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)

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.

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.

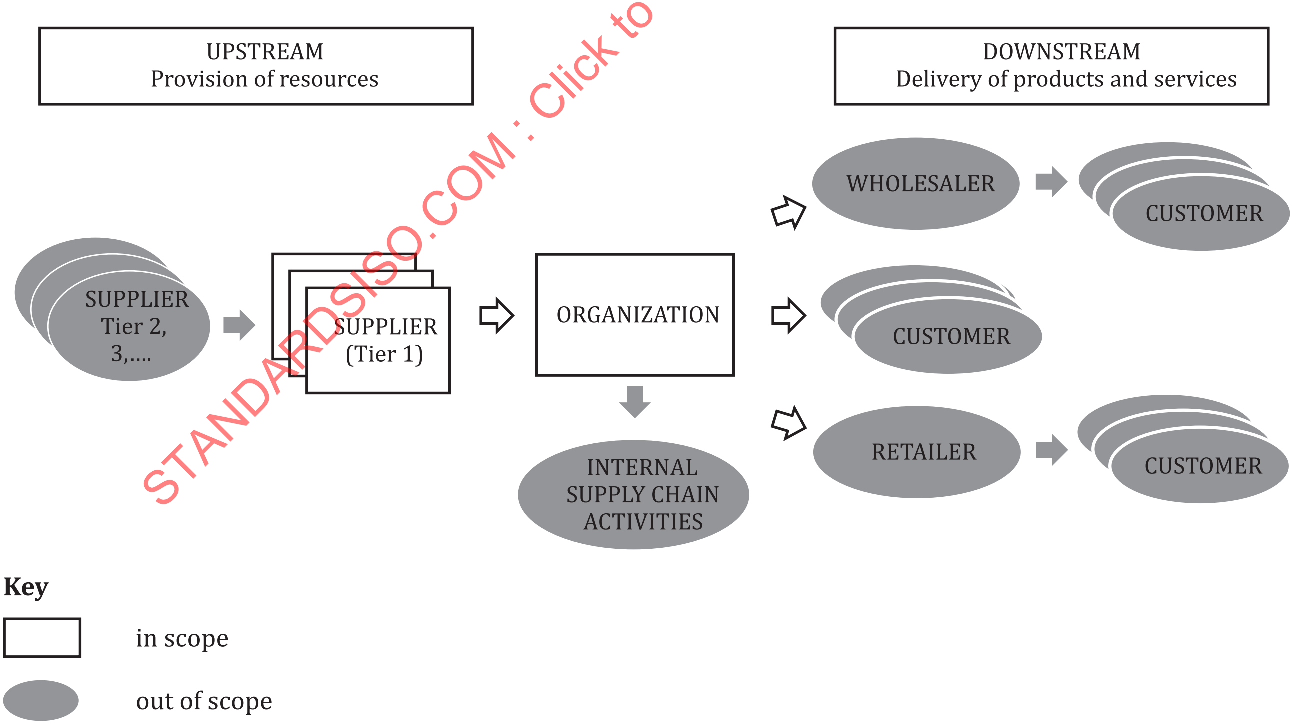

Figure 1 — Supply chain model

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.

