - Netherlands
  - Norway
  - Singapore
  - Sweden
  - UK
CURRENT STATUS
OF BS7799-2

**Present - BS7799 (Part 2)**

- **5th September 2002**
  - BS 7799-2:2002 Launched / Published in the UK
- **Major Updates**
  - Plan, Do, Check, Act (PDCA) Process Model
  - Process based approach based on PDCA Model
  - Improved definition and clarification of the links between:
    - Risk Assessment Process
    - Selection of Controls
    - Contents of the Statement of Applicability
  - Importance of Continual Process Improvement to the ISMS
  - Clarified Requirements for Documentation & Records
  - Enhanced Risk Assessment & Management Process
  - Controls from ISO 17799 Included as a Normative Annex
  - Annex Providing Guidance on New Version’s Use
  - Annex Showing correspondence with BS7799-2; ISO 9001; & ISO 14001
• Provides
  – Guidance on Creating an ISMS
  – Critical Success Factors to Successfully Implement Information Security
  – Ability to Harmonise With Other Management Systems
  – Plan-do-check-act Model for Creating and Maintaining an Effective ISMS
  – Ability to Continually
    • Improve Process of Security Management
    • Assess Security Procedures in the Light of Changing Business Requirements, Technology Threats and New Circumstances
  – Clarity of Relationship with:
    • International Standards
    • Newly Revised Guidelines From the Organisation for Economic Co-operation and Development (OECD)

Implement Improvements in the Information Security Management System Process, Implement Modifications to the Controls As Necessary to Meet Changing Circumstances
Monitor Control Performance, Review Risk Levels (Changing Circumstances), Perform Internal Information Security Management System Audits

Plan-Do-Check-Act
ISO 17799 & BS 7799-2

FUTURE

Future of ISO 17799

- October 2003
  - ??? Comments
  - International ISO Voting
- October 2004
  - ??? Comments
  - International ISO Voting
- 2005 Aimed Publication Date
  - Revised and Updated With a New Look
  - Contain New Additional Material
  - New Controls Will be Included
  - May even Include a new Major Topic Section
    - 10 → 11 Sections
Future of BS 7799-2

- **October 2002**
  - Study Period Commenced Within ISO
  - Review Need for an Information Security Management Systems Standard
  - International Countries Expected to Contribute to Study Period
  - Several Countries Have Already Indicated Very Strong Support
  - BSI (UK) Yet To Decide their form of Contribution (e.g. BS7799-2)

- **Expectation**
  - New Version to Be Issued Either by:
    - BSI
    - or
    - ISO
  - Within Six Months of ISO 17799 Being Republished

BS 7799
INTERNATIONAL USER GROUP
(IUG)
### Countries Represented

<table>
<thead>
<tr>
<th>Australia</th>
<th>Japan</th>
<th>Singapore</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>Korea</td>
<td>South Africa</td>
</tr>
<tr>
<td>Canada</td>
<td>Malaysia</td>
<td>Sweden</td>
</tr>
<tr>
<td>Germany</td>
<td>The Netherlands</td>
<td>Switzerland</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>New Zealand</td>
<td>Taiwan</td>
</tr>
<tr>
<td>Iceland</td>
<td>Norway</td>
<td>UAE</td>
</tr>
<tr>
<td>India</td>
<td>Poland</td>
<td>UK</td>
</tr>
<tr>
<td>Ireland</td>
<td></td>
<td>USA</td>
</tr>
</tbody>
</table>

### IUG Chapters

- Australia
- Canada
- Germany
- Hong Kong
- India
- Singapore
- Sweden
- Taiwan
- UK

---

**ROADMAP FOR CERTIFICATION**

*(ONE EXAMPLE)*

![Roadmap Image](image-url)
BS7799-2 Standard Specifies Requirements for Establishing, Implementing and Documenting an ISMS
- Define Security Policy
- Define the ISMS Scope (Boundary)
- Identify Assets
- Undertake Asset Risk Assessment
- Identify Asset Weak Areas
- Make Decisions to Manage Risk
- Select Appropriate Controls
- Implement & Manage Selected Controls
- Prepare Statement of Applicability

