GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

**Name: Avinash Kadam**

**Version Number: GSEC Practical Requirements (v.1.4b) (August 2002)**

# Title: Implementation Methodology for Information Security Management System (to comply with BS 7799 Requirements)

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

# INDEX


| Topic | Page No. |
|---|---|
| Abstract | 3 |
| Overview of BS 7799 standard | 3 |
| The twelve steps to Information Security 'Nirvana' | 3 |
| Step 1: Establish the importance of Information Security in Business | 5 |
| Step 2: Define the Scope for ISMS [5] | 7 |
| Step 3: Define the Security Policy [10] | 8 |
| Step 4: Establish the Security Organization Structure | 8 |
| Step 5: Identify and Classify the Assets | 9 |
| Step 6: Identify and Assess the Risks6 | 12 |
| Step 7: Plan for Risk Management [6] | 15 |
| Step 8: Implement Risk Mitigation strategy | 18 |
| Step 9: Write the Statement of Applicability | 20 |
| Step 10. Train the staff and create Security Awareness | 21 |
| Step 11. Monitor and Review the ISMS performance | 22 |
| Step 12. Maintain the ISMS and ensure continual Improvement | 23 |
| ISMS Documentation | 25 |
| Implementation Schedule for BS 7799 [7] | 28 |
| References | 29 |


© SANS Institute 2003, Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

# Implementation Methodology for

# Information Security Management System

### (to comply with BS 7799 Requirements)


## Abstract

Importance of the information security is now well understood by the business managers. Organizations, whose very existence depends on the information technology, usually take all necessary precautions to protect it. However, like Caesar's wife, information should not only be pure/secure, it should also appear to be pure/secure. This demonstration of security is often required to convince customers, business partners and government. Periodic security audits conducted by external auditors is an accepted procedure. Acquiring a security certificate like BS 7799, that requires adherence to the standard and periodic external audits is rapidly gaining importance. Number of BS 7799 certified organizations increased from 104 in April 2002 to 197 in Feb. 2003. [4]

This paper presents an overview of the requirements of the BS 7799 standard and a twelve-step methodology for systematic implementation of the 'Information Security Management System' (ISMS) in an organization. If followed stringently, it can lead to BS7799 certification.


## Overview of BS 7799 Standard [9]

An organization can achieve recognition for its information security efforts by getting a BS 7799 certificate for its 'Information Security Management System' (ISMS). The BS 7799 provides two standards for this purpose. BS 7799 -1:2000, which is also adopted by ISO as ISO/IEC 17799:2000, provides a code of practice for information security management. This standard, which is known by the composite name BS ISO/IEC 17799:2000 provides "a comprehensive set of controls comprising the best practices in information security". [1]

Second standard, which is known as BS 7799-2:2002 provides specifications with guidance for use. This can be used by, "internal and external parties including certification bodies, to assess an organization's ability to meet its own requirements, as well as any customers or regulatory demands". [2] The standard provides a list of 10 main control domains comprising of 36 control objectives and 127 controls, which are used for the assessment.

The standard promotes the adoption of a "process approach for establishing, implementing, operating, monitoring and improving the effectiveness of an organization's ISMS" [2]. Keeping this approach in mind, this paper presents a twelve-step methodology for systematic implementation of Information Security Management System in an organization.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**The twelve steps to Information Security 'Nirvana'**

The twelve steps described below are based on the Plan, Do, Check and Act (PDCA) model suggested by the BS 7799 standard. [7]

Plan (establish the ISMS)

Step 1: Establish the importance of Information Security in Business
Step 2: Define the Scope for ISMS
Step 3: Define the Security Policy
Step 4: Establish the Security Organization Structure
Step 5: Identify and Classify the Assets
Step 6: Identify and Assess the Risks
Step 7: Plan for Risk Management

Do (Implement and operate the ISMS)

Step 8: Implement Risk Mitigation strategy
Step 9: Write the Statement of Applicability
Step 10. Train the staff and create Security Awareness

Check (monitor and review ISMS)

Step 11. Monitor and Review the ISMS performance

Act (Maintain and improve the ISMS)

Step 12. Maintain the ISMS and ensure continual Improvement

© SANS Institute 2003, Author retains full rights.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**Step 1: Establish the importance of Information Security in Business**

Information security is very important for the business. However, it's importance is generally not understood fully and so, it is not emphasized enough. As figures speak louder than mere words, resulting business losses should be quantified as a consequence of hypothetical/simulated/actual security breaches. The procedure to be followed is as below:

a. Identify and document the business objectives, critical business processes and critical IT processes [10]

Objective of the information security is to provide security to the IT processes that carry out business functions to achieve the business objectives. You may have to interview top management, business managers and various end-users to understand the business objectives and various business processes deployed by the organization to achieve these. From these, select the critical business processes. These will usually be time-sensitive operations for which, reliable information has to be made available, in time. For example, the supply chain management system or enterprise resource planning system or client relationship management process of the organization. The IT systems performing these business-critical functions would be the critical IT-processes.

b. Identify dependence of business on IT systems [3]

You do not have to be a business consultant to perform this analysis. Asking a few 'what if? ' type of questions to the business managers will establish the dependence of business on IT.

