BS 31111:2018

BSI Standards Publication

Cyber risk and resilience – Guidance for the governing body and executive management

bsi.

Publishing and copyright information

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

Published by BSI Standards Limited 2018

ISBN 978 0 580 94482 6

ICS 75.040.01

The following BSI references relate to the work on this document:
Committee reference RM/1
Draft for comment 16/30342526 DC

Amendments/corrigenda issued since publication

Date	Text affected

Contents

Summary of pages
This document comprises a front cover, and inside front cover, pages i to ii, pages 1 to 23, 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 March 2018. It was prepared by Technical Committee RM/1, *Risk management*. A list of organizations represented on this committee can be obtained on request to its secretary.

Information about this document

This British Standard provides guidance for the governing body and executive management to manage cyber risk and resilience, and is aimed at public, private and not-for-profit organizations.

References to relevant resources are given in Annex A for the convenience of users of this standard and do not constitute an endorsement by BSI of the products/services named. Equivalent products/services may be used if they can be shown to lead to the same results.

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.

0 Introduction

0.1 General

Organizations have a changing relationship with technology, with most now dependent on its capabilities and technology becoming even more deeply embedded into the very fabric of society.

Cyberspace provides considerable opportunities for an organization to, for example, improve products and services, develop new ones, reduce operational costs and improve performance. However, these opportunities are also highly likely to create new vulnerabilities and additional threats, and can result in direct financial loss, regulatory penalty, operational disruption, intellectual property loss, safety or privacy impact, and reputational damage to the organization.

As a result, the organization needs to address technology, information and connectivity risk issues when pursuing the potential benefits presented by digital technology. To maximize these benefits, the organization needs to manage risks while simultaneously reducing any accompanying threats that arise from increased connectivity or complexity.

NOTE BS ISO 31000 provides further guidance on risk management across the organization.

Any major failure of systems can seriously damage an organization, but cyber attacks in particular can be devastating. As cyber attacks and other malicious actions are increasingly prevalent, sophisticated and targeted, the organization needs to understand and protect itself and its stakeholders against the accidental and unintended consequence of any failure or error when utilizing cyber-related solutions.

There is increased recognition of the pressing need to clearly demonstrate to stakeholders that operations and processes are effective, resilient and mature, particularly as organizations are now held accountable by regulation, legislation and society in general.

Too often, cyber risk is being managed solely by the information technology function or cyber security groups. However, the risks affect the wider organization and need to be recognized and addressed by the wider governance and risk management processes that involve other management functions across the organization. An organization's cyber risk cannot be delegated in this way, and it is the executive management that is accountable for ensuring that informed, appropriate decisions are being made which meet, or exceed, the expectations of the organization's stakeholders, including regulators, regardless of the size or sector of the organization.

0.2 Purpose and benefits of this British Standard

The guidance in this British Standard provides strategic insight on the relationships and critical factors to be incorporated in the management of risks associated with the use of all forms of information and digital technology. It helps clarify and prioritize strategic considerations for executive management by establishing a connected commercial and technical context, taking account of the level of resources available, and helps to decide which risk management strategy to adopt.

The guidance helps an organization, of any type and size, connect and understand the components essential for managing cyber risk and resilience in commercial terms. It provides an understanding of business risks associated with all cyber and information technology activities, which enables more effective decision making.

The guidance emphasizes and encourages the use of principles established by other management standards or frameworks that, together, can help develop cyber risk and resilience capabilities that align with the objectives of the organization. It helps executive management to understand the areas to focus on in order to ensure that cyber resilience is built in across all levels and functions of the organization.

The guidance supports the identification and assessment of emerging risks associated with technology development, such as artificial intelligence (AI) and the Internet of Things (IoT).

Additional good practice advice is provided to help risk managers improve the quality, value and effectiveness of their contribution by aligning cyber activity with, and including this in, their current processes and providing better risk management input to achieve good management practice.

The guidance helps executive management, risk managers and information technology professionals to demonstrate value by developing a broader understanding of the business risk and value for cyber.

This British Standard does not provide detailed technical guidance, which is already given in specific standards or frameworks, such as the ISO/IEC 27000 suite of standards and the US National Institute of Science and Technology (NIST), as well as guidance from the UK National Cyber Security Centre (NCSC). However, by connecting the commercial and technical areas that need to be addressed, the guidance supports an organization in building effective cyber risk management and resilience.

1 Scope

This British Standard provides guidance on cyber risk management and resilience for societal, regulatory, governance and behavioural risks that need to be understood, assessed, quantified, qualified and addressed, and overseen by the governing body and executive management of an organization.

This British Standard helps the governing body and executive management manage cyber risk and resilience, explaining the various approaches to making an organization cyber resilient. It is applicable to public, private and not-for-profit organizations of all sizes, and provides guidance on the essential features of cyber risk and resilience management to ensure that cyber resilience is built into decision making.

This is not a technical cyber security or risk management standard. It is intended for a non-technical audience, although some of the relevant standards with more technical content are listed in Annex A.

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 65000, *Guidance on organizational resilience*

NOTE 1 The standard also gives an informative reference to BS 65000:2014.

BS EN ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

NOTE 2 The standard also gives an informative reference to BS EN ISO/IEC 27000:2017.

BS ISO 31000, *Risk management – Principles and guidelines*

NOTE 3 The standard also gives an informative reference to BS ISO 31000:2018.

PD ISO Guide 73, *Risk management – Vocabulary*