Framework of Information Security Management System (ISMS) Standards ISO 17799 / BS 7799

Muhammad M. Satti
Macquarie Corporate Telecommunications.
Sydney Australia.
msatti@macquarie.net.au

Mahmood H Nagrial
University of Western Sydney Australia
m.nagrial@uws.edu.au

Brian J. Garner
Deakin University Geelong Vic. Australia
brian@deakin.edu.au

Abstract

International Standards Organization (ISO) 17799 is originally derived from British Standards Institution (BSI) BS 7799. It is the intention of both standards to be a reference point from which information security management can be effectively and securely implemented. Assuring the confidentiality, integrity and availability of all information assets continue to be paramount during all phases of implementation. As the Internet community drives business further we are finding that it is network security, and in particular, Internet security, which is at the forefront of business network management and data integrity assurance practices. The trust of Internet user(s) especially for e-commerce and online businesses relies on a strong security mechanism (eg. digital certificate) offered by service providers. On the other hand a serious security commitment is required from higher management to the system administrator to endorse best method practices, defined in ISO 17799 / BS 7799 charter. It is at "ground zero" where the information security battle will be fought, with both ISO17799 and BS7799 providing the frameworks for designing and implementing a secure strategy created specifically to protect every facet of the business and user environment.

Keywords: Communication security; Information Standards; ISMS; Corporate Security; Internet Security; BS 7799; ISO 17799,

I. Introduction

" No enterprise is more likely to succeed than one concealed from the enemy until it is ripe for execution "

(Niccolo Machiavelli " The Art of War " 1469-1527)

Taking Information Security as a major corporate concern, an arm against Cyber-war, the British Standards Institution (BSI) has developed BS 7799 with some input from Australian contributors, in the mid 1990s. The need arose from the demand by government, corporates and industry sectors for common and standardized guidelines for designing and implementing an Information Security Infrastructure [1]. This particular standard covers the appropriate security deployment, and effective use of security controls. It also encompasses the preliminary "business risk analysis" which is primarily used to identify the unique business specific assets and the potential security, threats to them [2]. The key areas identified are delineated into ten points, as a *"body of knowledge"* from which all Information Security Officers can derive a clear reference path.
These points are mentioned below [1]:

A. Security Policy

The management of a user organization should make its commitment to information security clear to the entire organization, by defining the scope, objectives and depth of information security in a security policy. The security policy directs all security related activities in the organization [2].

B. Security Organization

A 'security organisation' should be set-up to manage information security within a user organisation. For example, who is responsible for which security activities, how is the co-ordination of organisational safeguards settled and how is the authorisation process for facilities defined.

C. Asset classification and control

To maintain appropriate protection of organizational assets, asset classification and control are recommended. Every asset should be assigned a level of protection

D. Personnel security

An underestimated risk. Addresses, among others, job descriptions, recruitment, screening, training for security awareness and type of response to reports on security incidents.

E. Physical and environmental security

Focused on the prevention of unauthorized access, damage and interference with, for example, employee and visitor badges, supply delivery, location of the data, computer centers and servers

F. Communications and operations Management

This includes, among others, operating procedures, procedures that answer questions such as " What to do when this incident occurs" separation of duties in the tasks of employees, separation of design and operational facilities, capacity planning, protection against malicious software and media handling.

G. Access control

Prevent unauthorized computer access by means of, among others, user registration, password management, review of user right, unattended user equipment, authentication means, network segregation, network routing and application access control.

H. Systems development and maintenance

Ensure that security is built into information systems, like Intrusion Detection systems (IDS), Firewalls data integrity checkers, log servers and physical security.

I. Business Continuity management

The user organization should cope with disasters such as lightning, bomb alarm and flood. Planning addresses, among other requirements, emergencies, fallback and resumption procedures, and a test schedule. Complete Disaster recovery Procedure (DRP) is required for an organization.

J. Compliance

The entire user organization should show compliance with information security requirements to avoid breaches of any relevant information security requirements.

Information Security Management System (ISMS), BS 7799 has been identified universally as a vital tool to identify, manage and minimize the range of threats to which information is regularly subjected. Some of the threats it helps to minimize or remove are [4]:

II. Classifications of common threats

There are many threats in Cyberspace and particularly on Internet, that the list can be exhausted, but in summary few are real management's concerns:

A. Internal threats

Defined as a trusted threat, e.g.: from partners, disgruntled employees, Inappropriate Data Manipulation, Fraud.

B. External threats / Business Espionage

Defined as originating from external sources to the business entity, e.g.: Competitors/Business Rivals, Industrial Espionage.

C. Accidents

Defined as "Acts of God" e.g.: Fire, floods, and natural disasters.

D. Malicious actions

Defined as Hacking, Denial of Service (DoS), attacks malicious damage

It is important to note at this point that a number of factors are causing both the increase and the significance of security threats within the corporate environment. Of these factors, the major threats are;

- An ever-increasing dependence on the business to store and manage information
- The burdening complexity of the business environment and its support systems
- The rapidly increasing discovery of vulnerabilities within every system type (Servers, software etc)

ISO/IEC 17799 Part 1 is a standard that contains over 100 security controls to help the Corporate and Government sectors to identify elements of their business that impact on information security. Part 2 of the same standard is a specification from which an organization can be assessed and registered for ISO/IEC 17799 compliance. The following documents are core systems in ISO/IEC 17799: Part 2 certification.