Categorize the business dependence as:

Basic to moderate (1): Where the business process can be performed by alternative means, with a modicum of additional expense.

Or

High (2): Where the business process or specialist task can be performed by alternative means (e.g. manually) at a significant additional expense.

Or

Very high (3): Where the business process or specialist task cannot be performed at all without the IT application.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

c. Protection requirement from damage scenario [3]

Identify various damage scenarios, caused by the loss of confidentiality, integrity or availability of information. These could be based on experience, published cases/incidents for your industry, your geographical location or other industries dealing with similar products or services.

The six damage scenarios are:

- Violation of laws, regulation or contracts
- Breaches of the privacy of an individual
- Physical injury
- Prevention from performance of normal duties
- Negative effect on external relationship
- Financial consequences

Categorize the protection requirement against loss of confidentiality, integrity and availability for each of the above damage scenarios. Higher the number, higher is the protection requirement.

Categorize the business impact if any of the damage scenarios materializes, as:

Basic to moderate (1): The impact of any loss/damage is limited
Or
High (2): The impact of any loss/damage may be considerable
Or
Very High (3): The impact of any loss/damage can attain catastrophic proportions, which could threaten the very survival of the organization.

Identify the number signifying the business impact and protection requirement rating for the three parameters, confidentiality, integrity and availability from the business impact and protection requirement reference matrix. One example of a matrix for confidentiality is given below:

| Business Impact | Protection Requirement for Confidentiality | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 |
| 2 | 2 | 3 | 4 |
| 3 | 3 | 4 | 5 |

Refer to similar matrices for integrity and availability.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

You will be able to prioritize the information security requirement for your organization, based on the ratings. Higher the rating, more critical is the IT process for business, requiring higher protection.

Table for prioritizing the information security requirement:

| Rating | Description |
|---|---|
| 1 | Little business impact, low protection requirement (C/ I / A)* |
| 2 | |
| 3 | |
| 4 | |
| 5 | High business impact, high protection requirement |

* Confidentiality, Integrity, Availability

**Step 2: Define the Scope for ISMS [5]**

The process of prioritizing the protection requirements for individual business areas, based on business impact, should give us a good measure of the critical IT processes requiring a good ISMS. Describing these processes will define the scope for ISMS for the organization. Your subsequent efforts will be to secure the systems defined as per this scope. BS 7799 audit and the certificate will be specific to this scope. If you add more physical locations or business processes which change the scope, you will have to reapply for BS 7799 certification as per the new scope.

Include the following details to make the scope complete:

- Description of the organization
- Description of the business function
- Description of geographical location
- Business processes included in the scope
- Information systems included in the scope
- A physical layout of the location
- A logical networking diagram

If some areas of business operation are being excluded, reasons for the exclusions should be documented and justified.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**Step 3: Define the Security Policy [10]**

Security policy is the demonstration of management's intent and commitment for the information security in the organization. This should be based on facts about the criticality of information for business as identified during step 1. Security policy statement should strongly reflect the management's belief that if information is not secure, the business will suffer. The policy should clearly address issues like:

- Why information is strategically important for the organization?
- What are business and legal requirements for information security for the organization?
- What are the organizations' contractual obligation towards security of the information pertaining to business processes, information collected from clients, employees etc.?
- What steps the organization will take to ensure information security?

A clear security policy will provide direction to the information security efforts of the organization as well as create confidence in the minds of various stakeholders.

The Chief Executive of the organization should issue the security policy statement to build the momentum towards information security and set clear security goals and objectives.

**Step 4: Establish the Security Organization Structure**

After issuing the security policy statement, the first step an organization should take is to establish a security organization structure. This is necessary to ensure organization's involvement in identifying and implementing various security measures.

The security organization should consist of the following:

- Security Steering Committee headed by the Chief Executive and including representatives from key business and technology departments.
- Information Security Officer (ISO) should be the secretary of this committee and will be responsible for coordinating the security efforts of the organization.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- The ISO should form various security teams to carry out security responsibilities, like

    - Incident Response Team
    - Security Maintenance Team
    - Security Training Team
    - Disaster Recovery Team
    - Security Policy Owners

    ISO should coordinate the activities of all these teams. The team members of these teams could be either full time members or part time, depending on the size and requirements of the organization.

Information Security Officer plays a key role in the security organization. He will have to shoulder the following responsibilities:

- The ISO should define security roles and responsibilities for identification and protection of various information assets by specific individuals, including end-users, who are responsible for handling these assets.
- ISO should be responsible for designing and implementing detailed security policies to cover all the areas to be addressed by ISMS.
- ISO should coordinate periodic reviews of the security efforts by internal and external experts as well as auditors.

