Information security

daniel.dresner@ncc.co.uk
You can’t undisclose a disclosure

• The National Computing Centre
• The landscape of Information Security standards
• Introduce a corporate information security programme step-by-step
• Good practice security controls for information management

1 Gerry O’Neill, CEO, IISP
3 No. The National Computing Centre doesn’t do escrow!
History (Learning Lessons)

• 1994: Security Breaches Survey
• 1995: DTI Code of Practice/BS 7799
• 1999: BS 7799
  Code of practice for information security (the catalogue of controls)
• 2000: ISO 17799 (aka BS 7799 Part 1)
  No certificates!
• 2002: BS 7799 Part 2 (Plan-Do-Check-Act)
  Specification for and information security management system
• 2005: ISO 17799 (Revised):=27002
• 2005 ISO 27001 (aka BS 7799 Part 2)
The landscape of Information Security standards

ISO/IEC 38500 IT Governance
BS 25777 IT service continuity
ISO/IEC 27031 ICT readiness for business continuity
ISO/IEC 27032 Cyber security
ISO/IEC 27033 IT network security
ISO/IEC 27034 Applications security
ISO/IEC 18044 Information security incident management
ISO/IEC 24762 Disaster recovery services

BS 25999 Business continuity

Inseparable
Services

ISO/IEC 27000 Overview and vocabulary
ISO/IEC 27001 ISMS requirements
ISO/IEC 27002 Code of practice for information security management
ISO/IEC 27003 ISMS implementation guidance
ISO/IEC 27004 Information security management measurement
ISO/IEC 27005 ISMS risk management
ISO/IEC 27006 Requirements for bodies providing certification and auditing services of ISMS
ISO/IEC 27007 ISMS auditing guidelines

Core ISO/IEC 27nnn

Automotive industry
Small businesses
Critical infrastructure
e-Government

ISO/IEC 27011 Telecoms ISMS requirements

Sector Specific
May appear
What they really mean

• ISO 27001 (BS 7799 Part 2)
  – Information security management system requirements
  – Plan-do-check-act
  – Like ISO 9001/ISO 20000
  – Certification Benchmark

• ISO 27002 (ISO 17799; BS 7799 Part 1)
  – Code of practice
  – Catalogue of 135 controls!
  – Pick and mix using ISO 27001
  – No certificates!
A taxonomy of treatment (not a wish list)
Do what was planned

What to do?

ISO/IEC 15288
System Life Cycle Processes
ISO/IEC 20000 IT service management
Protection
STARTS Software Techniques for Reliable, Trusted Systems
ISO 18019 Guidelines for the design and preparation of user documentation for application software
ISO/IEC 12207 Software life cycle processes
ISO 27001 Information security management systems.
Requirements management

How to do it?

BS ISO/IEC 38500 Corporate governance of information technology
ISO/IEC 25000 Software Quality
IT Service Continuity Management: Systems and Processes
ISO/IEC 24762 Guidelines for ICT disaster recovery services
BS 25777 IT Service Continuity Management Systems

All business or service processes need the ability to do-check-act. This chart shows how the top 8 national and international standards (emboldened text) form part of the best practice framework in information technology. This standards framework is the foundation for organisations to accept the technical standards of particular technologies including those special to vendors.
ISO/IEC 27001 in 13 Steps
Project plan

(1) Senior management acceptance and endorsement of security
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment
(7) Risk treatment plan
(8) Security standards document (control measures)
(9) Statement of applicability
(10) System security plans and procedures
(11) Monitor and review the ISMS performance
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
Project plan

(1) Senior management acceptance and endorsement of security
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment
(7) Risk treatment plan
(8) Security standards documents
(9) Statement of applicability
(10) System security plans and procedures
(11) Monitor and review the ISMS performance
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
Project plan

(1) Senior management acceptance and endorsement of security
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment
(7) Risk treatment plan
(8) Security standards document (control measures)
(9) Statement of applicability
(10) System security plans and procedures
(11) Monitor and review the ISMS performance
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
Project plan

(1) Senior management acceptance and endorsement of security
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment

(7) Risk treatment plan
(8) Security standards document (control measures)
(9) Statement of applicability
(10) System security plans and procedures
(11) Monitor and review the ISMS performance
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
Project plan

(1) Senior management acceptance and endorsement of security
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment
(7) Risk treatment plan
(8) Security standards document (control measures)
(9) Statement of applicability
(10) System security plans and procedures
(11) Monitor and review the ISMS performance
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
Project plan

(1) Senior management acceptance and endorsement of security
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment
(7) Risk assessment
(8) Security standards document (control measures)
(9) Statement of applicability
(10) System security plans and procedures
(11) Monitor and review the ISMS performance
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
Project plan

(1) Senior management acceptance and endorsement of security
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment