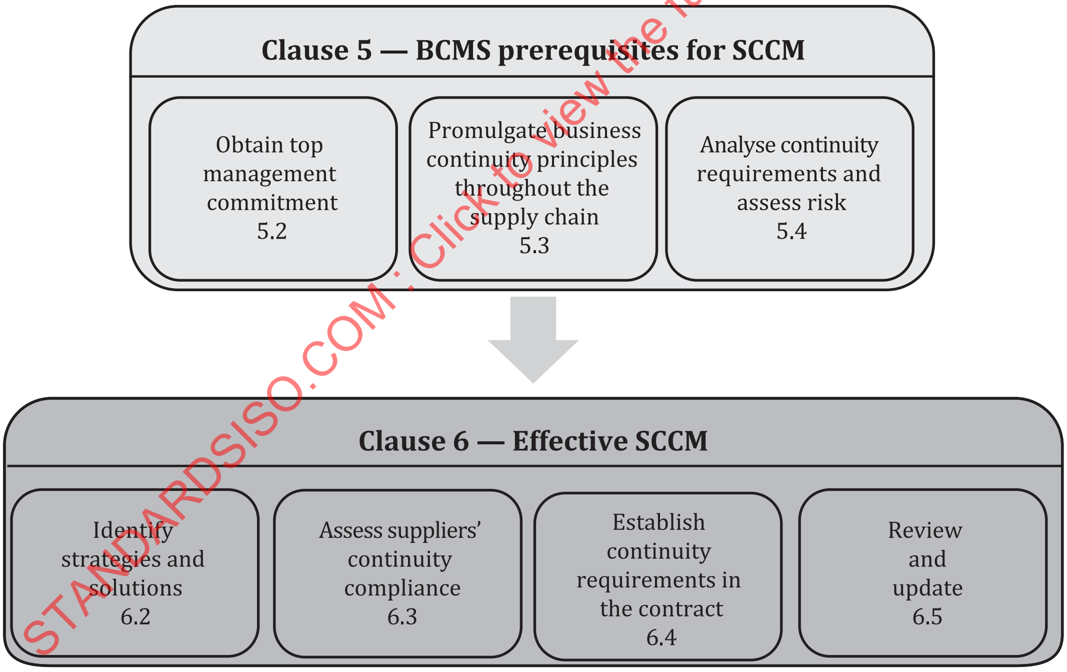
Clause 5 — BCMS prerequisites for SCCM
Obtain top management commitment 5.2
Promulgate business continuity principles throughout the supply chain 5.3
Analyse continuity requirements and assess risk 5.4
Clause 6 — Effective SCCM
Identify strategies and solutions 6.2
Assess suppliers' continuity compliance 6.3
Establish continuity requirements in the contract 6.4
Review and update 6.5

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);

  - analyse continuity requirements, as obtained during the BIA process, and assess risks to the organization (see 5.4);

- SCCM execution:
  - identify SCCM-specific strategies and solutions (see 6.2);
  - assess priority suppliers' continuity compliance and ensure that their contracts reflect agreed continuity measures (see 6.3);
  - establish contractual obligations that meet the organization's requirements (see 6.4);
  - review and update the continuity requirements agreed with each supplier (see 6.5).

4.2.3 Benefits and opportunities

Potential benefits for all parties of effective SCCM include:

- better understanding of the supply chain and the impact of potential disruptions;
- improved supplier relationship management to reduce the impact of supply chain disruption;
- improved response to supply chain disruptions resulting from effective collaboration with suppliers;
- identification and mitigation of supply chain risks;
- improved planning, due diligence, assurance and working relationships with suppliers;
- competitive advantage over competitors who do not have effective SCCM.

SCCM presents several opportunities, including:

- improved ability to provide management with information to make effective decisions to allocate necessary personnel and resources to maintain SCCM;
- effective integration of SCCM responsibilities across the organization through the SCCM owner (see 4.4);
- understanding the suppliers' continuity capabilities and their requirements of the organization;
- establishment of performance metrics;
- engagement to enhance understanding and strategy relating to suppliers beyond Tier 1.

4.3 Risk ownership

The organization owns and retains the risk that it is not always able to deliver its products and services to its customers as a consequence of a disruption in its supply chain. It is responsible for mitigating this risk by being prepared to respond to a supply chain disruption. Customers hold the organization, not its suppliers, responsible for failure to deliver products and services. For example, an organization's brand and reputation are at risk of damage if there is a problem within its supply chain.

4.4 SCCM ownership

The organization should identify those with responsibility for supplier relationship management and for securing and monitoring supply chain continuity assurance.

SCCM ownership should be delegated to personnel responsible for contracting and purchasing operations. The responsibility should be closely linked to the wider arrangements for business continuity within the organization.

The SCCM owner is responsible for:

- appointing representatives to manage SCCM tasks;
- ensuring SCCM requirements are included in contracts, purchase orders and other binding agreements;
- ensuring suppliers adhere to the terms of their agreements;
- ensuring that evidence of supplier compliance is appropriate and that any agreed remediation is completed within agreed timescales.