**Step 5: Identify and Classify the Assets**

In step 1 we identified critical business processes and the IT systems, which support these critical business processes. Each IT system in turn comprises of various information assets, which are created by the organization to perform the business functions. These information assets utilize other critical components like software, hardware, physical and infrastructure facilities to perform designated task in an efficient and secure manner. Identification of all such information assets and critical components and maintaining an up-to-date record is essential to know what we intend to protect. Once we have this inventory, next step is to devise a scheme for classifying the assets, based on their criticality towards confidentiality, integrity and availability of information. This classification is necessary to implement various protection measures.

The assets are grouped under the following categories:

- Information assets:
    - These are the assets, which have been created by the efforts of an organization and would be most difficult to replace. Examples are databases, documentations, procedures, plans, drawings, diagrams etc. These in turn will be stored on various types of media like


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

paper, magnetic tapes, magnetic disc drives, optical discs and many other media which are becoming more and more compact in size and larger in capacity.
    - These critical assets should be carefully protected throughout their life, but their death should be final and irrevocable if the authorities order deletion. Removal or movement of a critical information asset needs to be thoroughly controlled. An information asset could be temporarily transformed from the data element in a database to an attachment of an email stored on the hard disk, to a printed copy of the email and finally as a fax document. The protection as well as deletion schemes should protect or delete the critical asset in all its forms, simultaneously and entirely.
- Software assets
    - Application software, system software, development tools and utilities are part of these assets. Application software, which has been developed in-house or customized, would be difficult to replace compared to the off-the-shelf software. Depending on the assessment done during Step 1 we should be able to identify the critical software assets, which will require a higher level of protection.
- Physical Assets
    - All the hardware devices, communication devices, magnetic media, technical infrastructure devices like power supplies, air conditioning units etc. are part of these assets. Storage medium, by itself, may not be a high-cost item but if it contains vital, critical information or software assets, its security rating will go up.
- Services
    - Computing and communication services, general utilities like heating, lighting, power, air-conditioning etc. Step 2 will provide a detailed scope for ISMS, which will define the areas, that are critical for the business, and dependence on these services make them critical too.

**Asset Identification**

An identification scheme should uniquely identify each of the above listed assets. This could be part of an organization-wide asset tracking system, to avoid duplication of the effort.

Following information should be compiled for the organization:

- List of information systems included in the ISMS
- List of assets and their owners
- Replacement value of these assets
- Location of the assets
- Classification of these assets as per the scheme described below


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**Asset Classification:**

Individual information assets will have to be classified based on the C, I, A classification of the individual IT systems.

Example: Human Resources System

> Confidentiality : Very high, the employee data should be maintained at highest confidentiality level.
> Integrity : Medium, the data is verified at various stages and any changes to it would be detected.
> Availability: Low, the system is not required on-line. A delay of up to one day in getting requisite information is acceptable.
>
> Security classification of components of the HR System will have following classifications:

| Component | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Database | Very high | Medium | Low |
| Server | Very high | Medium | Low |
| Backup tapes | Very high | Medium | Medium |
| Services | Low | Low | Low |

**Information access classification**

Based on the C, I, A classification done for the IT systems in Step 1, each of the IT system will have appropriate access classification.

Most business organization follow a four level classification for providing access to the information systems

**Unclassified**: Considered publicly accessible. There are no requirements for access control or confidentiality.

**Shared**: Resources that are shared within groups or with people outside of your organization.

**Company Only:** Access to be restricted to your internal employees only.

**Confidential:** Access to be restricted to a specific list of people.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Specific portions of HR database would be identified and classified for the defined level of access. Only the HR database owner, i.e. the Head of HR, should be responsible for this classification.

Once appropriate classification of information on HR database is done, following access control table could be built:

| | Unclassified | Shared | Company Only | Confidential |
|---|---|---|---|---|
| Public | ⌋ | | | |
| Employees | | ⌋ | | |
| Head of the Departments | | | ⌋ | |
| Head of HR | | | | ⌋ |

Controlling access to various information assets is thus based on defining who has access to what information through access control lists (ACL). The ACLs are implemented through various security measures like data base access control tables as well as perimeter security devices like access control cards and firewalls.

Final responsibility for defining the information classification and access permissions rests with the owner of the information asset.

**Step 6: Identify and Assess the Risks[6]**

From previous step 5, we should have a comprehensive list of all the critical assets whose failure could impact a business. We will also have the C, I, A rating for each of these assets which will help us in identifying suitable protection measures, commensurate with the C, I, A ratings of individual assets. We should now proceed to identify and assess risks to these assets.

**Perform a threat analysis**

Every asset is exposed to numerous threats. These threats are broadly classified in three categories:

Natural Threats - These are Acts of God like floods, earthquakes, tornados, landslides, avalanches, electrical storms and other such events.

