PD ISO/TS 22318:2015

BSI Standards Publication

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

bsi.

...making excellence a habit.™

National foreword

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 It supersedes PD 25222:2011 which is withdrawn.

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

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

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

Published by BSI Standards Limited 2015

ISBN 978 0 580 86362 2
ICS 03.100.01

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2015.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/TS 22318:2015

TECHNICAL SPECIFICATION

ISO/TS 22318

First edition
2015-09-01

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

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

Reference number
ISO/TS 22318:2015(E)

COPYRIGHT PROTECTED DOCUMENT

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

Contents

Page

Foreword

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

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

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

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

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

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

1 Scope

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

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

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

2 Normative references

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

ISO 22300, *Societal security — Terminology*

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

3 Terms and definitions

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

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

3.1 Terms included in ISO 22300

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

[SOURCE: ISO 22300:2012, 2.1.10]

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

[SOURCE: ISO 22300:2012, 2.2.6]

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,

— activity must be resumed, or

— resources must be recovered

Note 1 to entry: For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.

[SOURCE: ISO 22301:2012, 3.45]

3.2.12
resources
all assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objective

[SOURCE: ISO 22301:2012, 3.47]

3.3 Terms and definitions applicable to this Technical Specification

3.3.1
critical customer
individual or entity, the loss of whose business would threaten the survival of the organization

3.3.2
critical supplier
provider of critical products or services

Note 1 to entry: This includes an "internal supplier", who is part of the same organization as its customer.

3.3.3
critical products or services
resources obtained from a supplier which, if unavailable, would disrupt the organization's critical activities and threaten the survival of the organization

Note 1 to entry: Critical products or services are essential resources to support an organization's high priority activities and processes identified in its BIA.

3.3.4
disruption
event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organization's objectives

3.3.5
supply chain
network of organizations that are involved, through upstream and downstream linkages, in the processes and activities that produce value in the form of products and services in the hands of the ultimate consumer

3.3.6
supply chain continuity management
SCCM
application of business continuity management to a supply chain

Note 1 to entry: BCM should be applied to all the tiers of an organization's supply chain.

Note 2 to entry: In practice, an organization usually would only apply it to the first tier of their suppliers and influence critical suppliers to apply SCCM to their suppliers.

3.3.7
Tier 1 supplier
directly supplies products or services to the organization usually through a contractual arrangement

3.3.8
Tier 2 supplier
provides products or services to an organization indirectly and through a Tier 1 supplier

4 Why supply chain continuity is important

4.1 General

This Clause considers the factors which provide the structure within which SCCM is conducted. Supply chains are becoming increasingly complex, extended (often extending internationally) and frequently changing, exposing the organization to additional risk of supply chain interruption. As a supply chain is always subject to potential disruption, SCCM is required.

Usually, the customer-supplier relationship will be governed by contractual agreements including service level agreements (SLA) for external outsource arrangements and operational level agreements (OLA) governing internal service arrangements between the organization and the supplier but it may also be applicable to one time purchases.

4.2 Describing the supply chain

A broad view of a supply chain includes both the manufacturing and distribution of products and services, outsourcing and off-shoring. It is applicable to organizations of all types and sizes. Figure 2 illustrates a simple supply chain model.

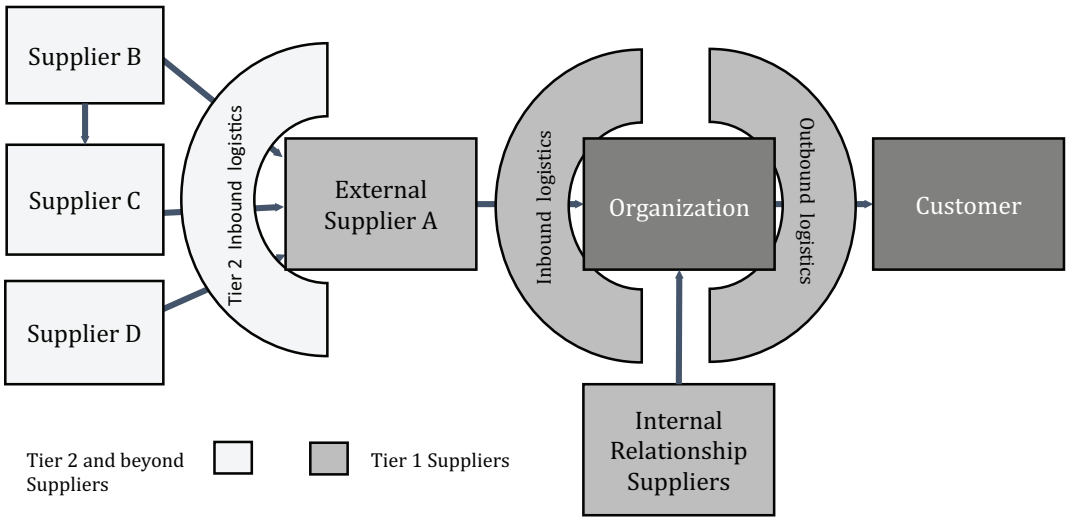

Figure 2 — Supply chain model

NOTE 1 Real supply chains will be more complex.

