Global Information Assurance Certification Paper

INFORMATION SECURITY MANAGEMENT SYSTEM (BS 7799-2:2002) IMPLEMENTATION OVERVIEW

Prepared by: **Mohammed Rifan**
Version Number: **GSEC Practical Requirements (v.1.4)**
Date: **January 19, 2004**

ABSTRACT

The British Standard has been prepared for business managers and their staff to provide a model for setting up and managing an effective Security Management System (ISMS). The adoption of ISMS should be a strategic decision for an organization.

BS7799 gives recommendations for information security management for use by those who are responsible for initiating, documenting, implementing or maintaining security in their organization. BS7799 also specifies requirements for establishing, implementing and documenting information security management systems.

BS7799 is actually "*a comprehensive set of controls comprising best practices in information security*"[2]. It is an internationally recognized information security standard.

The standard is intended to provide a common basis for developing organizational security standards and effective security management practices. It specifies requirements for security controls to be implemented according to the needs of individual organizations. In addition, this ensures that controls are effective – a valuable tool for both the IT Department and IT Audit community.

BS 7799 help to identify manage and reduce the range of threats to which information is continually exposed. Once compliance to, they provide organizations with the assurance and satisfaction of knowing that they are protecting their information using controls in common use by well-managed businesses. It is an excellent framework for developing or enhancing an organization's security structure.

Certification and Compliance

Compliancy with BS7799-2 requires an organization to have implemented and documented their Information Security Management System (ISMS) in accordance with the control objectives set outlined in the BS7799-2:2002 documentation.

BS7799-2 certification provides evidence and assurance that an organization has complied with the control objectives set out in the standards documentation. Certification outlines the scope of an organizations ISMS, and any exclusions to the control objectives.

In order to reach certification, organization must first achieve compliancy as set out in the BS 7799-2:2002 guideline. Once this has been achieved, the certification process requires an external review of by a BS7799 accredited auditor.

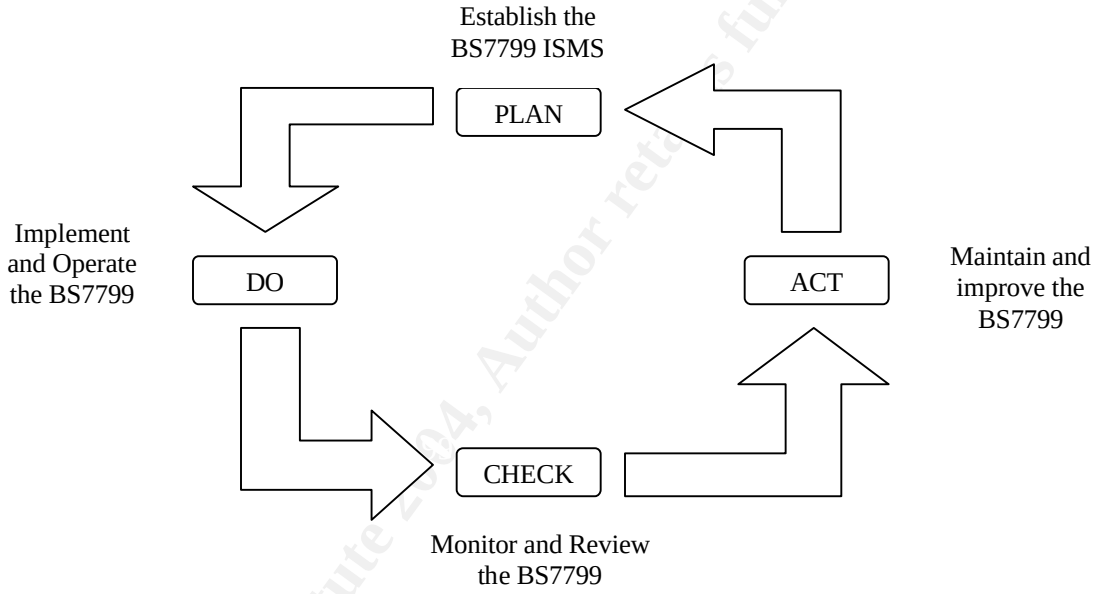
The auditor will work for a certified body or BSI; they will audit the organizations ISMS in line with the controls set out in the BS 7799-2:2002. On successful completion of the audit, organization will be awarded the BS7799-2 certificate.

The certificate will detail the scope of organizations ISMS and statement of applicability (SOA).