(7) Risk treatment plan
(8) Security standards document (control measures)
(9) Statement of applicability
(10) System security plans and procedures
(11) Monitor and review the ISMS
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
Project plan

(1) Senior management acceptance and endorsement
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment
(7) Risk treatment plan
(8) Security standards document (control measures)
(9) Statement of applicability
(10) System security plans and procedures
(11) Monitor and review the ISMS performance
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
Project plan

(1) Senior management acceptance and endorsement of security
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment
(7) Risk treatment plan
(8) Security standards document (control measures)
(9) Statement of applicability
(10) System security plans and procedures
(11) Monitor and review the ISMS performance
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
Project plan

(1) Senior management acceptance and endorsement of security
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment
(7) Risk treatment plan
(8) Security standards document (control measures)
(9) **Statement of applicability**
(10) System security plans and procedures
(11) Monitor and review the ISMS performance
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
## Project plan

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Senior management acceptance and endorsement of security</td>
</tr>
<tr>
<td>2</td>
<td>Information security organisation and infrastructure</td>
</tr>
<tr>
<td>3</td>
<td>High level security policy</td>
</tr>
<tr>
<td>4</td>
<td>Staff training and education – creating security awareness</td>
</tr>
<tr>
<td>5</td>
<td>Identify and classify the assets</td>
</tr>
<tr>
<td>6</td>
<td>Risk assessment</td>
</tr>
<tr>
<td>7</td>
<td>Risk treatment plan</td>
</tr>
<tr>
<td>8</td>
<td>Security standards document (control measures)</td>
</tr>
<tr>
<td>9</td>
<td>Statement of applicability</td>
</tr>
<tr>
<td>10</td>
<td>System security plans and procedures</td>
</tr>
<tr>
<td>11</td>
<td>Monitor and review the ISMS performance</td>
</tr>
<tr>
<td>12</td>
<td>Maintain the ISMS; continuous improvement</td>
</tr>
<tr>
<td>13</td>
<td>Extending the scope</td>
</tr>
</tbody>
</table>
3. Risk Assessment

What assets are we protecting?
What is our commitment to security?
How serious are the threats to our assets?
How much risk can we accept for each asset?

4. Security Controls

How is risk kept to acceptable levels?
Which assets are protected by which controls?

5. Applicability

Which assets are protected by which controls?

6. Business Continuity

What are the priorities for the business?
Are we achieving set service level measures?

7. Processes

How do we do all this?

1. Scope

What assets are we protecting?
Asset ownership?

2. Policy

What level of risk can we accept?

(10) System security plans and procedures
Project plan

1. Senior management acceptance and endorsement of security
2. Information security organisation and infrastructure
3. High level security policy
4. Staff training and education – creating security awareness
5. Identify and classify the assets
6. Risk assessment
7. Risk treatment plan
8. Security standards document (control measures)
9. Statement of applicability
10. System security plans and procedures
11. Monitor and review the ISMS performance
12. Maintain the ISMS; continuous improvement
13. Extending the scope
Project plan

1. Senior management acceptance and endorsement of security
2. Information security organisation and infrastructure
3. High level security policy
4. Staff training and education – creating security awareness
5. Identify and classify the assets
6. Risk assessment
7. Risk treatment plan
8. Security standards document (control measures)
9. Statement of applicability
10. System security plans and procedures
11. Monitor and review the ISMS performance
12. Maintain the ISMS; continuous improvement
13. Extending the scope

(time) cost content
Project plan

(1) Senior management acceptance and endorsement
(2) Information security organisation and infrastructure
(3) High level security policy
(4) Staff training and education – creating security awareness
(5) Identify and classify the assets
(6) Risk assessment
(7) Risk treatment plan
(8) Security standards document (control measures)
(9) Statement of applicability
(10) System security plans and procedures
(11) Monitor and review the ISMS performance
(12) Maintain the ISMS; continuous improvement
(13) Extending the scope
15.1.3 Protection of organizational records (ISO/IEC 27002:2007)

- Categorise records – *manage according to impact level*
- Protect against deterioration
  - Long term storage - use paper and microfiche (encrypt?!) 
- Guide retention, storage media type, handling, and disposal to meet business, statutory, regulatory or contractual requirements 
- Keep inventory of sources of key information 
- Implement procedures (with/without technology) to protect records and information from: 
  - Loss 
  - Destruction 
  - Falsification. 
- Store cryptographic keys and programs to enable decryption 
- See ISO 15489-1 . . .
Final thought

• 2008
  – The year of lost data (UK)
• 2009
  – The year of encryption
• 2010
  – The year of lost encryption keys
• Think: Retrieval and retention not loss

Good security is an enabler
You can’t undisclose a disclosure

- The National Computing Centre
- The landscape of Information Security standards
- Introduce a corporate information security programme step-by-step
- Good practice security controls for information management