TECHNICAL SPECIFICATION

ISO/TS 22318

Second edition
2021-12

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

Reference number
ISO/TS 22318:2021(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 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.

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.

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.