Environmental Threats – Long term power failure, pollution, chemicals, liquid leakage etc.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Human Threats – Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).

Make a comprehensive list of all the threats, which are likely to occur.[6] This list will have to be made, based on interviews, past records and experience of similar industries as well as organizations located in similar geographical areas and subjected to similar environment.

**Perform a vulnerability analysis**

Vulnerability is a weakness in the design of a system, which could be exploited by a threat. Discovering such vulnerabilities is the objective of this analysis. Following methods could discover the vulnerabilities.

Design documentation review: Do a complete design review beginning with the design specifications. You may discover that security was not a part of the specifications and hence was not implemented in the design.

This is because majority of the present-day Information Systems have evolved from a central configuration to a networked one, and this evolution has thrown new challenges to the security professionals. Information Security is only an afterthought of these systems.

Review incident logs: The historical incident logs, where available, will give a good insight into the vulnerabilities of a system.

Physical inspection of the premises: This is essential when identifying vulnerabilities. The premises could be exposed to natural and environmental threats.

Tools based security testing: [12] Various vulnerability assessment tools could be used to identify weaknesses, which are usually exploited by a hacker. This means that the same tools that are used by a hacker to break into a system should be used to test the strength of the system. Use of these security-testing tools could sometimes threaten the security. Hence prior written permission must be obtained before applying the tools.

Social engineering: [12] Social engineering is one of the most effective techniques used by a human attacker. Similar technique should be employed to test the vulnerabilities, which are usually present because of the lack of the security awareness. Similar to the use of security testing tools, social engineering should be used only with prior written permission.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Use of risk analysis tools: [11] Various commercial risk analysis tools are available to aid an organization in evaluating the level of security. These have large databases of questions, which help in analyzing the risks.

Examples of such tools are Cobra [14] and CRAMM [15].

**Assign overall vulnerability ratings**

Based on the threat and vulnerability analysis, each threat and vulnerability could be assigned specific rating based on what is the severity of the vulnerability and what is the resultant exposure.

Minor severity (1) of vulnerability means that the hacker requires significant resources to exploit it, whereas high severity (3) vulnerability means that the hacker requires few resources to exploit it with significant potential for loss.

Minor exposure (1) means that the effects of vulnerability are tightly contained where as high exposure (3) affects a majority of system components.

Vulnerability severity and exposure combined rating matrix gives a composite rating:

| Severity Rating | Exposure Rating | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 |
| 2 | 2 | 3 | 4 |
| 3 | 3 | 4 | 5 |

Overall vulnerability rating could be tabulated as per the following table:

| Rating | Description |
|---|---|
| 1 | Minor exposure, minor severity |
| 2 | |
| 3 | |
| 4 | |
| 5 | Highly exposed, high severity |


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**Asset risk evaluation:**

Now that we have a comprehensive list of risks, threats and vulnerabilities rating as per the severity and exposure rating, next step is to evaluate the level of risk that the organization is exposed to:

There are two factors that need to be considered.

Probability signifies the confidence level that a threat will be successful, in view of the current level of controls. Probability is directly related to the overall vulnerability rating calculated in the previous step and could be expressed as a percentage.

Consequences of a successful threat attempt are based on the business risk evaluation. These should preferably be expressed as monetary figures.

Level of risk is the product of probability and consequence. This gives an absolute value if consequences are expressed in monetary terms or relative value if the consequences are shown as a relative number. Whatever is the measure used, the level of risk could be used for prioritizing the security implementation efforts.

Table for identifying Level of risk:

| Description of risk | Probability of a threat exposing a vulnerability | Consequences (preferably tangible) | Risk rating (Level of risk) = Probability X Consequences |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Step 7: Plan for Risk Management [6]**

Options for risk management are based on cost benefit analysis of various options available to handle the risk.

These are:

Transfer the risk: For example, take a fire insurance policy and transfer the risk for fire to an insurance company.

Avoidance of the risk: For example, if there is an old server, which is malfunctioning, replacing it will avoid all the associated risk.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Acceptance of the risk: You are aware of the risk but the solution to avoid the risk is too costly. You decide to live with the risk and face the consequences.

Risk reduction: You decide to take the bull by the horn and plan to identify the security measures, which will reduce the risk to an acceptable level.

BS 7799 provides the 127 controls, which can be deployed to reduce the risk.[2, 8] However, these controls are general in nature. Selection of specific controls should be based on threat and risk assessment performed in the earlier step.

Following steps could be followed to select appropriate controls:

Define security policies: [16, 17] This should be the beginning point for risk reduction. Security policy statement described in Step 2 was to demonstrate the management's commitment towards information security. Detailed security policy statements define the operational level commitment to tackle each of the security risk identified during the threat and risk assessment. For example, if electronic mail is recognized as a business critical function, every risk to electronic mail system as well as the threats that could be carried out by using electronic mail system will be addressed by an 'Electronic mail security policy document'. This policy should cover the organization's concern, approach to tackle the security issue and compliance requirements.