5 BCMS prerequisites for SCCM

5.1 General

The BCMS prerequisites for SCCM are illustrated in Figure 2 (embedding SCCM). These are:

- obtain top management commitment (see 5.2);
- promulgate the organization's business continuity principles throughout the supply chain (see 5.3);
- analyse continuity requirements and assess risk (see 5.4).

5.2 Obtain top management commitment

5.2.1 Accountability and responsibility

Top management should allocate accountability and responsibility for the management of SCCM including:

- ensuring SCCM conforms to the business continuity policy;
- promoting awareness of SCCM throughout the organization (see 5.3);
- ensuring the effectiveness of the processes implemented (see Clause 7);
- reporting on the performance of SCCM to top management for review and as the basis for improvement (see 7.3 and 7.4).

5.2.2 Resources for managing SCCM

Top management should determine and ensure availability of the resources (e.g. people, facilities, funding) needed to manage SCCM that will:

- achieve its objectives;
- meet the changing requirements of the organization;
- enable effective communication on SCCM matters, internally and externally;
- provide for the ongoing operation and continual improvement of SCCM.

5.2.3 SCCM framework

Top management should establish a framework to manage the impact of supply chain disruption and support the continuity of the supply chain when a disruption occurs. This includes:

- scope, goals and objectives;
- requirements analysis, risk assessment, strategies and solutions (see 5.4 and 6.2);

- exercise and test programme;
- specific contract clauses and appropriate service level agreements (SLAs) with suppliers;
- supplier notification and incident response procedures.

5.2.4 Performance evaluation programme

Top management should establish a performance evaluation programme (see 7.3) guiding the organization to establish and maintain a strategy to build a more resilient supply chain by:

- embedding SCCM in all applicable processes of the organization;
- engaging with suppliers;
- ensuring contractual obligations have been met and are being monitored;
- ensuring complete assessment of supply chain continuity risks for new products and services and new suppliers.

The performance evaluation should:

- specify what is to be evaluated;
- identify how, when and by whom the evaluation should be performed;
- set performance metrics, including qualitative and quantitative measurements;
- facilitate subsequent corrective action analysis, if needed.

5.3 Promulgate business continuity principles throughout the supply chain

The organization should promulgate its business continuity principles throughout its supply chain to promote awareness and improve effectiveness. This can be achieved by:

- including compliance with continuity requirements in suppliers' contracts;
- establishing required supplier compliance levels based on their disruptive impact;
- developing methodologies to monitor compliance;
- requiring that the organization's suppliers also promulgate business continuity principles throughout their own supply chain.

5.4 Analyse continuity requirements and assess risk

5.4.1 General

The organization should determine the business continuity required from suppliers to meet the organization's continuity requirements.

Organizations typically have many suppliers, but it is not always necessary to perform a detailed analysis on all of these. The organization should focus the analysis only on those suppliers which can disrupt the organization's prioritized activities. For selected suppliers, a structured approach is needed. The BIA should provide a list of the suppliers supporting the prioritized activities; however, it is possible that it is not complete or up to date. This process is intended to ensure that the list is accurate.

5.4.2 Continuity requirements

Within SCCM, the organization should:

a) collate relevant available documentation including the BIA, risk assessments and list of existing suppliers;

b) identify the suppliers supporting the organization's prioritized activities, which become the priority suppliers; this can be achieved by obtaining a list of suppliers from procurement and by:

   1) using external dependency information from the BIA;

   2) selecting suppliers who provide critical resources (e.g. utility companies, telecommunication providers);

c) for each priority supplier, assess:

   1) the criticality of the resources provided to the organization (upstream) or the delivery service provided regarding the organization's products and services (downstream);

   2) whether they are a single source;

   3) the extent to which they have already assessed their own supply chain risks (Tier 2 and beyond);

   4) the risk of disruption to their continued ability to supply to the organization;

   5) whether effective business continuity is in place;

