

BS 7799-3:2017



BSI Standards Publication

Information security management systems

Part 3: Guidelines for information security risk management
(revision of BS ISO/IEC 27005:2011)



Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2017

Published by BSI Standards Limited 2017

ISBN 978 0 580 97052 8

ICS 03.100.70 | 35.020 | 35.030

The following BSI references relate to the work on this document:

Committee reference IST/33

Draft for comment 17/30354571 DC

Amendments/corrigenda issued since publication

Date	Text affected

Contents

	Page
Foreword	ii
Introduction	1
1 Scope	1
2 Normative references	2
3 Terms and definitions	2
4 Overview of information security risk assessment and risk treatment	2
<i>Figure 1 — The information security risk assessment and risk treatment processes of BS EN ISO/IEC 27001</i>	3
5 Communication and consultation	3
6 Context establishment	4
<i>Table 1 — Example logarithmic likelihood scale</i>	8
<i>Table 2 — Example logarithmic consequence scale</i>	8
<i>Table 3 — Example indicator scales</i>	9
7 Risk identification and analysis	11
<i>Table 4 — Example scenarios that give coverage of the controls in BS EN ISO/IEC 27001:2017, Annex A</i>	13
8 Information security risk treatment	16
9 Verification of necessary controls	21
<i>Figure 2 — The cross-checking process</i>	22
<i>Figure 3 — The cross-checking process following rework</i>	23
10 Approval	24
11 Operation	24
12 Monitoring, audit and review	25
13 Documented information	27
Annex A (informative) Correspondence between BS 7799-3:2006 and BS 7799-3:2017	29
<i>Table A.1 — Correspondence between BS 7799-3:2006 and BS 7799-3:2017</i>	30
Bibliography	31

Summary of pages

This document comprises a front cover, and inside front cover, pages i to iv, pages 1 to 31, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 October 2017. It was prepared by Technical Committee IST/33, *IT – Security Techniques*. A list of organizations represented on this committee can be obtained on request to its secretary.

Supersession

This British Standard supersedes BS 7799-3:2006 and BS ISO/IEC 27005:2011, which are withdrawn.

Relationship with other publications

BS 7799-3:2006 was produced as a British Standard to provide guidance and advice to support the implementation of the BS ISO/IEC 27001:2005 requirements that related to risk management processes and associated activities. It was withdrawn following the publication of BS ISO/IEC 27005:2008, which effectively fulfilled the same needs, thereby rendering BS 7799-3 redundant. BS ISO/IEC 27005 was revised in 2011 to align it with the vocabulary and concepts embodied in BS ISO 31000.

However, BS ISO/IEC 27005:2011 is not aligned with the requirements of BS EN ISO/IEC 27001:2017 and a revised version of BS ISO/IEC 27005 is still under discussion within ISO/IEC. A new version is not expected in the foreseeable future.

Given this situation, and with the ever-growing user demand for risk management guidance, BS 7799-3 has been updated to align with the requirements of BS EN ISO/IEC 27001:2017 and republished as BS 7799-3:2017 to fill the market gap.

Information about this document

This is a full revision of the standard, and introduces the following principal changes:

- guidance on using the event-consequence approach as well as the asset-threat-vulnerability approach to risk assessment; and
- an explanation of the new requirements for dealing with BS EN ISO/IEC 27001:2017, Annex A controls.

Use of this document

As a guide, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of The Shorter Oxford English Dictionary is used (e.g. “organization” rather than “organisation”).

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Introduction

This British Standard is intended to assist organizations in addressing the risks and opportunities highlighted by the requirements of BS EN ISO/IEC 27001:2017, principally **6.1** and **Clause 8** of that document.

This British Standard is intended to be considered, interpreted and adapted to suit each organization's specific situation. The concepts and approaches are intended to be broadly applicable, but the particular method that any particular organization requires depend on contextual factors (such as its size, sector, maturity, information security risks, compliance obligations and management style) that vary widely in practice.

This British Standard contains the description of the information security assessment and the risk treatment process and its activities.

A general overview of the information security risk assessment and risk treatment processes is given in [Clause 4](#).