Define procedures: Procedures define details regarding implementation of the security policy. These will provide details like responsibilities of various groups, actions to be taken for preventing, detecting, correcting and reporting security lapses.

Define standards: Organization may decide adhering to some international standards in the area of information security. For example, for email security, the organization may select S/MIME as the standard for secure email exchange.

Identify security products: Security policy cannot be implemented just by having well defined administrative procedures. It may be necessary to select some products to implement some of the clauses of security policy. For example E-mail security policy may state that the user should not use profane, obscene language in the email. Only a device like content filter could detect violation of this policy by users.

Cost vs. benefit: Finally, selection of the control depends on cost vs. benefit analysis. We should check whether cost of implementation of control is more than the risk we are attempting to reduce. For example, if we have to select the access control device for a location, we have a bewildering range of controls, ranging from simple swipe card system to biometric devices like retina scanners. Selection will be based on the C, I, A rating of the objects we are trying to protect and the business impact of the security compromise. We have to take a judicious


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

decision and select the control whose cost is less than the risk it is attempting to reduce.

Current state assessment and gap analysis: Prepare a table of all the Threats / Risk and identify where these risks are being controlled in the current set up. Identify all the gaps and inadequacies in the current security set up and present it to the management with cost benefit analysis.

| No. | Threat / Risk | Priority | Policy | Procedure | Firewall | IDS | Antivirus |
|---|---|---|---|---|---|---|---|
| 1 | Unauthorized access to application and internal networks. | H | ✔ | ✔ | ✔ | | |
| 2 | Data integrity | H | | | | | |
| 3 | Viruses and macro bombs. | H | | | | | ✔ |
| 4 | Unauthorized transmission of confidential information. | H | | | | | |
| 5 | Spoofing | H | | | | ✔ | |
| 6 | Denial of service attacks | H | | | ✔ | | |
| 7 | Confidentiality | H | | | | | |
| 8 | Theft of Data | H | ✔ | | | ✔ | |
| 9 | Data Corruption | H | | | | | |
| 10 | Access to inappropriate content | H | | | ✔ | ✔ | |
| 11 | Junk email. | | | | | | |
| 12 | Transmission of inappropriate information | | | | ✔ | | |
| 13 | Pornography | | | | ✔ | | |
| 14 | Sniffing | | | | ✔ | ✔ | |
| 15 | Java applets. | | | | ✔ | | |
| 16 | Java scripts. | | | | ✔ | | ✔ |
| 17 | Automatic mailing. | | | | | | |

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**Step 8: Implement Risk Mitigation strategy**

Implementation or risk mitigation strategy involves converting all the risk management plans into actions. As an outcome of the previous step you should have following items ready for implementation:

- Detailed Security Policies
- Procedures and guidelines
- New security products
- Improvements for existing devices

Detailed Security policies:

These could be addressing a number of security concerns. Typically an organization will have following policies:

Essential Policies:

Natural and Environmental Threats:
- Disaster recovery plan
- Backup and recovery plan
- Wide area network recovery plan

Human Threats
- Password Security & Controls
- Internet access and security
- Punitive Actions
- Email security

Technical controls
- Program Change Controls
- Version Controls
- Application Software Security
- Database Security
- Network & Telecommunication Security
- Operating Systems Security
- Firewall Security
- Incident Response and Management
- Data Classification
- Web server Security
- Intranet Security
- Virus Protection
- E-commerce Security
- Data encryption

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Administrative Controls

- Third Party Security
- Tele-working security

Procedures and guidelines:

Each of the above policies will be supported by appropriate procedures, instructions and guidelines based on selected standards and products. The procedures should be detailed and unambiguous enough for every person to follow.

New security products:

You would have acquired a range of new security products. Installing, configuring and integrating them with the existing security architecture will be a daunting task.

Improvements for existing devices:

Finally, you would also have acquired or downloaded new versions of software, new patches and service packs to enhance the security of your current devices.

**Project planning:** Implementing the security policies by deploying appropriate procedures and products will be major task. This needs to be done by creating teams with specific and time-bound responsibilities. This will involve coordination with the end-users of systems as well as suppliers of products. If the vulnerability assessment has indicated numerous holes in the current implementation of operating systems, relevant patches will have to be implemented after appropriate testing.

**Testing the new security measures:** Repeat all the steps described in Step 6 namely:

- Perform a vulnerability analysis
- Assign overall vulnerability ratings
- Asset/ risk evaluation
- Prepare a new current state assessment and gap analysis table

You should be able to see a substantial improvement in all the ratings as well as reduction in security gaps.