   6) the priority assigned to the organization by the supplier on its list of customers;

   7) whether their recovery time objective (RTO) is aligned with that of the organization for the activity or process they support;

d) define the actions to be taken in the event a supplier does not meet the organization's requirements;

e) identify existing strategies and solutions for priority suppliers (see 6.2);

f) assess where suppliers share common dependencies which increases the risk to the organization;

   EXAMPLE If the organization has several suppliers of the same product but they all rely on one supplier of a component of that product (Tier 2 and beyond) or where each supplier is located in the same geographical area which can be impacted by a single incident (e.g. a flood affecting a whole region, movement restrictions arising from quarantine measures).

g) produce a list of priority suppliers for which there is no satisfactory current strategy or solution.

These priority suppliers are then used as input to strategies and solutions (see 6.2) to determine which approaches the organization wishes to take with each of them that best mitigates the risk to the organization, including contractual obligations on the supplier where appropriate.

5.4.3 Risk assessment

Risks should be considered when selecting suppliers and establishing contractual obligations.

SCCM needs to consider applicable risks when evaluating a supplier. The organization's risk assessment should consider both the risks to the organization as well as the risks to the supplier.

The possible risks to the organization include loss or reduction of:

- timely supply;
- quality;

- flexibility.

The possible risks to the supplier as defined by the organization’s assessment include:

- share of supplier capacity;
- supplier solvency;
- supplier’s known supplier risks;
- natural disasters and geopolitical risks.

If a priority supplier does not consider the organization to be important, this can create a significant risk. The organization should determine the priority assigned by the supplier in case of a disruption.

A disruption to the organization or its suppliers (upstream and downstream) can cause an impact to other parts of the supply chain and can amplify the impact to the organization. This should be considered during the risk assessment. The organization and downstream suppliers can identify opportunities for strategies and solutions that provide mutual benefit.

6 Effective SCCM

6.1 General

Clause 5 describes the BCMS prerequisites for SCCM. The implementation of processes to achieve an effective SCCM is illustrated in Figure 2 (embedding SCCM). These are:

- identify strategies and solutions (see 6.2);
- assess suppliers’ continuity compliance (see 6.3);
- establish contractual obligations (see 6.4);
- review and update (see 6.5).

This will enable SCCM to set and meet the expectations of relevant interested parties.

6.2 Identify strategies and solutions

6.2.1 General

To select the appropriate strategies and solutions, the organization should quantify the cost of disruption, e.g. in terms of lost output, cost of customer compensation and damage to brand and reputation. The level of SCCM measures to be implemented should be commensurate with the cost of disruption.

The organization should use the continuity requirements (see 5.4.2) and risk assessment (see 5.4.3) to identify appropriate SCCM strategies and solutions for each identified supplier.

Determining the most appropriate strategies and solutions should be a joint effort reflecting different viewpoints from representatives within the organization. It can include:

- SCCM owner (see 4.4);
- top management;
- procurement or contract management;
- business continuity team;
- activity owners dependent on the identified priority suppliers.

It can also include representatives of priority suppliers.

Residual risks should be documented and reported to top management.

Solutions are not mutually exclusive and mitigating the risk arising from an individual supplier can require more than one approach to be implemented. Achieving an optimum solution can take time. It can be necessary to adopt interim approaches with some suppliers until the opportunity arises to implement the preferred solution, particularly where the existing contract has a considerable time to run and there is limited opportunity to negotiate any change of conditions.

There are different options to implement the most adequate solutions, which can require several in combination. Some options are described in 6.2.2 to 6.2.5.

6.2.2 Option 1 — Reduce dependency and impact

The organization can reduce dependence on (a) supplier(s) by the following actions:

- Ensuring two or more sources of supply at all times. The organization should check that these are not subject to the same risk of disruption, e.g. because they are located in the same region or both use a common supplier themselves (see Tier 2 and beyond in Figure 1).
- Increasing stock levels within the organization or with intermediaries to lengthen the time before a disruption affects the organization and its customers.
- Implementing pragmatic responses to manage risk arising from priority suppliers which the organization is unable to influence, e.g. providing a standby generator to cover for loss of power supplies or developing a multichannel communications systems to reduce dependence on a single channel or supplier.
- Having an insurance policy. The organization can use insurance to indemnify itself against disruption. Similarly, the organization can require that the supplier carries insurance to protect the organization. An insurance policy will only protect the organization's financial impact; therefore, it should be used in conjunction with other solutions given in this document.