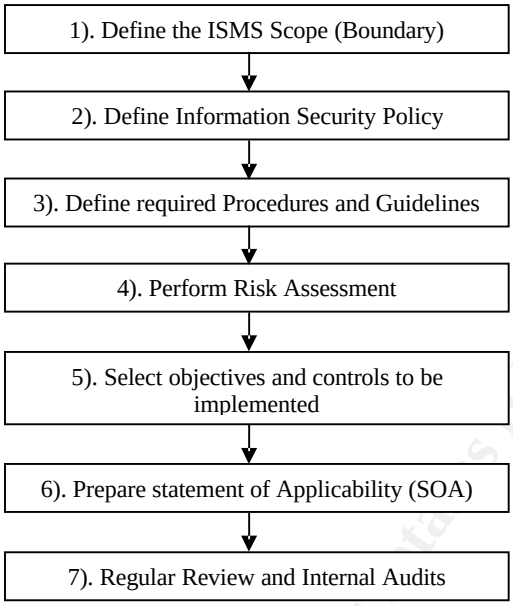
What is required to achieve compliancy?

This British Standard promotes the adoption of a process approach for establishing, implementing, operating, monitoring, maintaining and improving the effectiveness of an organization's ISMS. [2]

The model introduced by BSI, known as the "Plan-Do-Check-Act" (PDCA) model[2], can be applied to all ISMS processes.



Overview of BS7799 Implementation Process



Define the ISMS Scope:

Define the scope of the ISMS in terms of characteristics of the business, the organization, its location, assets and technology. The ISMS may cover all or part of an organization. Dependencies, interfaces and assumptions concerning the boundary with the environment need to be clearly identified. This is particularly relevant if only part of an organization is within the scope of the BS7799 ISMS.

Define Information Security Policy:

As building a good security policy provides the foundations for the successful implementation of ISMS, this is without a doubt the major measure that must be taken to reduce the risk of unacceptable use of any of the company's information resources.

The first step towards enhancing a company's security is the introduction of an enforceable security policy, informing staff on the various aspects of their responsibilities, general use of company resources and explaining how sensitive information must be handled. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities.

The development (and the proper implementation) of a security policy is highly beneficial as it will not only turn all of staff into participants in the company's effort to secure its Information's but also help reduce the risk of a potential security breach through mistakes. These are usually issues such as revealing information

to unknown (or unauthorized sources), the insecure or improper use of the Internet and many other activities.

The Information Security Policy contains the IT security objectives which the organization has set itself and the IT security strategy it pursues. In this way it constitutes both an aspiration and a statement that the IT security level specified is to be achieved at all levels of the organization.

The document acts as a "must read" source of information for everyone using in any way systems and resources defined as potential targets.

In order to realise the importance of a security policy, staff need to be aware and fully understand the consequences of violating the policy, thereby exposing critical systems to a malicious attacker, or causing unintended damage to other companies worldwide. Violations should be handled accordingly; those who in one way or the other violate the security policy should be made aware that they may face being put through a "trial period", which involves also the limited use of some of the company information assets until they can show they are able to act in a secure manner while using the corporate systems. They should also be aware that in some cases they also may risk being fired.

Define necessary Standards, Procedures and Guidelines:

Standards are *definite requirements* that an organization should put forth for everybody to follow. The standards should support the security policy and be measurable. It is good practice to document what the penalties are when standards are not met

Guidelines are *recommended ideas* for an enterprise. They can also be termed as ‘nice to haves’. It should be noted that the effectiveness of an organization’s security management will not be measured by the guidelines present. There, usually, are no penalties for not following the guidelines. However, there can be some incentives if the enterprise follows the guidelines.

Procedures are *step by step description* on how to meet the standards or guidelines so that the policy is supported. Procedures are usually targeted at the system level people who actually implement the control.

Perform Risk Assessment

Risk assessment is a fundamental prerequisite of BS7799-2. The standard does not require to use any particular approach, nor does it list any approved methods. Choose a method that is appropriate to organization and the scope of ISMS. Whatever methodology choose to adopt, as an absolute minimum should ensure

that it delivers the control environment that is documented within the policies and procedures of organization's own information security manual.

As in any other sensitive procedure, Risk Analysis and Risk Management play an essential role in the proper functionality of the process. Risk Analysis is the process of identifying the critical information assets of the company and their use and functionality -- an important (key) process that needs to be taken very seriously.

Essentially, it is the very process of defining exactly WHAT you are trying to protect, from WHOM you are trying to protect it and most importantly, HOW you are going to protect it.

