

---

---

**Security and resilience — Business  
continuity management systems —  
Guidelines for supply chain continuity  
management**

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

[ISO/TS 22318:2021](https://standards.iteh.ai/catalog/standards/iso/d9df69c9-0826-405d-a1d7-830c701bb901/iso-ts-22318-2021)

<https://standards.iteh.ai/catalog/standards/iso/d9df69c9-0826-405d-a1d7-830c701bb901/iso-ts-22318-2021>



iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

[ISO/TS 22318:2021](https://standards.iteh.ai/catalog/standards/iso/d9df69c9-0826-405d-a1d7-830c701bb901/iso-ts-22318-2021)

<https://standards.iteh.ai/catalog/standards/iso/d9df69c9-0826-405d-a1d7-830c701bb901/iso-ts-22318-2021>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 The value of supply chain continuity management</b> .....	<b>1</b>
4.1 The supply chain.....	1
4.1.1 General.....	1
4.1.2 Supply chain model.....	2
4.2 Supply chain continuity management.....	3
4.2.1 General.....	3
4.2.2 Embedding SCCM.....	4
4.2.3 Benefits and opportunities.....	5
4.3 Risk ownership.....	5
4.4 SCCM ownership.....	5
<b>5 BCMS prerequisites for SCCM</b> .....	<b>6</b>
5.1 General.....	6
5.2 Obtain top management commitment.....	6
5.2.1 Accountability and responsibility.....	6
5.2.2 Resources for managing SCCM.....	6
5.2.3 SCCM framework.....	6
5.2.4 Performance evaluation programme.....	7
5.3 Promulgate business continuity principles throughout the supply chain.....	7
5.4 Analyse continuity requirements and assess risk.....	7
5.4.1 General.....	7
5.4.2 Continuity requirements.....	8
5.4.3 Risk assessment.....	8
<b>6 Effective SCCM</b> .....	<b>9</b>
6.1 General.....	9
6.2 Identify strategies and solutions.....	9
6.2.1 General.....	9
6.2.2 Option 1 — Reduce dependency and impact.....	10
6.2.3 Option 2 — Rely on the organization's business continuity strategies and solutions.....	10
6.2.4 Option 3 — Rely on the supplier's business continuity strategies and solutions.....	11
6.2.5 Option 4 — Do nothing and retain the risk by informed decision.....	12
6.3 Assess suppliers' continuity compliance.....	12
6.4 Establish contractual obligations.....	12
6.4.1 General.....	12
6.4.2 Principles to establish the continuity requirements in the contract.....	12
6.4.3 Continuity requirements.....	13
6.5 Review and update.....	14
<b>7 Maintenance, performance and continual improvement</b> .....	<b>14</b>
7.1 General.....	14
7.2 Maintenance.....	14
7.3 Performance evaluation.....	15
7.4 Continual improvement.....	15
<b>Annex A (informative) Example of general questions to be sent to priority suppliers</b> .....	<b>17</b>
<b>Annex B (informative) Managing priority suppliers' disruptions</b> .....	<b>18</b>

<b>Annex C (informative) Examples of joint exercises with suppliers</b> .....	<b>19</b>
<b>Bibliography</b> .....	<b>20</b>

**iTeh Standards**  
**(<https://standards.itih.ai>)**  
**Document Preview**

[ISO/TS 22318:2021](https://standards.itih.ai/catalog/standards/iso/d9df69c9-0826-405d-a1d7-830c701bb901/iso-ts-22318-2021)

<https://standards.itih.ai/catalog/standards/iso/d9df69c9-0826-405d-a1d7-830c701bb901/iso-ts-22318-2021>

## 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](http://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](http://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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This second edition cancels and replaces the first edition (ISO/TS 22318:2015), which has been technically revised. The main changes are as follows:

- the document has been updated to reflect changes made to ISO 22301:2019;
- the upstream and downstream relationships within the supply chain have been clarified;
- the title has been updated;
- “key points” have been deleted as their concepts are included in the clauses;
- new diagrams have been inserted;
- annexes have been inserted.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at [www.iso.org/members.html](http://www.iso.org/members.html).

## Introduction

The focus of this document is on establishing appropriate levels of continuity within an organization's supply chain. It assumes that the organization seeking to establish supply chain continuity management (SCCM) is aware of the principles of business continuity. It is intended to be useful to those with responsibility for the continuity of the supply chain for resources required by the organization to produce and deliver its products and services. The guidelines given in this document also have relevance when the organization is the supplier as the organization can then prepare to meet the continuity expectations of its customers as well as consider vulnerabilities which can arise when dependent on a single customer.

This document considers the continuity implications to the organization if its suppliers do not have adequate continuity in place.