The organization can also decide to adopt a commercial solution to address the issue of supplier failure. This will usually be triggered by concerns about the commercial and financial viability of the supplier and, consequently, the organization requires a process that monitors the commercial and financial health of priority suppliers. When triggered, the organization can then decide to:

- take over the supplier's activity by employing or contracting the workforce of the supplier directly, taking into consideration that, for this to be a viable response:
  - the workforce must be willing to transfer and can need incentivizing to do so;
  - provision of existing premises and IT can be agreed with the supplier, or a plan developed for the rapid transfer of the teams to new premises and systems;
- buy the supplier's business or its competitor, either in whole or in part, to maintain the priority supply of products and services.

6.2.3 Option 2 — Rely on the organization's business continuity strategies and solutions

The organization can decide to rely on its own business continuity strategies and solutions. In this case, it is essential that the following are considered:

- Obtaining an alternative supplier at the time of the disruption. In this case, the organization needs to be sure that the alternative supplier has resources, products and services that are a direct substitute for the normal supplier. If not, then a plan is needed to adapt to this change at short notice.
- Developing a contract with alternative suppliers on standby, e.g. by paying a retainer to have the ability to deliver when required. There are specialist suppliers who will provide alternative office

environments and IT on a standby contract, and others that can supply generators at short notice, etc.

- Updating the organization's business continuity plans to ensure those strategies and solutions are implemented.

To ensure that alternative suppliers can deliver when required, the organization should do the following:

- Verify that alternative suppliers have the capability to meet the needs of the organization at short notice. The organization can consider implementing an emergency procurement process (including approval of budget, authorization levels, due diligence, etc.) in case a disruption occurs.
- Consider whether it is possible that the alternative suppliers will be affected by the same disruption as the normal supplier. This can be because they are located in the same area, or both use a common supplier themselves.

Any reliance on the organization's business continuity solutions to respond to supplier disruption should be regularly exercised to confirm that it is effective and current. Joint exercises can be organized to prove that in case of disruption to the organization, the supplier and the organization both have effective strategies and solutions in place.

6.2.4 Option 3 — Rely on the supplier's business continuity strategies and solutions

The organization can decide to rely on the supplier's own business continuity strategies and solutions. In this case, it is essential to verify that these meet the needs of the organization (see Annex A). There are several steps to this, as follows:

a) Where a supplier is ISO 22301 certified, the organization still needs to assure itself that the supplier can specifically provide the products and services the organization needs. The organization can gain some level of comfort by:

   1) checking that the scope of certification covers the products, services and resources that are relevant to the organization;

   2) verifying with the supplier that their business continuity response will meet the contractual requirements of the organization in terms of delivery of resources, products and services.

   NOTE The supplier's business continuity will be designed to maintain its own business. It is not necessarily the case that this includes the supply to the organization.

b) Where a supplier is not ISO 22301 certified, then a more detailed examination should be undertaken. The supplier should be asked to explain how they will continue to meet the organization's contractual requirements after a disruption. Whenever reliance is placed upon the supplier's business continuity, the organization should verify that their own requirements would be met. The organization can choose to assist the supplier in this phase. For instance, it is possible that the supplier will be able to supply at reduced capacity, or with a similar but not an identical product, or with extended time frames. If this is deemed acceptable, then the organization should incorporate these constraints into its business continuity strategies and solutions (option 2).

c) Regardless of whether the supplier declares conformity to ISO 22301, the organization should seek assurance that:

   1) supply should be continued at an agreed level even in the face of disruption (see 6.4.2);

   2) it has a right to audit the supplier's business continuity capabilities to verify the supplier's claims.