Option of Formal Certification Now Available

Audit Objectives
- Review Compliance to BS 7799–2
- Review Degree of Implementation to BS 7799–2
- Review the Effectiveness and Suitability in meeting:
  - Security Policy
  - Security Objectives
- Identify Security Holes & Weaknesses
- Provide an Opportunity to Improve ISMS
- Meet Contractual Requirements
- Meet Regulatory Requirements

TO ACHIEVE CERTIFICATION
Approach

• **Preparation**
  - Understanding of the effort required
  - Clear that it is a continuous effort
  - A key operational champion is identified
  - People Resources are available (minimum 6 months)
  - Budgetary Resources are available
  - Identified the end goals to be achieved (why proceed)

• **Management Commitment**
  - Key management champion is identified
  - Understanding of what will be achieved
  - Support to make it happen
  - Ability to prioritise the commitment (e.g. high)

---

Approach

• **Day 0**
  - Determine details of ISMS Certification Process

• **Day 1**
  - Map out a project plan
  - Determine key milestones
  - Select key people resources
  - Form project team (Security Forum)
  - Commence documentation (e.g. minutes)
  - Determine and allocate a budget
  - Determine what professional assistance/advice is required
### Approach

**Day 2–5**
- Plan major activities
  - Information Security Policy
  - Asset Identification
  - Risk Assessment
  - Training and Awareness
  - Scope of assessment
    (e.g. physical, people, shifts etc...)

**Week 1**
- Project Team Meeting
- Initial Scope of Assessment Determined
- Asset Identification Process Commenced
- Gap Analysis of ISMS Requirements within Scope Completed

---

**Week 2–4**
- Project Team Meeting (held fortnightly)
- Plan/Update Project Plan/Milestones
- Develop security organisational structure (Security Forum)
- Develop/update information security policies
- Commence Risk Assessment (determine methodology)
- Identify weak and strong security areas/risks

**Month 2**
- Finalise information security policies (ready for approval)
- Review scope of assessment
- Commence risk management process (safeguard selection)
- Commence development of Information Security Manual
- Continue to document your efforts
## Approach

### Month 3
- Project Team Meeting (held Monthly) (Security Forum)
- Submit Information Security Policies – Senior Mgt Approval
- Commence/continue safeguard (control) implementation
- Continue to monitor Gap Analysis Study (from week 1)

<table>
<thead>
<tr>
<th>Part 1</th>
<th>Statement</th>
<th>Comply</th>
<th>Non-Comply</th>
<th>Exclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1.1</td>
<td>Information security policy document</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.2.2</td>
<td>Review and evaluation</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.2.1.1</td>
<td>Management information security forum</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Month 4
- Continue safeguard (control) implementation (risk mgt)
- Ensure personnel awareness/training of information security
- Ensure management approval of Information Security Policy
- Continue development of Information Security Manual
  - Document what you actually do – not what you should do!
  - ISM forms a key element in the certification audit (As do) – Meeting Minutes
  - Risk Assessment documentation
  - Organisational structure
  - Statement of Applicability
- Continue to review/revise supporting documentation
  - Not necessarily security related
  - But support of security safeguards/controls


**Approach**

- **Month 5**
  - Commence development of ‘Statement of Applicability’
    - Progressive update from Gap Analysis document
  - Continue Information Security Manual
  - Continue implementation of safeguards (control)
  - Commence process of:
    - Continuous review
    - Continuous documentation
    - Perform (2nd) Risk Assessment (if applicable)
    - Visitor’s log etc...
  - Engage internal auditors (if available)
    - To assist in reviewing work to date
    - To provide an element of increased confidence
    - To determine any non-conformities earlier in process
  - Engage External (Accredited) Certification Body