**Confirm the change in risk levels:** You will have to ensure that the risk levels have really changed due to the new security measures. Doing peer review of each team's work by another team can achieve this. You could also invite other competent individuals and groups like external consultants as well as vendors.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**Step 9: Write the Statement of Applicability**

So far we took the risk management approach for identifying and mitigating the risks. Now we should start checking our selection of controls against the127 controls defined by BS 7799. As explained, these controls are described in very general terms and no specific interpretation has been provided. There is no 'how to implement a control' defined anywhere. Entire emphasis is on selection of appropriate controls based on the risk assessment.

To identify if we have missed any of these controls, carry out the following exercise:

Mapping the implemented controls against BS7799 control objectives and controls:

Map the implemented controls against the BS 7799 controls:

Make a table of all the 127 controls and map the controls implemented by you against relevant BS 7799 control objectives and controls. One implemented control may address more than one BS 7799 control.

Identify the gaps:

If there are some gaps, find out, whether these are unintentional omissions or there are no requirements of controls. Recheck the evaluation of risks and threats performed by you. Validate the business risk analysis performed earlier.

Prepare justification for any gaps in the table. You may be able to justify a gap if the risk assessment has not shown requirement for a particular control.

Reasons for exclusion:

Explain the controls implemented and reason for exclusion, if any, in the appropriate column. Also give the risk reference, which will support your statement.

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Statement of Applicability [7]

Detailed list of all the controls that have been selected and the ones, which have not been selected, will form the 'Statement of Applicability'. Each of the statement should be backed up by risk assessment.

Format for the 'Statement of Applicability':

| Sr .No. | Clause No. | Control Objective | Control | Controls implemented and reason for exclusion if any | Risk Reference | Control Reference |
|---|---|---|---|---|---|---|
| **A.8.1 Communications and operation management** | | | | | | |
| 51 | A.8.5 | Network management | A.8.5.1 Network controls | | | |
| 52 | A.8.6 | Media handling and security | A.8.6.1 Management of removable computer media | | | |
| 53 | | | A.8.6.2 Disposal of media | | | |
| 54 | | | A.8.6.3 Information handling procedures | | | |
| 55 | | | A.8.6.4 Security of system documentation | | | |
| 56 | A.8.7 | Exchange of information and software | A.8.7.1 Information and software exchange agreements | | | |
| 57 | | | A.8.7.2 Security of media in transit | | | |
| 58 | | | A.8.7.3 Electronic commerce security | | | |
| 59 | | | A.8.7.4 Security of electronic mail | | | |
| 60 | | | A.8.7.5 Security of electronic office systems | | | |
| 61 | | | A.8.7.6 Publicly available systems | | | |
| 62 | | | A.8.7.7 Other forms of information exchange | | | |

## Step 10. Train the staff and create Security Awareness

Information security management involves each and every person who interacts with information. Broadly speaking, it will be everybody who ever touches the keyboard or mouse. Each person has capability of sabotaging the information security through ignorance, or with malicious intent. Training should explain each individual's role in maintaining the information security and his/her responsibilities towards every information asset that they handle. Training each person on information security is similar to training the entire organization about fire prevention measures. Training should be comprehensive and adequate to ensure that each person clearly understands the security policies of the


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

organization, various security risks and threats and finally consequences of not abiding by the security procedures.

Following steps should be taken:

Design security training programs:

These programs should be designed for all levels. Broadly these will be:

- Top management Security Awareness program
- End user Security Awareness program
- IT Department Security Management program

The training programs should be relevant to the organization's security requirements, and as such, should be based on the security policy and risk assessment performed for the organization.

Annual calendar:

You may have to prepare an annual schedule for these programs and ensure that all the users are trained.

Creating Security awareness:

To ensure that information security measures do not become routine stuff and get ignored, create slogans, posters, newsletters and competitions to keep the interest in security topics alive.

Also, give publicity to relevant security incidents. There will be increased awareness if the hypothetical threats really materialized.

**Step 11. Monitor and Review the ISMS performance**

Implementation of information security management system is not a one-time job. It needs to be constantly monitored and reviewed.

Create the following mechanism for effectively monitoring and reviewing the ISMS performance:

Reporting system [2]

BS 7799 has defined a specific control objective: A.6.3 Responding to security incidents and malfunctions. This involve the following measures:

- Reporting security incidents
- Reporting security weaknesses


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Reporting software malfunctions
- Operator logs
- Fault logs

Each of these controls will generate huge amount of information. Ensure that this information is properly recorded and stored for any analysis

Review mechanism

The incident reports will be of no use if they are not reviewed regularly. The formation of security organization should include assigning specific responsibilities to teams or individuals to periodically review the logs and reports.

Internal Audit

Periodic audit should be performed to review the performance of various controls and measures defined in ISMS. Internal audit teams or external consultants could perform the audit. The audit findings should be documented and all non-conformities must be corrected and reported within a specific time frame.

