The Road to BS7799 Certification and using ISO17799 as an Information Security Framework

John Theobald
Copyright

The Copyright is this document is vested in i-defence Ltd. and the document is issued in confidence for the purpose only for which it is supplied. It must not be reproduced in whole or in part or used for any purpose except with the prior consent of i-defence Ltd and then only on the condition that this notice is included in such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any matter whatsoever to any third party with the prior written consent of i-defence Ltd.

@Copyright i-defence ltd
The Code of Practice to model the security management system

Introduction

Information is arguably a company's most precious asset, yet failure to design an effective Information Security Management System (ISMS) can unnecessarily put these assets at risk. Although in the past there was only a moral responsibility for the executive to protect information assets, there is now legislation in force to ensure information security remains on the board agenda. Indeed a company’s executive can be prosecuted if mitigating controls are neglected and the interests of the company are ignored. As many authorities rightly point out, **Risk is now a board game.**

Information comes in many forms and different methods are required to protect the confidentiality, integrity and availability (CIA), although most management systems are technology based. Information can be current or historic, held statically or moved from A to B.

The Role of Information Security Management

Regardless of which model is used to establish the security framework, an Information Security Management System is fundamental in engaging effective and appropriate controls to protect information assets. Without a management system and ongoing commitment from senior management it is difficult to commit resources and ensure information security is appropriately embedded in the business.

It is recommended that the ISMS be based on the Deming Wheel model introduced in BS7799-2002 Part 2 (PDCA - Plan, Do, Check & Act), which is a de-facto methodology and ensures that the correct components are engaged, evaluated, monitored and improved on a continuous basis.
There are a number of stages involved with implementing an ISMS framework. The initial stage concentrates on building an asset register and conducting a risk assessment. This should not be limited to software and hardware, but include services and data assets. The subsequent stages include defining the security policy, forming a risk treatment plan and developing business continuity plans. The security policy should include legislation and other outside forces that govern the use and handling of information. It is imperative that the ISMS be consistently reviewed for effectiveness and the lessons learnt are fed back into the management cycle.

History of the Code of Practice –BS7799/ISO17799

The original Code of Practice was developed in January 1993 (BSI 1993, DISC PD0004; A Code of Practice for Information Security Management) by an industry working group and released in September 1993. The standard became BS7799 Part 1 in 1995 and Part 2 was not published until 1998. Revised versions of Part 1 and 2 were published in 1999 and In December 2000 BS7799 Part 1 was superseded by ISO/IEC 17799, when it became an international standard. BS7799 Part 2 published in 2002 recommended the management process required to build, operate, maintain and improve an ISMS. The ultimate goal of BS7799 is to provide a development plan in which the information security management system could be built. The standard was written to cross all boundaries, regardless of sector, size of organisation and structure. A number of companies formed the industry group to ensure the controls were commercially acceptable.

Throughout its existence BS7799 has had very little in terms of competition and this was further endorsed when Part 1, was superseded by the International ISO 17799 standard and was appreciated by a much wider audience.

BS7799 is a framework and should be treated as such; the standard offers guidance and recommendation which assist in protecting information assets. Not all controls are applicable to every environment and its imperative that the ISMS be aligned to the security policy and not just in compliance with the standard – In fact this is where many management systems fail. It is important to note that a company can only be accredited against BS7799 and ISO17799 is provided for explanatory purposes.
Some of the Benefits of BS7799/ISO17799

There are an abundance of benefits in aligning the information security management system with ISO 17799 and once again these will vary from company to company. If nothing else, the framework will ensure that the information assets are appropriately handled and the controls are established to mitigate unnecessary risk. Other benefits include:

- Improved security throughout the organisation
- Improved security planning
- Demonstrates company’s commitment in protecting information
- Security management effectiveness
- Ongoing protection over Information
- Less risk when dealing with partners
- Improved e-commerce security
- Improved customer, employee and partner confidence
- More realistic and manageable auditing
- Reduced liability over information
- Ultimately creates a centre of excellence which increasingly hits customer’s ‘hot button’.