Organizations rely on resources to be delivered on time and at an agreed quality and cost. These include, for example, materials, labour, information and data, workplace, facilities and associated utilities, equipment, consumables, information communication technology (ICT) systems, transportation, logistics, finance and other services required to support the business activities of the organization. This is referred to as "upstream".

Organizations also rely on being able to deliver their products and services to their customers, whether they are the next link in the supply chain or the end customer. Product and service delivery (e.g. transportation, logistics, implementation services, machinery installation services) is performed by the organization or by a third party under the organization's responsibility. This is referred to as "downstream".

An organization needs to recognize the potential impact of not resuming activities within an acceptable time frame due to supply chain disruption. Failure by a supplier to deliver resources on time at an agreed quality and cost can trigger a business disruption. The organization needs to take account of and manage conflicting objectives such as reducing supply chain cost by reducing cycle times or buffer stock and managing the supply chain continuity risk arising from a single source and just-in-time supply approaches. The organization needs to achieve an acceptable balance between risks and continuity measures.

The criticality of suppliers and the required recovery time is determined during the business impact analysis (BIA) (see ISO/TS 22317) phase of the business continuity management system (BCMS). Priority suppliers are those who support prioritized activities and are identified as having the greatest impact if they fail to deliver resources, thereby impacting the organization's ability to deliver its own products or services.

The "supplier tier" defines the supplier's relationship with the organization. A contracted supplier (Tier 1) has a direct relationship with the organization, while an indirect supplier (Tier 2 and beyond) provides resources to a contracted supplier and, as a result, is more difficult to control. Suppliers should be encouraged to implement SCCM within their own supply chain, which will improve the continuity of the whole supply chain.

This document expressly excludes:

- customer management issues, such as retention and impact as a result of new or lost clients;
- supply chain activities within the organization; internal suppliers within the scope of the BCMS should be identified as dependencies or interdependencies and their ability to continue their deliveries should be part of the organization's BCMS.

Following the guidance of this document will be beneficial to the supply chain. Suppliers can also choose to conform to the requirements of the ISO 28000 family of standards for security management within the supply chain. Conforming to these standards will give organizations further confidence in the resilience of their supply chain and potentially reduce the risk of disruption when buying resources.

# Security and resilience — Business continuity management systems — Guidelines for supply chain continuity management

## 1 Scope

This document gives guidance on methods for understanding and extending the principles of business continuity embodied in ISO 22301 and ISO 22313 to the management of supplier relationships. It enables an organization to develop and document the strategy to be better prepared to manage supply chain continuity.

This document is generic and applicable to all organizations. It is applicable to suppliers of products, services and resources, both upstream and downstream.

Supply chain continuity management (SCCM) specifically considers the issues faced by an organization which relies on the continuity of supply of resources as well as the ability to continue delivery of its products and services. The objective of SCCM is to protect the organization's business activities from supply chain disruption.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

ISO 22300, *Security and resilience — Vocabulary*

ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

ISO 22313, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300, ISO 22301 and ISO 22313 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

## 4 The value of supply chain continuity management

### 4.1 The supply chain

#### 4.1.1 General

Supply chains are growing in length and complexity. Effective SCCM requires the organization to ensure that each link in its supply chain has effective continuity measures in place.

Supply chains extend beyond the organization’s direct control, with many factors determining the degree of control including relative size and leverage, geography and the number and type of suppliers.

Besides direct disruptions in the supply chain, the organization should also consider impacts on supply and demand based on global or local events as well as market dynamics which can result in:

- excessive demand over supply which can cause resource constraints;
- widespread excess of supply which can cause a collapse in demand for the products and services that the organization provides.

