

Quality Group Practice Guides

Information Security Guidelines

Abstract

The purpose of information security is to ensure business continuity and reduce business damage by preventing and minimising the impact of security incidents. The purpose of this section is to introduce the concept of developing an Information Security Management System (ISMS) as defined in BS 7799, that will reflect the organization's approach to risk management, the control objectives and controls, and the degree of assurance required. The aim is that the ISMS should be effective and efficient undertaking only the necessary tasks in a manner appropriate for the organization while avoiding over control and waste of valuable resources.

Introduction

Information security is first and foremost a management issue: the best technical security is worthless without a management commitment to adopting and enforcing a security policy which ensures that people understand the role they play. An up-to-date security policy demonstrates that management is serious about security and provides a framework within which to operate as well as a benchmark against which the security practices can be measured. The purpose of information security is to ensure business continuity and reduce business damage by preventing and minimising the impact of security incidents.

This document should be read in conjunction with the following Quality Group Practice Guides:-

- Risk Management

Scope

The purpose of this section is to introduce the concept of developing an Information Security Management System (ISMS) as defined in BS 7799, that will reflect the organization's approach to risk management, the control objectives and controls, and the degree of assurance required. The aim is that the ISMS should be effective and efficient, undertaking only the necessary tasks in a manner appropriate for the organization while avoiding over control and waste of valuable resources.

Glossary of Terms

<i>Information Security</i>	The security, preservation of confidentiality, integrity and availability of information:- <ul style="list-style-type: none">• Availability - ensuring that authorised users have access to information and associated assets when required;• Confidentiality - ensuring that information is accessible only to those authorized to have access;• Integrity - safeguarding the accuracy and completeness of information and processing methods.
<i>Information Security Management System (ISMS)</i>	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security NOTE The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.
<i>Risk Assessment</i>	The overall process of risk analysis and risk evaluation.
<i>Risk Evaluation</i>	The process of comparing the estimated risk against given risk criteria to determine the significance of risk.
<i>Risk Management</i>	The coordinated activities to direct and control an organization with regard to risk.
<i>Risk Treatment</i>	The treatment process of selection and implementation of measures to modify risk.

Process Description

Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately identified and protected.

Security requirements should be identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. Risk assessment techniques can be applied to the whole organization, or only parts of it, as well as to individual information systems, specific system components or services where this is practicable, realistic and helpful. The results of this assessment will help guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks. The process of assessing risks and

selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems. It is also important that the organization regularly reviews their risk assessments to constantly monitor changing environments and levels of risk.

The organization should develop, implement, maintain and continually improve a documented Information Security Management System within the context of the organization's overall business activities and risk.

BS 7799-2:2002 provides a process approach that encourages its users to emphasize the importance of:-

- Understanding business information security requirements;
- Implementing and operating controls in the context of managing an organization's overall business risk;
- Monitoring and reviewing the performance and effectiveness of the ISMS;
- Continual improvement based on objective measurement.

Process

The model, known as the "Plan-Do-Check-Act" (PDCA) model, can be applied to all ISMS processes.

PLAN - To establish an ISMS it is necessary to:-

- Define the scope of the ISMS;
- Define an ISMS policy;
- Define a systematic approach to risk assessment;
- Identify the risks;
- Assess the risks;
- Identify and evaluate options for the treatment of risks;
- Select control objectives and controls for the treatment of risks;
- Prepare a Statement of Applicability;
- Obtain management approval of the proposed residual risks and authorization; to implement and operate the ISMS.

DO - To implement and operate the ISMS it is necessary to:-

- Formulate and implement a risk treatment plan;
- Implement controls selected to meet the control objectives;
- Implement training and awareness programmes;
- Manage operations;
- Manage resources;
- Implement procedures to enable prompt detection and response to security incidents.

CHECK - To Monitor and review the ISMS it is necessary to:-

- Execute monitoring procedures to detect errors in the results of processing promptly; identify failed and successful security breaches and incidents promptly; enable management to determine whether the security activities are performing as expected;
- Determine the actions taken to resolve a breach of security;
- Undertake regular reviews of the effectiveness of the ISMS;
- Review the level of residual risk and acceptable risk;
- Conduct internal ISMS audits at planned intervals;
- Undertake a management review of the ISMS on a regular basis;
- Record actions and events that could impact on the effectiveness or performance of the ISMS.

ACT - To Maintain and improve the ISMS it is necessary to:-

- Implement identified improvements in the ISMS;
- Take appropriate corrective and preventive actions;
- Communicate results and actions;
- Ensure that the improvements achieve their intended objectives.

Metrics and Checklists

The overall objective is to check over a specified regular audit period using internal ISMS audit that all aspects of the ISMS are functioning as intended. A sufficient number of audits should be conducted to enable management to ensure that there is evidence that confirms that:-

- The information security policy is still appropriate;
- An appropriate risk assessment methodology is being used;
- The documented procedures are being followed;
- Technical controls (e.g. Firewalls, physical access controls) are in place and correctly configured;
- The residual risks are still acceptable to the management of the organization;
- Actions from previous audits and reviews have been implemented and are seen to be effective;
- The ISMS is compliant with BS 7799-2.

Further Reading

1. BS EN ISO 9001:2000, Quality management systems - Requirements.
2. BS ISO/IEC 17799:2000, Information technology - Code of practice for information security management.
3. BS 7799-2: 2002 Information security management systems - Specification with guidance for use
4. ISO Guide 73:2002, Risk management - Vocabulary - Guidelines for use in standards.
5. Preparing for BS 7799 Certification (PD 3001)
6. Guide to BS 7799 Risk Assessment and Risk Management (PD 3002)
7. Are you ready for a BS 7799 Audit? (PD 3003)
8. Guide to BS 7799 Auditing (PD 3004)
9. Guide on the selection of BS 7799 controls (PD 3005)
10. BS ISO/IEC TR 13335 Guidelines for the management of IT Security (GMITS)
Part 1: Concepts and Models for IT Security (GMITS)
11. Part 2: Managing and Planning IT Security (GMITS)
12. Part 3: Techniques for the Management of IT Security (GMITS)
13. Part 4: Selection of Safeguards (GMITS)
14. Part 5: Safeguards for External Connections (GMITS)