At the time of writing this paper, 285 companies have been accredited with BS7799 in 27 different countries. Outside of the UK, Japan far exceeds any other country in the number of accredited companies. Companies are beginning to recognise the marketing potential of certification, as was the case with ISO 9002 in the 90's.
ISO 17799 Composition

ISO 17799 is formed of ten control areas, which is further separated into 36 control objectives and 127 individual controls. Each control area is exhaustive in its nature and provides best practice recommendations in establishing effective information security.

<table>
<thead>
<tr>
<th>Control Area</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Policy</td>
<td>To provide management direction and support for information security.</td>
</tr>
<tr>
<td>Security Organisation</td>
<td>To manage information security within the organization.</td>
</tr>
<tr>
<td>Asset Control and Classification</td>
<td>To maintain appropriate protection of organizational assets.</td>
</tr>
<tr>
<td>Personnel Security</td>
<td>To reduce the risks of human error, theft, fraud or misuse of facilities.</td>
</tr>
<tr>
<td>Physical &amp; Environmental Security</td>
<td>To prevent unauthorized access, damage and interference to business premises and information.</td>
</tr>
<tr>
<td>Communications &amp; Operations Management</td>
<td>To ensure the correct and secure operation of information processing facilities.</td>
</tr>
<tr>
<td>Access Control</td>
<td>To control access to information.</td>
</tr>
<tr>
<td>Systems Development &amp; Maintenance</td>
<td>To ensure that security is built into information systems.</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.</td>
</tr>
<tr>
<td>Compliance</td>
<td>To avoid breaches of any criminal and civil law, statutory, regulatory or contractual</td>
</tr>
</tbody>
</table>
Introducing a Management Framework

The purpose of the Framework is to formulate the management system and ensure that the elements are formally documented, maintainable and support a continuous improvement program. It is typical to find components of the Framework already engaged, albeit not formally documented and/or uncontrolled.

BS7799 Part 2 introduced earlier, involves a number of logical steps, the majority of which relate to subsequent phases of the framework. The diagram below depicts the components of each phase and identifies the deliverables.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define security objectives</td>
<td>Security Policy</td>
</tr>
<tr>
<td>Define ISMS characteristics, including project scope</td>
<td>Project related material</td>
</tr>
<tr>
<td>Use project steering group to set objective, tasks and critical success factor</td>
<td>Business justification, cost analysis and scoping documentation</td>
</tr>
<tr>
<td>Conduct a gap analysis to identify shortcomings</td>
<td>Assessment of compatibility</td>
</tr>
<tr>
<td>Develop and enable the ISMS</td>
<td>Framework documentation, including policy, standards and guidelines.</td>
</tr>
<tr>
<td>Living with the standard. This stage must be conducted over a three month period.</td>
<td>Certification process</td>
</tr>
</tbody>
</table>

The most notable difference with the BS7799 Part 2 released in 2002 and its predecessor is the advice and instruction given as to how to build, operate, manage and improve the ISMS. The 1999 edition only instructed you to apply ISO/IEC 17799 and build an ISMS. Part 2 also discusses the inter-relationship with ISO 9002.
BS7799 Part 2 Certification process

Once the Gap Analysis has been conducted, the weaknesses identified are addressed and the ISMS has been embedded in the business for more than three months, a company is in a position to apply for BS7799 certification. The certification audit is conducted in two phases.

| Stage 1 | The auditor will review the documentation to assess the company’s compatibility with BS7799 and obtain an understanding of the local ISMS |
|         | The auditor will report their findings and allows for minor gaps to be closed. |
|         | The auditor is responsible for explaining the process of Part 2. |

Stage 1

The auditor will confirm that the ISMS has been engaged.

The auditor will assess the ISMS suitability and competency to protect information security.

The auditor will interview a selection of users, the person responsible for Information Security and Data owners.

The auditor will consider areas of risk, especially high risk areas.

The auditor will finally produce a report with the positive finding and non-compliant areas.

Stage 2

It is possible that the certificate is given on a conditional basis, meaning there is an issue not too serious to be considered a failure, but needs addressing nevertheless.
Policy/Standards and Procedures

Many people are confused by the difference between policies, standards and guidelines and geographical regions have their own interpretation. For the purpose of this document, there are four distinct layers to the information security document set.

