Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001
Information Security Management Systems Guidance series

The Information Security Management Systems (ISMS) series of books are designed to provide users with assistance on establishing, implementing, maintaining, checking and auditing their ISMS in order to prepare for certification. Titles in this Information Security Management Systems Guidance Series include:

- Guidelines on requirements and preparation for ISMS certification based on ISO/IEC 27001 (ref.: BIP 0071)
- Are you ready for an ISMS audit based on ISO/IEC 27001? (ref.: BIP 0072)
- Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001 (ref.: BIP 0073)
- Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001 (ref.: BIP 0074)
Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001

Ted Humphreys and Angelika Plate
Contents

Introduction ix

1 General 1
   1.1 Scope 1
   1.2 Definitions 1
   1.3 Related documents 1

2 About metrics and measurements 3
   2.1 What are metrics, measures and measurements? 3
   2.2 Why are measurements necessary? 4
      2.2.1 General reasons and benefits 4
      2.2.2 Requirements in ISO/IEC 27001 5
      2.2.3 PLAN, DO, CHECK and ACT (PDCA) Model 5
      2.2.4 Other benefits of using metrics 6

3 Classes of ISMS metrics and measurements 9
   3.1 Introduction 9
   3.2 Management controls 9
      3.2.1 Introduction 9
      3.2.2 Examples 9
   3.3 Business processes 11
      3.3.1 Introduction 11
      3.3.2 Examples 11
   3.4 Operational controls 12
      3.4.1 Introduction 12
      3.4.2 Examples 12
   3.5 Technical controls 14
      3.5.1 Introduction 14
      3.5.2 Examples 14
   3.6 Audits, reviews and testing 17
      3.6.1 Introduction 17
      3.6.2 Examples 17

4 Example methods and approaches 19
   4.1 Management controls 19
      4.1.1 Compliance with best practice 19
5.4 ACT phase

5.4.1 Implementing corrective and preventive actions

5.4.2 Adjusting the metric and measures

5.4.3 Improvements in the metrics and measurement scheme
Introduction

Information is one of your organization’s most valuable assets. The objectives of information security are to protect the confidentiality, integrity and availability of information. These basic elements of information security help to ensure that an organization can protect against:

- sensitive or confidential information being given away, leaked or disclosed both accidentally or in an unauthorized way;
- critical information being accidentally or intentionally modified without your knowledge;
- any important business information being lost without trace or hope of recovery;
- any important business information being rendered unavailable when needed.

It should be the responsibility of all managers, information system owners or custodians and users in general to ensure that their information is properly managed and protected from a variety of risks and threats faced by every organization. The two standards ISO/IEC 17799:2005,1 Code of practice for information security management and ISO/IEC 27001:2005 (revised version of BS 7799 Part 2:20022) Information security management systems — Requirements together provide a basis for organizations to develop an effective information security management framework for managing and protecting their important business assets whilst minimizing their risks, maximizing the investments and business opportunities of the organization and ensuring their information systems continue to be available and operational.

The standard ISO/IEC 17799:2005 provides a comprehensive set of best practice for information security, which organizations can adopt and implement to address the risks that they face using the risk management approach specified in the standard ISO/IEC 27001:2005. In addition, ISO/IEC 27001:2005 is the base requirements standard for accredited third-party ISMS (information security management system) certification3 based on this risk management approach. Organizations applying these standards, especially those going through the accredited certification route to obtain an ISMS certificate, will need mechanisms in place to enable them to determine the effectiveness of the overall ISMS as well as of the controls that have been implemented to reduce the identified risks.

---

1 This is the revised version of ISO/IEC 17799:2000, which was previously BS 7799-1:1999.
2 With the publication of ISO/IEC 27001:2005, the current version of BS 7799 Part 2 will be withdrawn and will no longer be a valid standard for third-party accredited certification. Any such certification work will be carried out against the requirements specified in ISO/IEC 27001:2005. Accreditation Bodies are responsible for issuing (see 4.2.1 of this guide) a ‘Transition Statement’ that provides details of the period during which organization’s and Certification Bodies (see 4.2.1 of this guide) involved in the ISMS certification process need to make the transition from BS 7799-2:2002 to ISO/IEC 27001:2005.
3 The accredited certification process also employs the accreditation and certification guides and standards ISO Guide 62/EN 45012 and EA 7/03.
Measuring the effectiveness of your ISMS implementations

This guide and the other guides in the BIP 0070 series are designed to provide users with assistance in establishing, implementing and maintaining their ISMS to help them in preparing for ISMS certification. This guide concentrates on describing the different methods and metrics that can be applied to measure the effectiveness and success of the ISMS processes and controls in place.

Note: A document such as this is provided with the best of intentions. It reflects common practice, which is derived by a consensus among those with a wide variety of skills, knowledge and experience in the subject. This guide makes no claim to be exhaustive or definitive and users of this guide may need to seek further guidance in implementing the requirements of ISO/IEC 27001:2005. Furthermore, there will always be other aspects where additional guidance is required relevant to the organizational, operational, legal and environmental context of the business, including specific threats, controls, regulatory compliance, governance and good practice.

It has been assumed in the drafting of this BSI guide that the execution of its advice is entrusted to appropriately qualified and experienced people.
1 General

1.1 Scope

This guide provides information and help on measuring the effectiveness of ISMS implementations, as required by the ISMS standard, ISO/IEC 27001:2005. This guide refers to two different types of measurement: one for the ISMS processes that are described in clauses 4–8 of ISO/IEC 27001:2005 and other forms of measurements for the controls from ISO/IEC 17799:2005 that have been selected to reduce identified risks. This guide introduces an approach to measuring the ISMS processes and controls that is aligned with the currently used methods and developments to support organizations in identifying the appropriate selection of metrics and measurement techniques. This guide also gives some examples of metrics and measurements by leading organizations and interest groups in the field of information security.

This document is one of a set of four guides published by BSI to support the use and application of ISO/IEC 17799:2005 and ISO/IEC 27001:2005. The reader may find it of benefit to have copies of the three other guides:

- BIP 0071 – Guidelines on requirements and preparation for ISMS certification based on ISO/IEC 27001;
- BIP 0072 – Are you ready for an ISMS audit based on ISO/IEC 27001?
- BIP 0073 – Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001.

1.2 Definitions


1.3 Related documents

This guide makes reference to the following standards and guidelines:

a) ISO/IEC 17799:2005 (revised version of ISO/IEC 17799:2000), Code of practice for information security management – the standard that identifies control objectives and controls and provides best practice advice for the implementation of these controls;

b) ISO/IEC 27001:2005 (the ISO revised version of BS 7799-2:2002), Information security management systems — Requirements – this is the requirements specification for an ISMS. This standard is used as the basis for accredited certification;