The risk assessment documentation should explain which risk assessment approach has been chosen, and why this approach is appropriate to the security requirements, the business environment, and the size of the business and risk the organization faces. The approach adopted should aim to focus security effort and resources in a cost-effective and efficient way. The documentation should also cover the tools and techniques that have been chosen explain why they are suitable for the ISMS scope and risks, and how they should be used correctly to produce valid results.

The objective of a risk assessment, in the context of BS7799, is to balance the safeguards identified in the Statement of Applicability against the risk (i.e. probability) of failing to meet business objectives.

Implementing sound strategies for managing information security risks is vital given the scarcity of resources and budgets, and the need to keep abreast of organizations need to get services and products to market as quickly as possible.

Designing and implementing an appropriate risk management strategy requires the assistance of a number of people within an organization, such as staff from business areas, technology, personnel, finance, legal etc.

In order to be able to conduct a successful Risk Analysis, need to get well acquainted with the ways a company operates; if applicable, the ways of working and certain business procedures, which information resources are more important than others (prioritising), and identifying the devices / procedures that could lead to a possible security problem.

List everything that is essential for the proper functionality of the business processes; like key applications and systems, application servers, web servers, database servers, various business plans, projects in development, etc.

A possible list of categories to look at would be:

- **Hardware**: All servers, workstations, personal computers, laptops, removable media (CD's, floppies, tapes, etc.), communication lines, etc.
- **Software**: Identify the risks of a potential security problem due to outdated software, infrequent patches and updates to new versions, etc. Also take into account the potential issues with staff installing various file sharing apps, entertainment or freeware software coming from unknown and untrustworthy sources.
- **Personnel**: Those who have access to confidential information, sensitive data, those who "own", administer or in any way modify existing databases.

What are the risks? Determine these by a consideration of the impacts that would occur if some threat exploits a weakness in defenses to compromise the security of an asset, and how likely is the impact to occur.

Risk assessment is systematic consideration of:

a) The valuation of the assets within the ISMS, including information about the valuation scale used when it is not monetary.

b) Identification of threats and vulnerabilities

c) The business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets.

d) The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

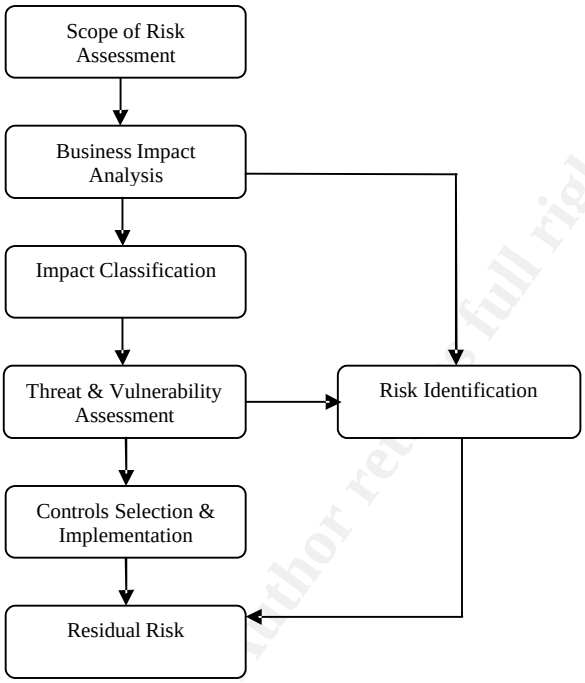
The results of this assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

It is important to carry out periodic reviews of security risks and implemented controls to:

a) take account of changes to business requirements and priorities;
b) consider new threats and vulnerabilities;
c) Confirm that controls remain effective and appropriate.

Reviews should be performed at different levels of depth depending on the results of previous assessments and the changing levels of risk that management is prepared to accept. Risk assessments are often carried out first at a high level, as a means of prioritizing resources in areas of high risk, and then at a more detailed level, to address specific risks.

Information Security Risk Management Stages in Risk Management Methodology:



Select Control Objectives and Controls to be implemented

Once security requirements have been identified, security controls should be selected and implemented to ensure risks are reduced to an acceptable level.

Controls can be selected from BS7799-2:2002 control sets, or new controls can be designed to meet specific needs as appropriate. It is necessary to recognize that some of the controls are not applicable to every information system or environment, and might not be practicable for all organizations.

Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Non-monetary factors such as loss of reputation should also be taken into account.

It might not always be possible to reduce risks to an acceptable level within an acceptable cost, and then a decision should be made whether to add more controls, or accept the higher risks. When setting an acceptable level of risk the

strength and cost of control should be compared with potential cost of an incident.