- Scope Statement,
- Security Policy and Security policy statement,
- Assets List, (preferably managed electronically; i.e. by the *Remedy* software)
- Once the Information Security Officer has produced documentation covering all ten

points on the "body of knowledge" mentioned above.
- In a format that is consistent with BSI guidelines

- Understanding and defining the geographical and physical situation of the business and how they affect the Information Security Plan

III. Preparation for ISO 17799 / BS 7799 Accreditation.

BS 7799 is in all respects a comprehensive and exacting standard to implement within any work place environment, both for a multinational corporate entity or a general-purpose business place. It demands a thorough study of its statements, and a complete understanding of its core requirements.

The outline given below in chronological order explains the author (s) experience, albeit briefly, while preparing for the Information Security Management Systems implementation, specifically, for BS 7799 accreditation for a Corporate Telecommunication Company [5].

A. Scope of Work

- Identifying the nature of the business and where information security is a paramount factor in its success.
- Understanding and defining the geographical and physical guidelines of the business and how they affect the information Security Plan.

B. Documentation

- Each and every process has to be documented, justified and signed off (where applicable) with the appropriate documentation.
- There may be a need for Technical Documentation specialists to frame the material in a format that is consistent with BSI guidelines.

C. GAP Analysis by External Auditors(s)

- Once the Information security Officer has produced documentation covering all ten points on the " *body of knowledge*" mentioned in the BS 7799 guideline, a third-party Auditor will review the documentation for "errors and omissions" before submission for a Stage 1 Audit [4].

D. BSI Lead Auditor(s) Final Audit

- At this point the organization officially applies to BSI for a review of their infrastructure including; documentation, processes and physical configuration.

- BSI Qualified Auditors review all facets rigorously and identify any non-conformity while onsite and under test conditions. This may take anywhere from five to seven working days to complete all the auditing aspects required under BSI recommendation

- The BSI Auditor(s) can operate autonomously and are empowered to decline any applications for BS7799 qualification based on any number of non-conformities to the code.

Once the organization(s) fulfilled the requirements and compliance with standards, the BSI issues a Certificate for the period of three years validity. This accreditation is subjected to adherence of rules and procedures set out in the BS-7799 document and summarises best methodology of professional practice along with continuous audit both internal and external. It is generally every six-month local (internal) audit by an organization's information Security Officer (ISO) and yearly by BSI auditor (External).

IV. Implementation Experience of Information Security Management Systems (BS 7799)

Information Security has attracted the serious concern of most of the corporate and government businesses. The Certification/ registration of an organization's information security management system (ISMS) is one means of providing assurance that the certified/ registered organization has implemented a system for the management of information security in accordance with other national level standards [6].

The need to share information is increasingly prevalent in all nations for cultural, social, economical and religious reasons. The Internet is a cost-effective platform. Geographical distances are no longer a barrier, and people can communicate instantly with each other. For example, 'Net Chat' is one of the popular communication and even entertainment and it is available almost without paying additional cost, for anyone having Internet access.

Table 1.0 shows the participation of countries, which have implemented a unique standard for managing their information security systems. This shows the commitment towards the global awareness and importance of information security standards

SNO	Region	No. Of Certificates
1	Australia	1
2	Austria	1
3	China	3
4	Egypt	1
5	Finland	5
6	Germany	5
7	Greece	2
8	Hong Kong	5
9	Hungary	1
10	Iceland	1
11	India	6
12	Ireland	3
13	Italy	1
14	Japan	8
15	Korea	7
16	Netherlands	1
17	Norway	6
18	Singapore	5
19	Spain	1
20	Sweden	4
21	Taiwan	3
22	UAE	1
23	UK	70
24	USA	3

TOTAL Accredited Organization = 144

Table 1.0. Depicts the BS 7799 International registration of Countries pursuant to their accreditation.

** From 1998, BS 7799 became ISO 17799, and all USA organization(s) implemented ISO 17799.*

V. Conclusion

The ISO 17799 and BS 7799 guidelines are fortunately not a single instance compliance requirement. As a part of compliance, there is a requirement for continually monitoring all facets of the Information Security system whilst actively encouraging ongoing improvements to the existing system. Consequently, an internal audit by the Information Security Office is required with a yearly examination by a qualified BSI auditor required to maintain the qualification. It is important to note that ANY change in business model, premises (physical location) or re-structuring of any significant type may lead to the accreditation being withdrawn [7].

It should also be noted that BS 7799 is not a quality standard as such! It assumes that the required actions to conform to the accreditation are going to be implemented using the correct processes by the applicant. The philosophy '*Say what you do and do what you say*' underpin the audit process. This re-enforces any corporate based Service Level Assurance (SLA) or Service Level Guarantees (SLG) by reason of already implemented internal processes. A service provider with such a process in place not only guarantees the credibility and stability of their own systems, but also assures the extension of those services to all customers and corporate entities that choose to do business with the provider.

VI. References

1. BS 7799: 2 1999 The Standards for Information Security Management BSI (UK), 1999.
2. Lehman Brothers "The Internet Security Investor Handbook'" March 2001.
3. A E, Hut. S, .Bosworth and BD, Hoyt." Computer Security Handbook" 3rd Edition, 1995
4. Information Security Evaluation Criteria (ITSEC) Ver. 1.2 April 2001,
5. Satti, M. Macquarie Corporate Telecommunication BS 7799 Documentations, 2001. http://www.mct.com.au/NewsArticles/Announcements/index.html
6. BS 7799 implementation http://www.xisec.com/Register.htm
7. Gateway Certification Guide Ver 2.0 Defence Signal Directorat (DSD), Canberra Australia, 2000. http://www.dsd.gov.au/infosec/Gateway/