NOTE 2 External Supplier A could provide products or be an outsourced service.

NOTE 3 Internal suppliers include any relationship where the organization buys services or facilities from within its wider business group.

A supply chain exists where product or service delivery depends on inputs that are not under the direct management or control of the operating unit (the organization). It includes both internal and external

supply relationships. The relationships with the various suppliers vary with the degree of flexibility and the ability of the organization to control the relationship (see Figure 3).

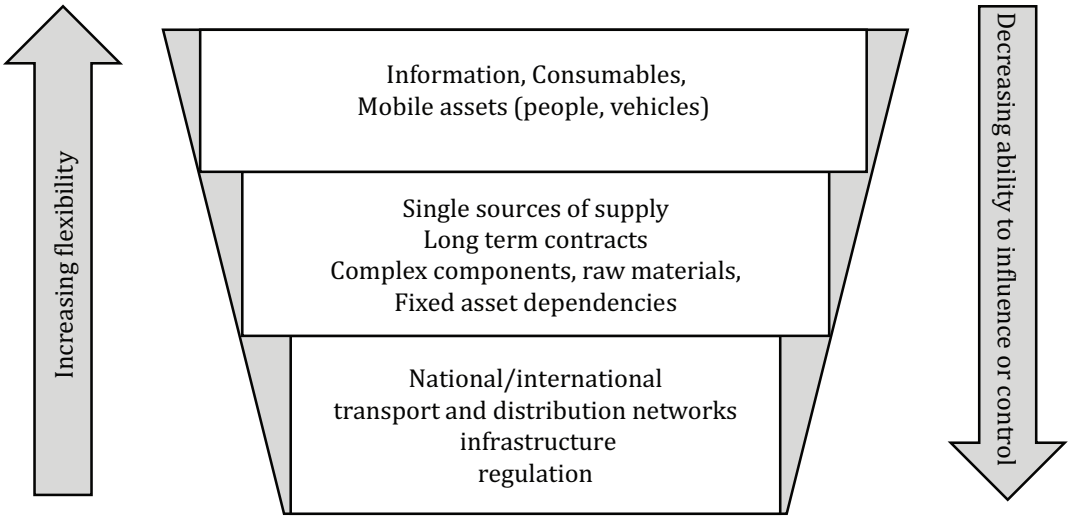

Figure 3 — Supply chain – Flexibility, influence and control

The range of potential customer relationship types includes the following:

— business-to-business (including distributors, wholesalers, etc.);

— business-to-consumer;

— third-party served (customers are served or supplied directly by subcontractors or agents).

The range of potential supplier relationship types includes the following:

— recurring product or service suppliers of components, raw materials, financing, property rental, essential fixed asset maintenance, etc.;

— one time or infrequent product or service suppliers (providing, for example, new capital equipment);

— outsourced or contracted service or business process suppliers (payroll bureau, IT services, contact centres, logistics or distribution);

— strategic partners/alliances (franchises, distributors and joint ventures);

— co-operative relationships or interdependencies between suppliers.

Other interested parties, in addition to customers and suppliers, might be involved and impacted by supply chain interruptions. Interested parties may include local communities such as the community from which the work force is drawn, informal community network members, trade bodies, contracted consortium partners, and partial competitors.

The factors upon which supply chain relationships may be based include the following:

— people and personal relationships;

— formal agreements such as contracts, work orders, service level agreements, and operating level agreements;

— information provided electronically or on paper such as purchase orders and design specifications;

— processes describing workflow, product/service creation and delivery;

— infrastructure such as transportation systems, Internet;

— cultural factors such as business networks, trading relationships;

— environment: political, economic, regulatory, etc.

NOTE This list provides examples only and is not intended to be complete.

4.3 Dynamics of supply chains

4.3.1 General

The supply chain is important to organizations of all types and sizes, particularly as they seek to reduce costs and enhance efficiency. Through reducing inventory, time and other inefficiencies, goods, services, information and money can move more efficiently, which in turn means that the impact of an interruption to the supply chain will be felt more acutely, sooner and more often. An increasing and significant proportion of costs lie within the supply chain, presenting both a risk and an opportunity. Poor supply chain management can destroy value and jeopardize brand and reputation.

Supply chains have extended beyond the organization's direct control, both in terms of geography and the number and type of suppliers. The drivers for this include the following:

— the global access at relative low cost provided by the Internet;

— the reduction of international trade barriers and the free movement of capital;

— the availability of educated and relatively low-cost skilled workers;

— the focus by the management of organizations on core, value-adding activities and a trend to outsource peripheral business processes, such as logistics, distribution, payroll, catering, cleaning, security and IT, makes organizations more interdependent;

— any global excess of demand over supply resulting in resource constraints where certain supplies, including some natural resources, are only available in some parts of the world.