The remainder of this standard is structured as follows:

- communication and consultation in [Clause 5](#);
- context establishment in [Clause 6](#);
- risk identification and analysis in [Clause 7](#);
- information security risk treatment in [Clause 8](#);
- verification of necessary controls in [Clause 9](#);
- approval in [Clause 10](#);
- operation in [Clause 11](#);
- monitoring, audit and review in [Clause 12](#); and
- documented information in [Clause 13](#).

There is a table showing the relationship between this document and the previous edition, BS 7799-3:2006, in [Annex A](#).

1 Scope

This British Standard provides guidance to assist organizations to:

- a) fulfil the requirements of BS EN ISO/IEC 27001 concerning risks and opportunities; and
- b) define, apply, maintain and evaluate risk management processes in the information security context.

This British Standard is relevant to:

- 1) organizations who have or are intending to have an information security management system (ISMS) that conforms to BS EN ISO/IEC 27001; and
- 2) persons that perform or are involved in information security risk management (e.g. interested parties, risk owners and ISMS professionals).

This document is applicable to all organizations, regardless of type, size or nature.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes provisions of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN ISO/IEC 27001:2017, *Information technology — Security techniques — Information security management system — Requirements*

3 Terms and definitions

For the purposes of this part of BS 7799, the terms and definitions given in BS EN ISO/IEC 27000:2017 apply.

4 Overview of information security risk assessment and risk treatment

BS EN ISO/IEC 27001 is not only a management system standard, it is also an information security risk management standard. This is because the primary tools it uses for information security management are risk assessment and risk treatment.

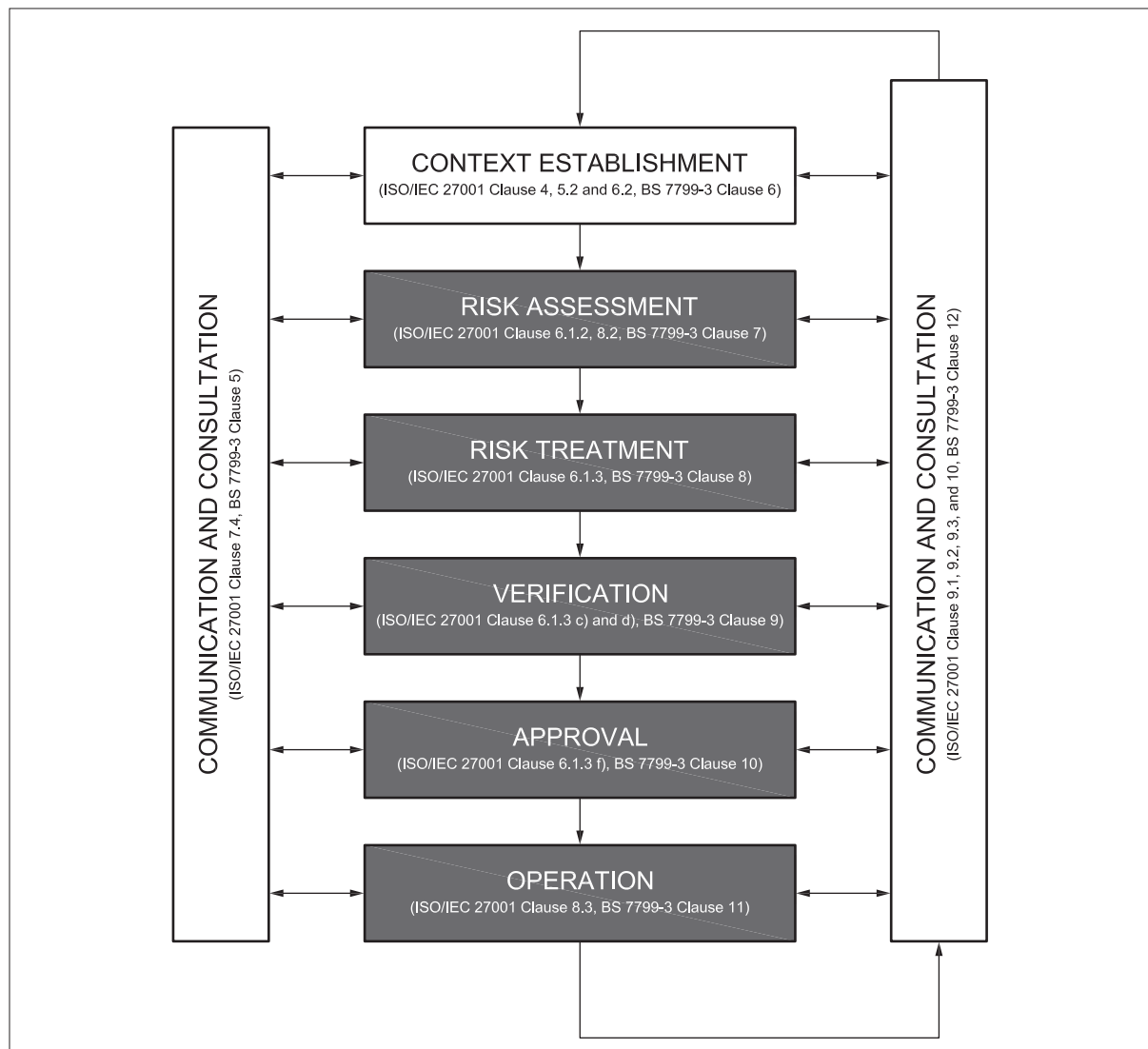
Organizations have objectives, and in exploiting the opportunities that they create or seize to meet those objectives, they can encounter risks which need to be managed for the objectives to be successfully realized. Some of those risks are information security risks and therefore come within the scope of BS EN ISO/IEC 27001:2017.