Diagram 2 represents the relationship between the various aspects of the management document set.

Diagram 2 – Policy, Standard, Procedures and Records

1. Policy
The policy should be owned by a function and a formal process adopted to ensure the document is reviewed and maintained according to a defined review process (i.e. six months). The process should ensure the policy is able to respond to changes in the business and the basis of the original risk assessment. This includes vulnerabilities, personnel and contact changes, contract amendments and changes subjected to the change control process.

2. Standards
BSI describes a standard as “a published specification that establishes a common language, and contains a technical specification or other precise criteria and is designed to be used consistently, as a rule, a guideline, or a definition”. Standard covers the ‘What’ are we protecting. An example is a mobile computing standard that discusses in detail, acceptable use of mobile computers. It is good practice to follow the S.M.A.R.T. (specific, manageable, accurate, realistic and timebound) philosophy when developing documentation to ensure the standards remain manageable, appropriate, and consistent with the asset(s) they are protecting.

3. Guidelines and Procedures
The purpose of implementing security guidelines and procedures is to provide instruction in securing information assets. Guidelines include operating system configuration, Firewall administration and Access control and change control procedures.

4. Records
Example of records includes access to sensitive facilities, change control journaling, access control requests and approval process. The BS7799 certification auditor will expect to be given records for a three month period.
ISMS improvement and maintaining compliance

Once certification has been acquired it is imperative to ensure that the ISMS does not lose focus and the improvement cycle is effective with the lessons learnt fed back into improving the management process. The most effective way to maintain interest is by forming a special interest group and meeting on a regular basis (i.e. bi-weekly). It is not difficult to maintain compliance as this was a prerequisite of certification and the process must have been originally engaged.

The certification process includes a bi-annual review and surveillance audit every three years. Therefore it is very important to ensure a Gap analysis is conducted on an annual basis. It is also advisable to conduct ad-hoc spot checks on random components of the information security management system.

Concerns

There are a number of concerns to consider when implementing ISO 17799. First and foremost certification is a business decision and should not be taken lightly. No matter how professional an environment, it will still require significant management support to implement the Information Security Management System. It is essential you have senior management commitment and are they prepared to commit resources? Are you able to demonstrate the objectives of the project to gain sponsorship?

During the scoping phase it is imperative to consider what should and should not be within the scope of the project. Furthermore, proper planning at this stage can considerable reduce the stresses and risk during implementation.

Can you determine an acceptable level of risk? This will not be restricted to technology but will extend to all parts of the business including people, facilitates and processes. Have the risks been identified and quantified. Has consideration been given to which risks are treatable, by transferring responsibility, acceptance or mitigation?

Once the ISMS has been engaged are the audit mechanisms established to continuously monitor compliance, improve the management process by feeding back the lessons learnt and dovetailing the change management process. Will the budget extent to third-party assessments of the management system on a regular basis. Do you know when and what changes to the business will require review of ISMS?

The ISMS must not lose focus and be continually improved; it is much more difficult and expensive to reestablish the ISMS prior to a re-audit and demonstrates that the ISMS is really not suitable for the business.
Conclusion

From the smallest company to the largest conglomerate, business relies on the confidentiality, availability and integrity of information. Whereby in the past information security was applied on a piecemeal basis, today the boundaries have extended and businesses are demanding for more collaborative methods and business tools which are available in the public domain.

The result of the reliance on information has meant that the many security systems have failed to adequately protect the company’s assets. Regardless of the approach to information security and consideration to ISO 17799 an ISMS is a critical component of the management process.

Using a systematic management approach to information security, such as ISO 17799, a company is able to adopt best practice controls, quantify the level of acceptable risk and implement the mitigating measures which protect the confidentiality, integrity and available of information. The standard is recognised globally and provides an excellent stage for introducing effective protection measures.

Companies that are BS7799 Part 2 registered clearly demonstrate their commitment to protecting the interests of the company, employees, partners and shareholders.

© 2003 I-Defence Ltd.

Internet: http://www.i-defence.co.uk
Email: security@i-defence.co.uk