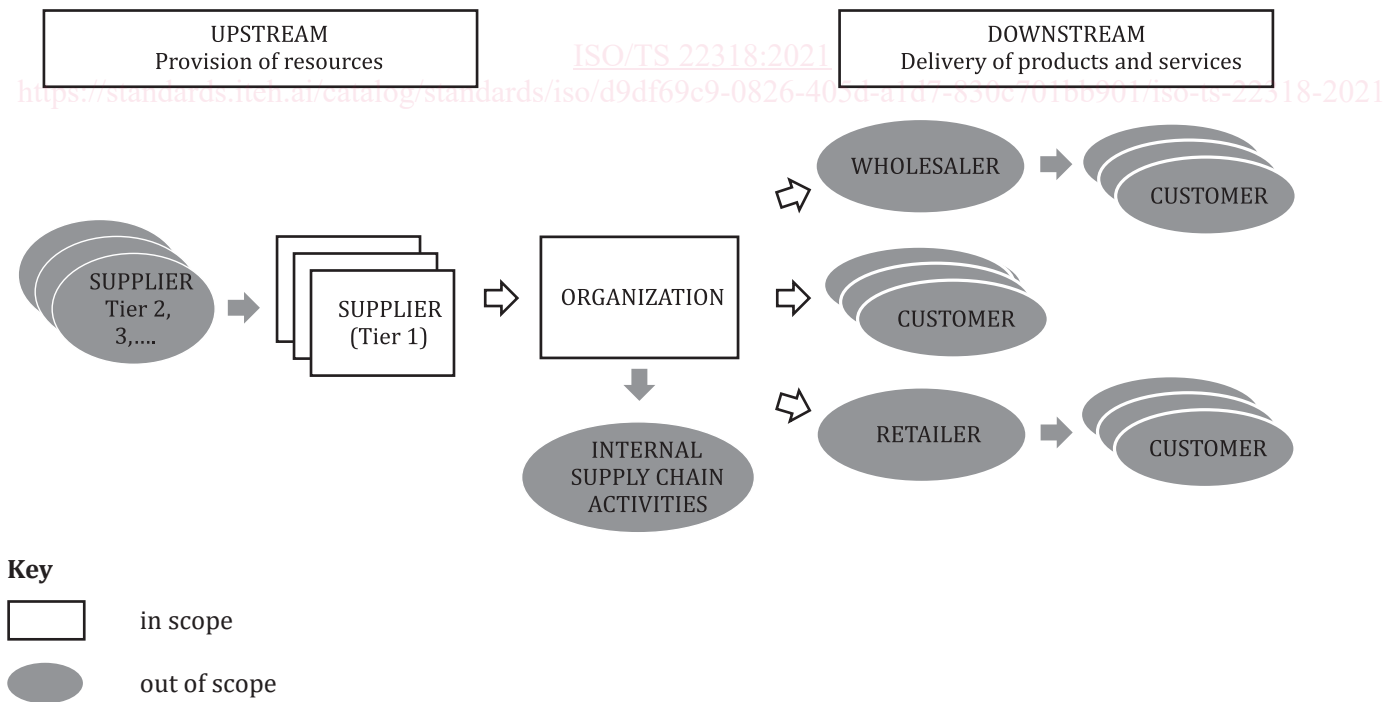
Supply chains have extended due to:

- global access at relatively low cost provided by evolving technology;
- cost-effective international transport;
- changing international trade barriers and the free movement of capital;
- availability of educated and relatively low-cost skilled workers across the world.

Organizations have become more interdependent due to the focus on core value-adding activities and the trend is to outsource activities, such as logistics, distribution, payroll, catering, cleaning, security and IT.

**4.1.2 Supply chain model**

A broad view of a supply chain includes the provision of resources by suppliers to the organization (upstream), and the delivery of products and services of the organization to its customers (downstream). It applies to organizations of all types and sizes. [Figure 1](#) illustrates a simple supply chain model and also shows the relationships and direct influence of the organization, which is within the scope of this document.



**Figure 1 — Supply chain model**



NOTE 1 Resources include materials, labour, information and data, workplace, facilities and associated utilities, equipment, consumables, ICT systems, transportation, logistics, finance and other services required for the activities of the organization.

NOTE 2 Products and services delivery includes transportation, logistics, implementation, machinery installation services, etc. performed by the organization or by a third party under the organization's responsibility.

It is possible that the end user is not the immediate customer of the products and services. In some circumstances, the organization needs to consider that post-delivery use and consequences of the provision of their products and services, beyond the immediate customer, can impact brand and reputation. The organization can consider contracts to control subsequent use or implement end-user agreements to limit further downstream transfer.

A supply chain exists where the provision of resources depends on other organizations that are not under the direct management or control of the organization.

There are different types of relationships that an organization can have:

- upstream relationships:
  - long term for recurring resources such as raw material, workspace, professional services;
  - one time for infrequent resource acquisition such as special projects;
  - professional association such as franchises, supplier associations;
- downstream relationships:
  - business-to-business (wholesalers and retailers);
  - business-to-customer.

The basis for all these relationships is commitments to meet interested parties' expectations. These commitments can either be explicit (e.g. contract or purchase order) or implicit (e.g. what can be reasonably expected).

Organizations in the supply chain should take into account that the degree of flexibility and the related control on essential services and heavily regulated suppliers can be constrained, e.g. national electric companies, telecommunications, internet providers.

NOTE The above relationship types provide examples only and are not intended to be complete.