A number of controls can be considered as guiding principles providing a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common best practice for information security. Controls considered being essential to an organization from a legislative point of view.

BS7799-2:2002 Contains 36 Control Objectives and 127 Controls. And broadly divided into 10 Detailed Control Clauses

1. Security Policy
2. Organization Security
3. Asset classification and control
4. Personnel Security
5. Physical & environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

1. **Security Policy** [2]
   Security policy is general statement produced by senior management to dictate what type of role security plays within the Organization. Security policy will demonstrate management support and commitment to the Information security management.

2. **Organization Security**[2]

   The efficient implementation of ISMS and review of their efficiency required a well thought out, controlled IT security process. So it is important that functional IT security management is established at the start of the IT security establishment process. Security management's functions involve determining objectives, scope, policies, priorities, standards and strategies.

   The necessary resources, funding and strategic representatives need to be available and ready to participate in the ISMS implementation. Management must assign responsibilities necessary to get the ISMS Program implemented and maintained. Appropriate tasks must be assigned to each role, and these roles must be served by staff with the appropriate skills. This is the only way to ensure that all important aspects are taken into consideration and that all tasks are carried out efficiently and effectively.

   Inadequate IT security management is often a symptom of a poor overall organisation of the IT security.

   While considering the organization information security, it is important to have proper controls and policy in place for accessing organizations information assets by third party

   When responsibility of information processing has been outsourced, it is important that third party contract should address legal requirements, specifications and any protection mechanisms required to safeguard the organizations assets and information.

3. **Asset classification and control** [2]

   It is essential to classify information according to its actual value and level of sensitivity in order to deploy the appropriate level of security. A system of classification should ideally be:

   - *simple to understand and to administer*
   - *Effective in order to determine the level of protection the information is given.*

- *Applied uniformly throughout the whole organization (note: when in any doubt, the higher, more secure classification should be employed).* [5]

All major information assets should be accounted for and have a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be delegated.

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, and the business impacts associated with such needs.

It is important that an appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by the organization.

4. Personnel Security [2]

Security responsibilities should be addressed at the recruitment level and should include in contracts as well. All employees and third party users of information processing facilities should sign a non-disclosure agreement.

New staff must be made aware of the organizations IT-related regulations, practices and procedures.

Every staff member must be made aware of the need for IT security. Employees must be educated and trained in any general responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities and information security related threats, incidents reporting.

5. Physical & environmental security [2]

Physical security is defined as that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard against sabotage, damage, and theft.

Physical security needs must be reviewed and upgraded wherever necessary. Physical security remains a vitally important component of an

overall information security plan. Critical or sensitive business information processing facilities should be kept in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference.

A clear desk and clear screen policy is recommended to reduce the risk of unauthorized access or damage to papers, media and information processing facilities.

6. Communications and operations management [2]

Operations refer to the tasks and processes involved in up and running an IT System. The primary goal of operations is to ensure continued correct operation of systems, a goal clearly relate to the security goals of confidentiality, integrity and availability.

Operations security is used to identify the controls over hardware, media and the operators with access privileges to any of these resources.

Responsibilities and procedures for the management and operation of all information processing facilities should be established. Changes to information processing facilities and systems should be controlled. This can be achieved by the implementing proper change control procedure. Operational programs should be subject to strict change control.

Separating development, test and operational facilities is desirable to reduce the risk of accidental change or unauthorized access to operational software and business data.

Communication Security Refers to the proper safeguarding of everything associated with a network, internal and external communication lines, including data, media, and equipment. It involves administrative functions, such as threat assessment, and technical tools and facilities such as cryptographic products, and network access control products such as firewalls. It also involves making certain that network resources are used in accordance with a prescribed policy and only by people who are authorized to use these resources.

7. Access control [2]

Access control is considered to be the cornerstone of any security programs. The various features of physical, technical, and administrative access control mechanisms work together to construct the security architecture so important in the protection of an organization's critical and sensitive information assets.

The decision of which access controls to implement is based on organizational security policy. Generally two access control standards of practice are used, least privilege and separation of duties.

To ensure that access controls adequately protect all of the organization's resources, it may be necessary to first categorize the resources.

Whatever access control mechanism is used, it must be comprehensive, easy to use and well backed by activity logs.

8. Systems development and maintenance [2]

Systems development and maintenance security refers to the controls that are included within systems and applications software and the steps used in their development. The applications may be used in distributed or centralized environments.