Management Review

The Security Steering Committee should conduct management review of the performance of ISMS at least once a year. This review should be based on various reports submitted by incident reporting and review processes and internal audit reports.

**Step 12. Maintain the ISMS and ensure continual Improvement**

Implementing ISMS will not ensure sudden improvement in information security stance of the organization. It provides an opportunity to monitor the security in an organized manner and ensure continual improvement. You could ensure that the continual improvement actually takes place by having the following measures in place:

Management review and follow-up

Management review should ensure that appropriate actions are taken on various security lapses reported through the following mechanisms:

- Incident response reports
- Internal audit reports
- External audit reports
- Learning from incidents
- Disciplinary process


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Each such report and the actions taken to improve the security should be followed up in subsequent meetings till a measurable improvement is shown.

New business requirements

New business requirements will require deployment of new and untested technologies. These could expose the information systems to new threats. In such cases, a fresh risk assessment may be necessary before making changes to ISMS.

Identification of new threats

New threats may be identified in existing implementations. Constant watch should be kept on the reports posted by security agencies like CERT/CC. [13] Periodic risk assessment should be done to evaluate the impact of new threats on the existing security implementation.

**Appointment of an external auditor:** [7]

Once you are satisfied that the ISMS is working effectively and you are achieving continual improvement, you could select a certifying agency who would audit your ISMS implementation and recommend you for BS 7799 certification. An external auditor will typically perform the audit in following steps:

Pre-assessment:

This is an optional service, which you may take if you want a desk review to be done for all your documentation. The auditor will check all the documents including the security policies prepared and maintained by you, for thoroughness and completeness and give suggestions for improvements.

Initial audit:

During the initial audit, the auditors could check any aspect of your ISMS implementation. They could check how the controls have been decided, i.e. evaluating your risk assessment methodology, how the controls have been implemented and how these are being maintained. The auditors may test a few controls at random. They may interview a few end-users to check their understanding of the security. They may review the business continuity plan and how often it is being tested and revised. Statement of applicability will be analyzed and your approach will be verified. You should also be ready with all the minutes of various review meetings, including the Security Steering committee minutes.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Based on a thorough audit, auditors will give their observations in the form of 'non-conformities' that they may have noticed in the implementation of ISMS. You will be given a fixed time frame within which all the non-conformities should be rectified.

Final Audit:

This audit will review the state of non-conformities. In addition, auditors may randomly check any areas for compliance with the ISMS. In case there are no further non-conformities, the auditors will recommend your company for BS 7799 certification.

Periodic Audits:

BS 7799 certificate is valid for 3 years, but at least once a year, you have to invite the external auditors to perform the audit and satisfy themselves that your ISMS implementation is showing continual improvement in the security performance of the organization.

## ISMS Documentation

It is essential to document the entire Information Security Management Process. This is to maintain documentary evidence of the efforts, trace-ability of all the actions, and finally, to face the initial certification audit as well as periodic audits necessary to maintain the certificate.

BS 7799 follows the PDCA (Plan, Do, Check, Act) cycle. The step-by-step methodology suggested above fits in this approach. The table below shows the documents generated at each step. As per the BS 7799 requirments, these documents need to be periodically reviewed and kept up-to-date.

© SANS Institute 2003, Author retains full rights



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**Summary table for input / process / output for BS 7799 implementation**

| | Step No. | Input | Process | Output Documents |
|---|---|---|---|---|
| **P L A N** | 1. | Business objectives, Business processes, IT Protection requirements | Establish the importance of information security in business | Business risk analysis, List of IT processes in the order of criticality |
| | 2 | List of critical IT processes, Logical and physical layout diagrams | Define the scope for ISMS | ISMS scope definition document |
| | 3 | Business risk analysis | Define the Security Policy | Security Policy |
| | 4. | Security policy | Establish the security organization structure | Security Organization chart, Security roles and responsibilities |
| | 5 | Asset inventories, value, owners, sensitivity | Identify and classify assets | Information asset lists, Classification criterion, Classification of Assets |
| | 6. | Threat and vulnerability analysis | Identify and assess the risks | Risk assessment report, Vulnerability ratings, Asset risk evaluation |
| | 7. | Risk management strategy | Plan for risk management | Risk treatment plan, detailed security policies, procedures, standards, product selection, cost benefit analysis, current state assessment report |
| **D O** | 8. | Detailed security policies, procedures, products, patches | Implement risk mitigation strategy | Project plan for risk mitigation, testing reports, review of risk reduction, updated current state analysis report |
| | 9. | Current state analysis report, mapping the implemented controls with BS 7799 controls | Write the statement of applicability | Statement of Applicability |


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

| | | | | |
|---|---|---|---|---|
| | 10. | Security policies and procedures, new product operating procedures | Train the staff and create Security Awareness | Security Training for top management, end users and IT staff, Training records |
| **CHECK** | 11. | Various incident analysis reports, software malfunction reports, operators logs, fault logs, Internal audit reports, external audit reports | Monitor and review the ISMS performance | Security reviews reports, minutes of security steering committee, action plans for improvement |
| **ACT** | 12. | Security review reports and action plans | Maintain and review ISMS for continual improvement | Continual improvement of security, reduction in incidents |

© SANS Institute 2003, Author retains full rights



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## Implementation Schedule for BS 7799 [7]

Total time required by an organization will depend on the size of the organization as well as scope of ISMS. Following timetable may be suitable for a medium to large organization with multiple locations.