## 4.2 Supply chain continuity management

### 4.2.1 General

SCCM is a management process that identifies potential impacts to an organization from disruption to its supply chain and provides an approach to manage this. Continuity of the supply chain is important to all organizations, enabling them to deliver products and services. Disruption to the supply chain can impact or even prevent the organization from delivering those products and services with consequent negative effects to its revenue, market share and reputation. Effective SCCM enables the organization to avoid or minimize the consequences of disruption.

There can be conflict between SCCM and the objectives of supply chain management such as the need to reduce costs, avoid excessive inventory and optimization of lead times. Organizations should recognize that effectively managing the supply of resources will lead to increased control of the supply chain, improved efficiency and help to avoid severe disruptions.

SCCM seeks to identify those suppliers who can significantly impact the organization and ensure that the organization has implemented strategies and solutions to address these. Formal agreements with suppliers should ensure appropriate business continuity provisions are made that satisfy the

organization’s requirements. For some suppliers, this will not be possible, e.g. where a large supplier insists on using its own standard contract terms, and in these cases the organization should develop strategies and solutions.

Supply chains extend beyond the organization’s direct control. The organization can be vulnerable to disruptions in suppliers who are remote from the direct contractual relationship (i.e. in Tiers 2, 3, etc.) and therefore SCCM seeks to promote continuity provisions to those organizations beyond its direct control.

Effective SCCM, therefore, needs to be embedded in the organization’s own supply chain management; continuity requirements need to be understood; strategies and solutions defined and implemented; additional contractual obligations agreed with suppliers and promulgated further where necessary; checks made that these obligations are met and then ensure that this is all monitored and updated as required.

#### 4.2.2 Embedding SCCM

For SCCM to be successful it must be effectively embedded within the organization’s existing processes. Suppliers’ contracts exist within a life cycle of acquisition, operation, review and renewal or discontinuation. Entry into a new contract or renewing an existing contract presents an opportunity for the organization to influence future supplier behaviour through the contract and/or service level changes. Conversely, long-term contractual commitments and high supplier-switching costs can shift the leverage between the organization and its suppliers, creating resistance to changing future suppliers’ behaviour. The analysis of the supply chain (see 5.4) will help to identify high-priority relationships and the requirements and opportunities for implementing SCCM. See Figure 2.

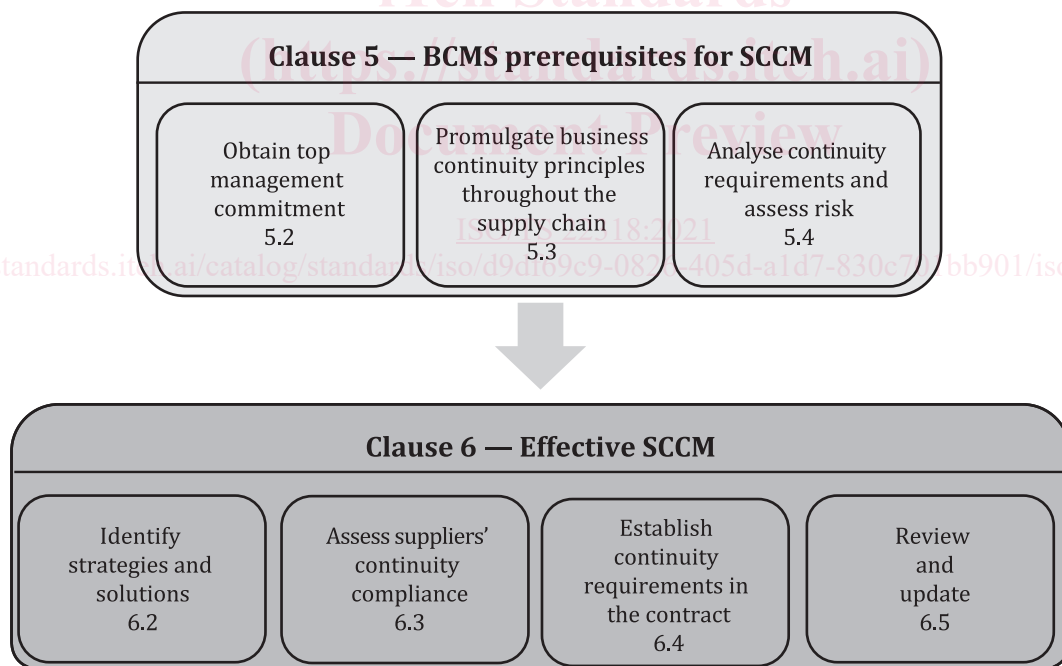


Figure 2 — Embedding SCCM

To embed SCCM, the following are essential:

- prerequisites:
  - obtain top management commitment to ensure SCCM is an integral part of the BCMS (see 5.2);
  - promulgate business continuity principles throughout the supply chain to promote awareness and improve effectiveness (see 5.3);