The BS EN ISO/IEC 27001 requirements concerning actions to address risks and opportunities fall into two groups:

- a) those in **6.1.1** and **8.1** of that document are common to all management system standards published since 2012; and
- b) those in **6.1.2**, **6.1.3**, **8.2** and **8.3** of that document are specific to information security risk.

There is nothing incompatible with these two sets of requirements. **6.1.2** and **6.1.3** can be regarded as the way to fulfil the requirements of **6.1.1** in the context of information security risk (and likewise a similar relationship exists between **8.2/8.3** and **8.1**).

Having established the context of the organization (see BS EN ISO/IEC 27001:2017, **4.1**) and the requirements of interested parties (such as the risk owners), the organization should perform a risk assessment to identify the risks and determine their likelihood of occurrence and potential consequences (see [Figure 1](#)). The organization should then use risk acceptance criteria to determine the acceptability of these risks. If the criteria are not met, a process of risk treatment is used to determine the controls necessary to modify the risks so that the criteria are met. In the case of information security controls, the organization compares these necessary controls with those in BS EN ISO/IEC 27001:2017, Annex A to see if any necessary controls have been inadvertently omitted. If it has, the proceeding activities should be reworked until the verification check succeeds. The risk owners then approve the risk treatment plans and any residual risk and the risk treatment plans can then be put into operation.

Figure 1 — The information security risk assessment and risk treatment processes of BS EN ISO/IEC 27001

5 Communication and consultation

BS EN ISO/IEC 27001:2017, **6.1.3 f)** requires the risk owners to approve the risk treatment plans and the residual risk. Communication and consultation with the risk owners is therefore an important activity. The purpose is to achieve agreement on how to manage risks by exchanging and/or sharing information about risk with the risk owners, and perhaps other interested parties and decision-makers. The information includes, but is not limited to, the existence, nature, form, likelihood, severity, treatment and acceptability of risks. Communication and consultation should be bi-directional.

BS EN ISO/IEC 27001:2017, **6.1.2 c) 2)** requires that risk owners are identified and that the risk owners approve the related risk treatment plan(s) and accept the residual risks. Some organizations might already have a formal risk registration process that identifies who owns what risks. In other organizations, this might not exist. Risk ownership could even be deliberately confused or concealed. Even when risk owners can be identified, they might be reluctant to acknowledge that they are responsible for the risks that they own, and obtaining their participation in the risk management process could be difficult. Unfortunately risk management is impossible unless ownership of risk is identified, acknowledged, accepted and communicated.