The BS7799 auditors will expect the organizations to have gone through at-least two cycles of Security Review and Improvements (Step 11 and Step 12) before performing the initial audit. The final audit will be after the closure of all the non-conformities observed during the initial audits. Initial audit to final audit time frame could be two to three months.

| | | IMPLEMENTATION TIMETABLE FOR BS7799 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | BS 7799 Activity | | | | | | | | | |
| Step 1 | Business Risk Analysis | ■ | | | | | | | | |
| Step 2 | Scope of ISMS | | ■ | | | | | | | |
| Step 3 | Security Policy | | | ■ | | | | | | |
| Step 4 | Security Organization | | | ■ | | | | | | |
| Step 5 | Asset Id & Classification | | | | ▨ | | | | | |
| Step 6 | Risk Assessment Report | | | | ▨ | | | | | |
| Step 7 | Risk Treatment Plan | | | | ▨ | | | | | |
| Step 8 | Risk Mitigation | | | | | ▨ | | | | |
| Step 9 | Statement of Applicability | | | | | ▨ | | | | |
| Step 10 | Security Training | | | | | | ▨ | | | |
| Step 11 | Security Review | | | | | | ■ | | ■ | |
| Step 12 | Security Improvements | | | | | | | ▨ | | ▨ |
| | | Month 1 | Month 2 | Month 3 | Month 4 | Month 5 | Month 6 | Month 7 | Month 8 | Month 9 |

| Legend | |
|---|---|
| One team | ■ |
| | |
| Multiple teams | ▨ |

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**References:**


1. BS ISO/IEC 17799 : 2000 Information technology - Code of practice for information security management,

http://emea.bsi-global.com/InformationSecurity/Overview/index.xalter

2. BS 7799-2: 2002: Information security management - Specification for information security management systems

http://emea.bsi-global.com/InformationSecurity/Overview/index.xalter

In order to buy a copy of the standards, please contact BSI Customer Services by telephone at (+44) 20 8996 9001 or go to:

http://www.bspsl.co.uk/17799/ or http://bsonline.techindex.co.uk/

3. Bundesamt für Sicherheit in der Informationstechnik (Federal Agency for Security in Information Technology, Germany), IT Baseline Protection Manual, 2.2 Assessment of protection requirement for IT applications

http://www.bsi.de/gshb/english/menue.htm

4. Information Systems Management Systems, International Users Group, International Register of BS 7799 Accredited Certificate,

http://www.xisec.com/Register.htm

5. Information Systems Management Systems, International Users Group, ISMS Scopes,

http://www.xisec.com/registerISMSscope.htm

6. Canadian Communications Security Establishment, "Threat and Risk Assessment Working Guide", October 1999, http://www.cse-cst.gc.ca/en/documents/knowledge_centre/publications/manuals/ITSG-04e.pdf

7. BS 7799-2 Inception to Certification Dale Johnstone, Chair, BS7799 User Group,(Hongkong)
www.pisa.org.hk/event/bs7799-2.pdf

8. Get Certified! - Protect your enterprise through audit and certification. by David Chin , Network Magazine India, Dec. 2002

http://www.networkmagazineindia.com/200212/focus1.shtml




© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

9. How 7799 Works, Gamma Secure Systems Ltd. UK,

http://www.gammassl.co.uk/bs7799/works.html

10. Creating, implementing and managing the information security life cycle, Internet Security Systems

http://downloads.securityfocus.com/library/securityCycle.pdf

11. Measuring Information Security, A. Martins

http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Martins.pdf

12. Open source security testing methodology manual, OSSTMM Ver. 2.0 Pete Herzog, Institute for Security and Open Methodology (ISECOM)

http://www.isecom.org/projects/osstmm.htm

13. Security threats, vulnerabilities, incidents and fixes, CERT Coordination Center, http://www.cert.org/nav/index_red.html

14. BS 7799 Compliance & BS7799 Management Using the Cobra Method http://www.securitypolicy.co.uk/bs-7799/

15. Risk Assessment Tool CRAMM Ver.5.0, Insight Consulting, http://www.insight.co.uk/cramm/

16. RFC 2196, Site Security Handbook, A Guide to develop computer security policies and procedures for sites that have systems on internet

http://www.ietf.org/rfc/rfc2196.txt?number=2196

17. The SANS Security Policy Project

http://www.sans.org/resources/policies/

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.