
**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*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TS 22318:2015](https://standards.iteh.ai/catalog/standards/sist/9b9a69e8-f9ef-4ef2-8f80-d04e7fb3a72a/iso-ts-22318-2015)

[https://standards.iteh.ai/catalog/standards/sist/9b9a69e8-f9ef-4ef2-8f80-
d04e7fb3a72a/iso-ts-22318-2015](https://standards.iteh.ai/catalog/standards/sist/9b9a69e8-f9ef-4ef2-8f80-d04e7fb3a72a/iso-ts-22318-2015)



iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/TS 22318:2015

<https://standards.iteh.ai/catalog/standards/sist/9b9a69e8-f9ef-4ef2-8f80-d04e7fb3a72a/iso-ts-22318-2015>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
3.1 Terms included in ISO 22300	1
3.2 Terms included in ISO 22301	3
3.3 Terms and definitions applicable to this Technical Specification	5
4 Why supply chain continuity is important	6
4.1 General	6
4.2 Describing the supply chain	6
4.3 Dynamics of supply chains	8
4.3.1 General	8
4.3.2 Supplier and contract lifecycle	8
4.3.3 Who owns the risk?	9
4.4 The essentials for SCCM	9
4.5 Benefits of effective SCCM	10
4.6 Challenges to effective SCCM	10
4.7 Key points of Clause 4 : Why supply chain continuity is important	11
5 Analysis of the supply chain	11
5.1 General	11
5.2 Considerations for analysing the supply chain	11
5.3 Define the approach	12
5.4 Structure of the analysis	12
5.5 Conducting the analysis	13
5.6 Output of analysis	14
5.7 Key points of Clause 5 : Analysis of the supply chain	14
6 SCCM strategies	15
6.1 General	15
6.2 Continuity strategy options	15
6.2.1 Option 1 — Accept status quo	15
6.2.2 Option 2 — Reduce dependency	15
6.2.3 Option 3 — Increase resilience	15
6.2.4 Option 4 — Work with the supplier	16
6.2.5 Option 5 — Ending the relationship	16
6.3 Including SCCM capability into a supply contract	16
6.4 Ownership of SCCM	17
6.5 Key points of Clause 6 : Considering options: developing strategies	17
7 Managing a disruption in the supply chain	17
7.1 General	17
7.2 Before an incident happens	18
7.3 Incident detection and notification	18
7.4 During an incident	18
7.5 Return to business as usual	19
7.6 Key points of Clause 7 : Managing a disruption in the supply chain	19
8 Performance evaluation	19
8.1 General	19
8.2 Engaging with suppliers	20
8.3 Implementing an SCCM performance evaluation programme	20
8.4 Maintaining the analysis	20
8.5 Outcomes of performance evaluation	21

8.6	Key points of Clause 8 : Performance management.....	21
Bibliography	22

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TS 22318:2015](#)

<https://standards.iteh.ai/catalog/standards/sist/9b9a69e8-f9ef-4ef2-8f80-d04e7fb3a72a/iso-ts-22318-2015>

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*.

[ISO/TS 22318:2015](#)

<https://standards.iteh.ai/catalog/standards/sist/9b9a69e8-f9ef-4ef2-8f80-d04e7fb3a72a/iso-ts-22318-2015>

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 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)

iTeh STANDARD PREVIEW

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

BCMS element	ISO/TS 22318:2015	ISO/TS 22318 Clause
Operational planning and control	https://standards.iteh.ai/catalog/standards/sist/9b9a69e8-f9ef-4ef2-8f80-d04e7fb3a72a/iso-ts-22318-2015	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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TS 22318:2015](#)

<https://standards.iteh.ai/catalog/standards/sist/9b9a69e8-f9ef-4ef2-8f80-d04e7fb3a72a/iso-ts-22318-2015>

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]

ISO/TS 22318:2015(E)

3.1.3

event

occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences and can have several causes.

Note 2 to entry: An event can consist of something not happening.

Note 3 to entry: An event can sometimes be referred to as an “incident” or “accident”.

Note 4 to entry: An event without consequences can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.

[SOURCE: ISO 22300:2012, 2.1.8]

3.1.4

exercise

process to train for, assess, practice, and improve performance in an organization

Note 1 to entry: Exercises can be used for validating policies, plans, procedures, training, equipment, and interorganizational agreements, clarifying and training personnel in roles and responsibilities, improving interorganizational coordination and communications, identifying gaps in resources, improving individual performance and identifying opportunities for improvement, and a controlled opportunity to practice improvisation.

Note 2 to entry: A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned.

[SOURCE: ISO 22300:2012, 2.4.8]

3.1.5

incident

situation that might be, or could lead to, a disruption, loss, emergency or crisis

[SOURCE: ISO 22300:2012, 2.1.15]

3.1.6

mutual aid agreement

pre-arranged understanding between two or more entities to render assistance to each other

[SOURCE: ISO 22300:2012, 2.2.13]

3.1.7

prioritized activities

activities to which priority must be given following an incident in order to mitigate impacts

Note 1 to entry: Terms in common used to describe activities within this group include critical, essential, vital, urgent and key.

[SOURCE: ISO 22300:2012, 2.3.5]

3.1.8

risk

effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected: positive and/or negative.

Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

Note 3 to entry: Risk is often characterized by reference to potential events, and consequences, or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

[SOURCE: ISO 22300:2012, 2.1.5]

3.1.9 top management

person or group of people that directs and controls an organization at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: An organization can, for this purpose, be identified by reference to the scope of the implementation of a management system.

[SOURCE: ISO 22300:2012, 2.2.4]

3.2 Terms included in ISO 22301

3.2.1 activity

process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products and services

EXAMPLE Such processes include accounts, call centre, IT, manufacture, distribution.

[SOURCE: ISO 22301:2012, 3.1]

3.2.2 business continuity management

holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

[SOURCE: ISO 22301:2012, 3.4]

3.2.3 business continuity management system BCMS

part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity

Note 1 to entry: The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes and resources.

[SOURCE: ISO 22301:2012, 3.5]

3.2.4 business continuity plan

documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption

Note 1 to entry: Typically, this covers resources, services and activities required to ensure the continuity of critical business functions.

[SOURCE: ISO 22301:2012, 3.6]

3.2.5

business continuity programme

ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management

[SOURCE: ISO 22301:2012, 3.7]

3.2.6

interested party stakeholder

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: This can be an individual or group that has an interest in any decision or activity of an organization.

[SOURCE: ISO 22301:2012, 3.21]

3.2.7

minimum business continuity objective

MBCO

minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption

[SOURCE: ISO 22301:2012, 3.28]

3.2.8

organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: For organizations with more than one operating unit, a single operating unit can be defined as an organization.

[SOURCE: ISO 22301:2012, 3.33]

3.2.9

outsource

make an arrangement where an external organization performs part of an organization's function or process

Note 1 to entry: An external organization is outside the scope of the management system, although the outsourced function or process is within the scope.

[SOURCE: ISO 22301:2012, 3.34]

3.2.10

products and services

beneficial outcomes provided by an organization to its customers, recipients and interested parties, e.g. manufactured items, car insurance and community nursing

[SOURCE: ISO 22301:2012, 3.41]

3.2.11

recovery time objective

RTO

period of time following an incident within which

- product or service must be resumed,