Perceptions of risk can vary due to differences in assumptions, concepts, needs, issues and concerns of interested parties as they relate to risk or the issues under discussion. Risk owners are likely to make judgments on the acceptability of risk based on their perception of risk, as well as their perceptions of benefits.

Depending on the nature and sensitivity of the risk(s) there might be a need to limit some information about risks, their assessment and treatment on a need-to-know basis to those responsible for identifying, assessing and treating them. Limiting the communication about specific risks should be on an appropriate and proportionate basis, in consultation with the risk owners or potential owners, with the aim of avoiding publicizing the more sensitive risks and their associated vulnerabilities.

6 Context establishment

6.1 Organizational context

An organization should gather information concerning the external and internal issues and the organization's interested parties and their requirements (see BS EN ISO/IEC 27001:2017, **4.1** and **4.2**), before any attempt is made by the organization to assess its information security risks, or indeed any other risks that could affect the intended outcome of the ISMS (see BS EN ISO/IEC 27001:2017, **6.1.1**). It should be borne in mind that the information security policy (see BS EN ISO/IEC 27001:2017, **5.2**) can constrain risk treatment (e.g. a risk treatment option might not be permitted by that policy). Furthermore, the organization's information security objectives (see BS EN ISO/IEC 27001:2017, **6.2**) can constrain the risk acceptance criteria (e.g. the acceptable level of risk can be a function of the potential rewards associated with different business activities).

Organizations should aim to understand their organizational context (i.e. the circumstances in which the organization operates) in sufficient detail to be able to reliably identify risks. How this is done depends on the organization's choice of risk identification and analysis method. With the event-consequence method, the organization should work to understand the normal and abnormal work flows that it might encounter internally and when interacting with the rest of the world (i.e. all external organizations and risk sources within scope of the ISMS). With the asset-threat-vulnerability method, the organization should aim to understand the threats that it is exposed to and the vulnerabilities in its interfaces to the rest of the world.

BS EN ISO/IEC 27001:2017, **6.1.3 c)** provides a safety net by requiring organizations to compare the controls that they determine as being necessary to mitigate their information security risks with those in BS EN ISO/IEC 27001:2017, Annex A, so that it is possible for an organization to identify and repair defects in its understanding of its context. If any Annex A controls or equivalents are missing, the organization should check that those controls are truly not applicable in its organizational context.

6.2 Risks and opportunities

An organization should identify or create opportunities and exploit them to meet its objectives. An example could be the use of internet technology to sell the organization's products. The objective is the sale of the organization's products for profit. The opportunity is the availability of suitable internet technology, and the method of exploitation is the use of that technology, e.g. by creating and deploying an e-commerce website. Such an "opportunity exploitation plan" is not without risk. For example, inadequate software development controls could lead to vulnerabilities in the website which could allow customer data to be stolen. This is an information security risk (see **6.3**). Poor layout could make the website difficult to use and put customers off buying. Likewise, if the prices were uncompetitive, products might not be sold. These, however, are not information security risks

and do not relate to the intended outcomes of an ISMS. Such risks are therefore outside the scope of an ISMS, but should still be treated by top management as a business risk.

Failure to identify information security risks, failure to treat them properly or to implement the risk treatment plan (perhaps though lack of adequate resources) are risks that affect the intended outcome of the ISMS. They are not information security risks, although they could expose the organization to unnecessary information security risk.

6.3 Scope of information security risk assessment and risk treatment

The scope and boundaries of the information security risk assessment and risk treatment are directly related to the scope of the ISMS as determined by BS EN ISO/IEC 27001:2017, 4.3.

If there is anything within the scope of the information security risk assessment that is outside the scope of the ISMS, then either that something should be excluded from the risk assessment, or the scope of the ISMS should be expanded to include it. This can happen if a risk source has been identified as a result of the risk identification process that was not known about when the scope of the ISMS was defined.

