PD ISO/TS 22318:2015

BSI Standards Publication

Societal security — Business continuity management systems — Guidelines for supply chain continuity

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/TS 22318:2015. It supersedes PD 25222:2011 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee CAR/1, Continuity and Resilience.

A list of organizations represented on this committee can be obtained on request to its secretary.

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

Published by BSI Standards Limited 2015

ISBN 978 0 580 86362 2
ICS 03.100.01

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 October 2015.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/TS 22318:2015

TECHNICAL SPECIFICATION

ISO/TS 22318

First edition
2015-09-01

Societal security — Business continuity management systems — Guidelines for supply chain continuity

Sécurité sociétale — Systèmes de management de la continuité en affaires — Lignes directrices pour la continuité de la chaîne d'approvisionnement

Reference number
ISO/TS 22318:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 292, *Security and resilience*.

Introduction

This Technical Specification expands the business continuity guidance on establishing appropriate levels of continuity management within an organization's supply chain given in ISO 22301 and ISO 22313. It assumes that the organization seeking to establish supply chain continuity management (SCCM) is aware of the principles of business continuity management and has established, or intends to implement, a business continuity management system (BCMS) broadly aligned to the established standards. It also considers the implications to the organization of suppliers of products or services that do not have adequate continuity arrangements in place.

This Technical Specification will be useful to those who buy, manage or are responsible for a product or service that is necessary for the organization to produce its own products or services and will assist them to apply good BCM practice in line with established standards.

Organizations rely on suppliers to deliver products or services on time and to agreed quality or standards. It is important for an organization, as part of its wider approach to business continuity management, to recognize the potential impact to its activities of disruption within its supply chain. Failure by a supplier to deliver on time to an agreed quality and cost, a product or service may trigger a business disruption event. Conflicting objectives must be managed between reducing supply chain cost, for example, by reducing cycle times and buffer stock, and managing the supply chain continuity risk arising from single source and just-in-time supply approaches.

This Technical Specification is relevant to both the supply of products and services from external suppliers and internal relationships within divisions of the same organization, under any type of continuing supplier relationship. It also has applicability to single or one-time sourcing arrangements where failure to deliver could impact the future of the organization.

Suppliers are classified according to their criticality considering the impact on the organization of a disruption to the supplied products or services and the "supplier tier", which defines that supplier's relationship with the organization. A Tier 1 supplier has a direct contractual relationship with the organization, while a Tier 2 supplier provides products and services to a Tier 1 supplier. The same supply chain continuity considerations apply to relationships between tiers. Tier 1 suppliers would be responsible for assuring their own supply chain relationships, recognizing that the customer may need visibility of these relationships both to ensure there is adequate resilience in the supply chain beyond Tier 1 and to take account of factors such as corporate social responsibility which may require visibility of further tiers.

The guidance given in this Technical Specification also has relevance to the supplier both so that it can prepare to meet the business continuity expectations of its customers and also to consider vulnerabilities which might arise from dependence on a single customer.

This Technical Specification recognizes that suppliers may also comply with the requirements of the ISO 28000 series of standards for security management within the supply chain. Conformance with these standards will give organizations further confidence in the resilience of their supply chain and potentially reduces the risk of disruption when buying goods or services.

The text is aligned with the elements of business continuity management (see Figure 1).

Figure 1 — Elements of business continuity management (BCM) (Source: ISO 22313:2012, Figure 5)

Table 1 — Elements of business continuity management and relevant Clause in this Technical Specification

BCMS element	ISO/TS 22318 Clause
Operational planning and control	Clause 4
Business impact analysis and risk assessment	Clause 5
Business continuity strategy	Clause 6
Establish and implement business continuity procedures	Clause 7
Exercising and testing	Clause 8

Societal security — Business continuity management systems — Guidelines for supply chain continuity

1 Scope

This Technical Specification gives guidance on methods for understanding and extending the principles of BCM embodied in ISO 22301 and ISO 22313 to the management of supplier relationships. This Technical Specification is generic and applicable to all organizations (or parts thereof), regardless of type, size and nature of business. It is applicable to the supply of products and services, both internally and externally. The extent of application of this Technical Specification depends on the organization's operating environment and complexity.

Supply chain management considers the full range of activities concerned with the provision of supplies or services to an organization as a part of business-as-usual. The scope of this Technical Specification is less broad in that it specifically considers the issues faced by an organization which needs continuity of supply of products and services to protect its business activities or processes, and the continuity strategies for current suppliers within supply chains, which can be used to mitigate the impact of disruption; this is SCCM.

Guidance on developing a business continuity plan or business continuity management system is set out in ISO 22301 and ISO 22313.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Societal security — Terminology*

ISO 22301, *Societal security — Business continuity management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300, ISO 22301, and the following apply.

NOTE All terms and definitions contained in ISO 22300 are available on the ISO Online Browsing Platform: www.iso.org/obp.

3.1 Terms included in ISO 22300

3.1.1
business continuity
capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident

[SOURCE: ISO 22300:2012, 2.1.10]

3.1.2
business impact analysis
process of analysing activities and the effect that the business disruption might have upon them

[SOURCE: ISO 22300:2012, 2.2.6]