With the consent of the supplier, the organization can engage with other customers of the supplier to validate the supplier's business continuity capability. The organization can consider the option of participating in supplier's exercises or conducting joint exercises.

The organization should consider that, even if a supplier has a validated business continuity plan, it is possible that the supplier still fails, e.g. through insolvency.

6.2.5 Option 4 — Do nothing and retain the risk by informed decision

If the organization chooses to do nothing for priority suppliers, this should be an informed, documented decision approved by top management.

6.3 Assess suppliers' continuity compliance

The organization should evaluate the selected strategies and solutions for each priority supplier.

SCCM should ensure the established continuity requirements are understood by each priority supplier (see Annex A). Suppliers should provide evidence of:

- their ability to meet the organization's continuity requirements, specifically their ability to deliver according to the RTOs and recovery point objectives (RPOs) as contracted;
- monitoring and reporting the effectiveness of their own continuity measures, including their own suppliers.

Alignment with or certification to ISO 22301 can contribute to this evidence.

The organization's SCCM representative should ensure the established continuity requirements (see 5.4.2) are understood by all prospective suppliers.

The organization's SCCM representative should review the information provided by the supplier during tendering to understand their ability to meet the organization's continuity requirements. The information provided should be retained for comparison in periodic reviews.

6.4 Establish contractual obligations

6.4.1 General

Organizations govern their relationship with their suppliers through contractual agreements. Similarly, suppliers manage their relationship with their suppliers. Agreements should include the agreed continuity requirements (e.g. contractual clauses, performance indicators, SLAs) to ensure suppliers have appropriate continuity capabilities in place.

6.4.2 Principles to establish the continuity requirements in the contract

Formal agreements should include the organization's continuity requirements as defined in 6.3:

a) delivery of products and services to meet agreed criteria during a disruption;

b) definition of the priority that would be assigned to the organization by the supplier during a disruption;

c) establish links between the respective owners of SCCM processes (organization's and supplier's);

d) manage the continuity response before, during and after a disruption, including in joint (or related) exercises;

e) periodically conduct continuity reviews and audits.

The organization can develop standard clauses to comply with the continuity requirements to be applied to new contracts.

The organization's continuity requirements should be reflected in new contracts and form part of contract renegotiation for existing contracts.

Changes to the organization’s continuity requirements should be reflected in contracts as soon as possible.

6.4.3 Continuity requirements

Formal agreements should describe continuity requirements.

The following clauses should be considered for inclusion in SCCM agreements:

- framework:
    - details of the BCMS and SCCM ownership, approach and evidence of any relevant certifications, e.g. ISO 22301;
- dependencies:
    - supplier’s criticality to the organization;
    - priority assigned to the organization by the supplier in case of disruption;
- strategies and solutions:
    - assurance that the supplier’s relevant prioritized activities, corresponding RTOs and key solutions in place (including mutual aid solutions provided by the supplier) support the organization’s continuity requirements;
    - requirements in case of unforeseen increase or decrease of the organization’s needs;
    - assurance that requirements of the supplier with its own priority suppliers are in place;
- communication process between the supplier and the organization:
    - designated communication channels;
    - escalation triggers and measures for notification of market changes and key events that can jeopardize the business continuity requirements;
    - notification of invocations, plan reviews, exercises and document revisions;
- disruption management (see Annex B):
    - before a disruption: escalation triggers and measures for notification of an incident;
    - during a disruption: crisis management cooperation, including communications;
    - after a disruption: lessons learned, corrective actions and, if needed, changes to the contract;
- requirements for validation and review of training and exercises (see Annex C), for example:
    - participation in joint exercising;
    - review of exercise evaluation reports;
    - observation of the supplier’s tests;
    - results of third-party audits;
- provisions for management review and audit of business continuity requirements.

The effects of force majeure and potential termination clauses should be considered. Force majeure clauses suspend the supplier’s obligations for the duration of the force majeure event and potentially conflict with the continuity requirements. The organization should ensure that these clauses are clearly specified.

The contractual requirements should be made known and be part of the supplier selection process.