The scope of an information security risk assessment can be a subset of the scope of the ISMS if the organization performs multiple risk assessments, e.g. to facilitate the assignment of risk ownership responsibilities to different organizational entities, to address groups of risks. However, in this case, care should be taken to ensure that the combined scopes of all such risk assessments exactly equals the scope of the ISMS in accordance with BS EN ISO/IEC 27001:2017, 6.1.2 c) 1).

The (combined) scope of the risk assessment should enable the identification of risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS.

6.4 Defining risk criteria

6.4.1 General

BS EN ISO/IEC 27001:2017, 6.1.2 a) requires organizations to define their risk criteria, i.e. the terms of reference by which they evaluate the significance of the risks that they identify. BS EN ISO/IEC 27001 specifically requires an organization to define the criteria that it intends to use to:

- a) determine the acceptability of a risk; and
- b) when risk assessments are to be performed.

6.4.2 Criteria concerning consequences

BS EN ISO/IEC 27001:2017, 6.1.2 c) refers to loss of confidentiality, integrity and availability of information within the scope of the ISMS. In deciding how it intends to judge the significance of such losses, the organization should take into account the wider consequences that might result, for example:

- a) loss of life or harm to individuals or groups;
- b) loss of freedom, dignity or right to privacy;
- c) loss of staff and intellectual capital (the information in people's heads);
- d) loss of business advantage or market share;
- e) damage to public trust;
- f) failure of the business function or organization;
- g) breaches of information security (e.g. loss of confidentiality, integrity and availability);
- h) impaired operations (internal or third parties);

- i) loss of business and financial value;
- j) disruption of plans and deadlines;
- k) damage of reputation;
- l) breaches of legal, regulatory or statutory requirements; and
- m) breaches of contracts or service levels.

It is essential that risk owners and assessors share a common understanding of the criteria and scales used to express consequence. It is therefore much better to say “up to £1M loss” rather than “significant loss”, or “downtime for up to one day” rather than “short-term downtime”.

If different scales are used, for example to distinguish effects on people from effects on business process delivery, it is prudent to be able to equate the points on one scale with those on the other. Financial loss is a commonly used means to achieve this.

In this case, the organization should estimate potential losses using criteria such as contract value, labour and material costs and fines. For example, a breach of data protection legislation can result in a substantial fine, additional work (and therefore unanticipated labour costs) and a significant loss of revenue due to customers taking their custom elsewhere. Indeed, the cost of information security breaches is often expressed in terms of monetary loss.

The consequences of a single information security event are not the same for different people or organizations. For example, the consequences of a crash of the Human Resources (HR) management server are different for the IT department hosting this server, the HR department that uses the server, and the sales department that is unaffected by it. In this case, the HR department should be recognized as the risk owner and it is that department that should approve the risk treatment plan (for that server) and any residual risk. The risk to the IT department would not be the failure of a server, so much as a failure to implement the risk treatment plan as agreed with the HR department.

6.4.3 Criteria concerning likelihood

Likelihood criteria describe how an organization intends to categorize the frequency of potential information security events, e.g. the number of potential information security events in a particular time period. Time-based (frequency) descriptions are often easier to assess and less subjective than probability-based descriptions. These criteria depend on the type of events under consideration. To be effective, the likelihood criteria should span and segregate the expected range of frequencies so that differences can be identified. The range of likelihood criteria should be capable of being applied to events that are almost inevitable as well as those that are expected to occur infrequently. Similarly, likelihood criteria depends on whether the anticipated rate of occurrence of events is widely variable or relatively predictable within a narrow range.

Likelihood criteria should be developed taking into account how likely anticipated information security events might be, which in turn depends on facts such as:

- a) the degree of motivation of a deliberate attack (e.g. the viability [cost/benefit] of such an attack);
- b) the required skill of an attacker;
- c) the tools and resources available to an attacker;
- d) influences such as serious crime, terrorist organizations or foreign intelligence;
- e) the probability of occurrence of accidental or natural events, e.g. force majeure events;
- f) the degree of exposure of relevant information or the asset related to information to an attacker;
- g) the type of opportunity that the organization gives to an attacker;
- h) technology failure; and