**Certification Audit – Phase 1**

- **Month 6**
  - Commence Phase 1 – Desktop/Documentation Audit
    - Review ISMS Management Framework
      - Security Organisation
      - Security (Committee) Meeting Minutes
    - Assess Scope of Assessment (ISMS)
    - Statement of Applicability
    - Risk Assessment and Management Approach
    - Security Policy and Supporting key Procedures
      - e.g. Information Security Manual
    - Determine any minor/major non-conformities
  - Action taken to correct non-conformities
  - Documentation updated to reflect changes
  - Finalise Information Security Manual
  - Finalise implementation of safeguards (control)

# May or may not be conducted on site
Month 7
- Commence Phase 2 – Implementation Audit
  - To confirm the:
    - Organisation adheres to its own policies, objectives and procedures
    - ISMS conforms with requirements of:
      (a) ISMS Standard; and
      (b) Is achieving the organisation’s policy objectives
    - Test the effectiveness of the ISMS
- On-site inspection to review/test effectiveness of (ISMS) Policies, Procedures, Objectives
  - Interview Owners and Users of ISMS
  - Review High, medium and/or low risk areas
  - Security objectives and targets
  - Links between the core documents within the system
  - Security and management reviews
- Report findings and give final recommendation

It’s worth knowing…
- Not Expect to Gain Certification Without Risk Assessment
- Without Internal Reviews, Unlikely to Pass External Audit
<table>
<thead>
<tr>
<th>Country</th>
<th>Certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>(1)</td>
</tr>
<tr>
<td>Austria</td>
<td>(1)</td>
</tr>
<tr>
<td>Brazil</td>
<td>(2)</td>
</tr>
<tr>
<td>China</td>
<td>(3)</td>
</tr>
<tr>
<td>Egypt</td>
<td>(1)</td>
</tr>
<tr>
<td>Finland</td>
<td>(8)</td>
</tr>
<tr>
<td>Germany</td>
<td>(6)</td>
</tr>
<tr>
<td>Greece</td>
<td>(2)</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>(6)</td>
</tr>
<tr>
<td>Hungary</td>
<td>(2)</td>
</tr>
<tr>
<td>Iceland</td>
<td>(1)</td>
</tr>
<tr>
<td>India</td>
<td>(8)</td>
</tr>
<tr>
<td>Ireland</td>
<td>(3)</td>
</tr>
<tr>
<td>Italy</td>
<td>(3)</td>
</tr>
<tr>
<td>Japan</td>
<td>(17)</td>
</tr>
<tr>
<td>Korea</td>
<td>(9)</td>
</tr>
<tr>
<td>Norway</td>
<td>(6)</td>
</tr>
<tr>
<td>Singapore</td>
<td>(6)</td>
</tr>
<tr>
<td>Spain</td>
<td>(1)</td>
</tr>
<tr>
<td>Sweden</td>
<td>(4)</td>
</tr>
<tr>
<td>Taiwan</td>
<td>(3)</td>
</tr>
<tr>
<td>UAE</td>
<td>(1)</td>
</tr>
<tr>
<td>UK</td>
<td>(74)</td>
</tr>
<tr>
<td>USA</td>
<td>(3)</td>
</tr>
</tbody>
</table>
BS7799 Benefits

• Improves
  – Management Understanding of the Value of Organisational Information
  – Customer Confidence, Satisfaction and TRUST
  – Business Partner Confidence, Satisfaction and TRUST
    • e.g. Handling Sensitive Information of Customers & Business Partners
  – Level of Assurance in Organisational Security & QUALITY
  – Conformance to Legal and Regulatory Requirements
  – Organisational Effectiveness of Communicating Security Requirements
  – Organisational Effectiveness of Communicating Security Requirements
  – Employee Motivation and Participation in Security (Best Practices)
  – Organisational Profitability
  – Management and Handling of Security Incidents
  – Ability to Differentiate Organisation for Competitive Advantage
  – Organisational Credibility & Reputation

Certification Benefits

• Certification Demonstrates:
  – Commitment
  – Continuous Improvement
  – Preparedness for Independent Review
  – Measure Against Best Practice

• Certification Provides
  – Means to Benchmark
    • Industry & Competitors
    • Business Partners
    • Customers
  – Increased Level of Certainty
Thank You

Q & A