In Systems development and maintenance security basically considered in the following areas, applications (systems, software) development and how security can be integrated into the software development life cycle; security controls in programs, database management systems and security issues they face and controls they implement, malicious code (e.g., viruses, Trojan horses) approaches, defenses and harm that can occur from programs or code (malicious or not) and countermeasures.

9. Business continuity management [2]

Business Contingency Planning continually confronts the unlikelihood of a disaster. An interruption could be something related to a storm, Civil Unrest, Sabotage, Terrorist Activities, Power Grid Failure, Telephone Failure or the complete and inaccessibility of a facility for an extended period of time.

Totally unexpected causes can also cause significant business interruption which could be disastrous to the corporations. Depending on the length or severity of the interruption, significant consequences or the

very survivability of the corporation may depend on management's ability to reestablish critical business functions. The cause of the interruption doesn't matter, but being capable of gaining management control of the interruption is important. Reestablishing the complex business environment in a timely manner requires a well thought out plan in place ready to be executed.

A disaster recovery plan is a comprehensive statement of consistent actions to be taken before, during and after a disaster. The plan should be documented and tested to ensure the continuity of operations and availability of critical resources in the event of a disaster.

The primary objective of disaster recovery planning is to protect the organization in the event that all or parts of its operations and/or computer services are rendered unusable.

The procedures should include methods for maintaining and updating the plan to reflect any significant internal, external or systems changes. The procedures should allow for a regular review of the plan by key personnel within the organization.

The disaster recovery plan should be structured using a team approach. Specific responsibilities should be assigned to the appropriate team for each functional area of the company.

It is essential that the plan be thoroughly tested and evaluated on a regular basis (at least annually). Procedures to test the plan should be documented. The tests will provide the organization with the assurance that all necessary steps are included in the plan.

10. Compliance [2]

The design, operation, use and management of information systems may be subject to any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements. All relevant statutory, regulatory and contractual requirements shall be explicitly defined and documented for each information security system.

Appropriate procedures should be implemented to ensure compliance with legal obligations on the use of material in respect of which there may be intellectual property rights.

All areas within the organization should be considered for regular review to ensure compliance with security policies and standards. Owners of information systems should support regular reviews of the compliance of

their systems with the appropriate security policies, standards and any other security requirements.

Prepare statement of Applicability (SOA):

An organisation will need to document the selected control objectives and controls, the reasons for selection and justification for the exclusion of any of the controls listed in the BS 7799-2:2002. Not all the controls described will be relevant to every situation, nor can they take account of local environmental or technological constraints, or be present in a form that suits every potential user in an organization. Organizations need to identify the most appropriate control objectives and controls to be implemented which are applicable to their own needs.

Having defined the SOA meant that the Organisation could now focus on the areas of security that required improvements. This was a tremendous help and meant that the organisation had a clear starting point and clear direction to take in addressing some of the security issues identified through the Risk Assessment.

The statement of applicability needs to be accessible to managers; personnel and any third party (auditors, etc.) authorized to have access to it.

Regular Review and Internal Audits

Auditing is the review and analysis of management, operational, and technical controls.

The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with security implementation standards.

Properly defined Internal Audit will explain organizations current compliance position with respect to each section of BS 7799. A follow-up audit can determine the success which is achieved by the implementing appropriate actions.

CONCLUSION

Information is already recognized as critical success factor both in the private and public sector. Hence, information needs to be protected and kept secure. Just looking for technical approaches is not sufficient. Without a systematic management of information there can be not effective protection. The BS7799 standard is a first step towards internationally recognized baseline security standards, against which organisation can certify themselves.

Achieving compliance with BS 7799 is a significant task. Assessing compliance levels for information systems, and then creating/implementing the necessary plans to become fully compliant, can by a very intensive process indeed. However, with the correct approach and method this effort can be minimized.

Registration after BS7799 Part 2 will especially help those organizations that want to demonstrate to customers and other stakeholders that confidentiality, integrity, and availability are always ensured.

References:

Internet

1) http://www.all.net/books/audit/bs7799.html (Summary of controls used in BS7799)
2) http://www.bsi-global.com/Corporate/17799.xalter (BS 7799)
3) http://www.securityauditor.net/iso17799/ (ISO 17799 Security Standard)
4) http://www.gammassl.co.uk/bs7799/works.html (How 7799 Works)
5) http://www.iso17799-web.com/issue9.htm(THE ISO17799 NEWSLETTER)

Literature

1. Information Systems Security: A Practitioner's Reference Second Edition, by Philip E. Fites, Martin P. Kratz
2. CISSP All-in-One Exam Guide, Second Edition (All-in-One) - by Shon Harris