6.5 Review and update

The organization should periodically review and update the continuity requirements agreed with each supplier. The organization should confirm that its continuity requirements are being met and are still appropriate to its needs.

The organization should review available evidence of:

- experience and outcomes of any disruption;
- outcomes of any exercises including joint exercises and tests;
- audit reports concerning business continuity;
- compliance with agreed performance measurements;
- documentation supporting the supplier's ongoing business continuity as agreed;
- status of remediation actions.

This applies both to the organization and to its suppliers.

The organization should review its continuity requirements including how these can change in the forthcoming period and should agree on changes with the supplier as required.

The organization should periodically review the supplier's risk profile, in particular:

- the interdependencies between the supplier and the organization;
- the supplier's solvency;
- known, evolving and emerging supplier's risks.

Based on the outcome of these periodic reviews, the organization should take the appropriate actions to maintain and improve its SCCM (see 7.2 and 7.4).

7 Maintenance, performance and continual improvement

7.1 General

The organization should maintain, evaluate the performance and continually improve its SCCM, to ensure effectiveness, and to identify successes and areas requiring correction or improvement. All the prerequisites (see Clause 5) and the processes to ensure effective SCCM (see Clause 6) should be considered. This includes a review of the criteria for SCCM capability required internally and agreed with suppliers. Continual improvement, in terms of the suitability, adequacy and effectiveness of SCCM should be driven by the goals and objectives, performance evaluation, analysis of disruptions and management review of the BCMS.

7.2 Maintenance

Maintenance should include:

- ensuring the continuing relevance of the established prerequisites (see Clause 5);
- ensuring strategies and solutions are regularly updated to ensure that they are fit for purpose (see 6.2);
- incorporating any enhancements found in the review process (see 6.5);

- implementing a continuous review process to monitor supply chain changes and implementation of improvements whether initiated by the organization or the supplier being reviewed;
- implementing a process to ensure all contracts with priority suppliers are updated with the applicable continuity requirements;
- responding to any audit issue.

7.3 Performance evaluation

The organization should periodically evaluate its SCCM to enable continual improvement (see 7.4) and establish an escalation process to be invoked when the performance criteria are not met.

Performance evaluation should include:

- maintaining the performance data;
- regularly refreshing the analysis (see 5.4);
- ongoing monitoring using key performance indicators (KPIs)/metrics;
- designing and using questionnaires/checklists/self-evaluation or any other methods used to assess performance by the organization, where relevant;
- evaluating the organization's procurement process to ensure continuity requirements are included;
- evaluating standard SCCM contract and schedule clauses to ensure they continue to meet the organization's needs;
- ensuring audits take place at planned intervals;
- monitoring nonconformity and other evidence of deficient SCCM performance and effectiveness.

The benefits of the process are:

- greater confidence in the resilience of the supply chain resulting from a better understanding of the risks and controls;
- evaluation of the extent to which the organization and each supplier meets the organization's continuity requirements;
- an early indication of changes likely to affect the supply chain;
- identification of gaps in capability which the organization and the supplier needs to address;
- organization and supplier monitoring and performance measurement against KPIs/metrics.

7.4 Continual improvement

Continual improvement is a key component of SCCM. This can be achieved through regular reviews, exercising and applying lessons learned. Continual improvement should enhance the effectiveness and efficiency of SCCM.

Continual improvement should include:

- identifying what to address and the present condition (room for improvement);
- identifying the present process and controls;
- determining what changes to implement (improvement);
- acting upon the changes and verifying they were successfully implemented.

The organization can achieve improvement by establishing the prerequisites for SCCM (see Clause 5) as well as effective SCCM (see Clause 6). The organization should also consider opportunities for improvement in SCCM, which can come, for example, from changes in:

- the context of the organization and its effect on the BCMS;
- the internal structure of the organization (e.g. acquisition of additional locations or staff);
- the means of production or delivery (e.g. technological change, infrastructure improvements);
- evolving methodologies or the availability of new recovery methods (e.g. new standby facilities or network technology);
- technology and practices, including new tools and techniques.

These should be evaluated to establish their potential benefit to the organization.