As organizations become increasingly interconnected and interdependent and supply chains become more global in their reach, new vulnerabilities are created, exposure is increased and horizon scanning to identify changing risk profiles (see Clause 7) becomes more challenging. As supply chains become more integrated and lean, any event affecting one link may affect other links in the chain. The BIA should uncover interdependence across a supply chain but may not extend into the supply chain past Tier 1 (direct) suppliers with whom the organization has contractual relations to those in Tier 2, the direct suppliers to Tier 1 suppliers, and beyond.

4.3.2 Supplier and contract lifecycle

Suppliers and contracts exist within a lifecycle of supply and service acquisition, operation and discontinuation (see Figure 4). Entry into a new contract or renewing an existing contract presents an opportunity for the organization to influence future supplier behaviour through contract and/or service level changes. Conversely, long term contractual commitments and high supplier switching costs can shift the balance of power between the organization and its supplier, creating resistance to changing future supplier behaviour (see Figure 3). Implementing SCCM has to be achieved within this environment. The analysis of the supply chain (see Clause 5) will help to identify the high priority relationships and the requirements and opportunities for implementing SCCM.

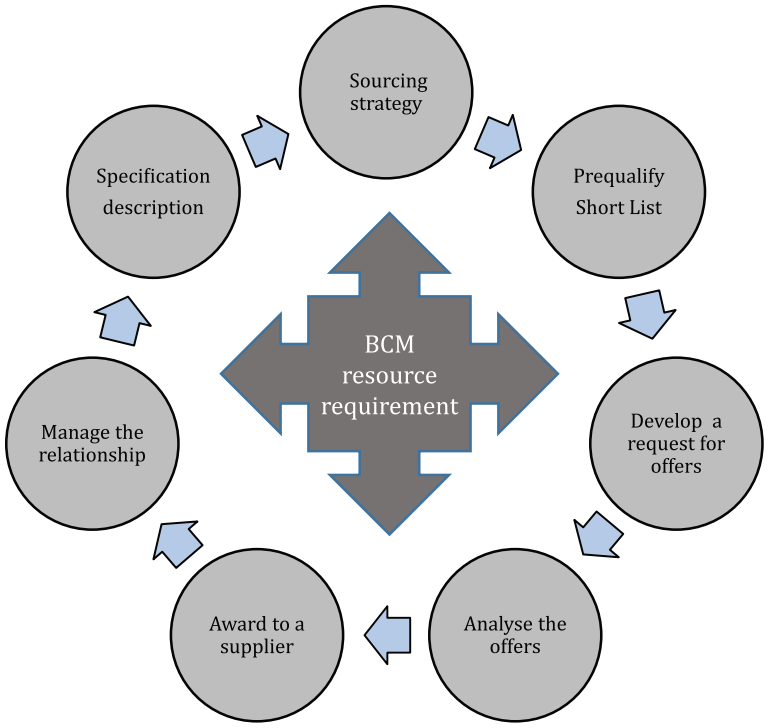

Figure 4 — Integrating SCCM into the supply chain lifecycle

4.3.3 Who owns the risk?

The organization retains the risk it might be unable to deliver its products or services to its customers as a consequence of a disruption in its supply chain and it is responsible for mitigating this risk by being prepared to respond to supply chain disruption. Customers hold the organization and not its suppliers responsible for failure to deliver products or services so an organization's brand is at risk of damage if there is a problem within its supply chain.

In extreme cases, a supply chain disruption could adversely affect an industry, market sector or the wider economy, government and public stakeholders.

4.4 The essentials for SCCM

The following are the essential requirements for effective SCCM:

— top management support for an integrated BCM and SCCM programme;

  — to set the priorities and standards required;

  — to allocate resources for conduct of the analysis;

  — to evaluate the impact of supply chain or individual supplier failure on the organization's high priority activities or processes;

— analysis to understand the organization's supply chain and the risk to the organization arising from its disruption;

— application of appropriate continuity strategies to each supplier;

— procedures for confirming that suppliers have appropriate continuity measures in place;

— a programme for supplier relationship management;

— a long-term strategy to build a more resilient supply chain.

4.5 Benefits of effective SCCM

Potential benefits of effective SCCM include the following:

— better understanding of the supply chain and potential threats;

— improved supplier relationship management to reduce the impact of supply chain disruption;

— improved response to supply chain disruptions resulting from effective collaboration with suppliers and customers;

— identification and mitigation of supply chain risks before they happen or before the organization is impacted;

— improved planning, due diligence, assurance and working relationships with suppliers;

— competitive advantage over competitors who do not have effective SCCM arrangements.

4.6 Challenges to effective SCCM

SCCM presents a number of challenges, including the following:

— scale and complexity, especially in large organizations with thousands of suppliers;

— distance and visibility of suppliers in the supply chain (geographic separation and number of tiers along the chain);

— persuading suppliers to participate openly and transparently because SCCM adds value to the relationship;

— inflexible contractual relationships making the service open to alteration less often;

— no structured approach describing where to start, how to proceed and how to overcome apathy or inertia;

— failure to develop the business case and to secure top management commitment and the necessary resources, including trained people;

— defining and embedding responsibility for SCCM across interested party functions within the organization and across organizations in the supply chain;

— balancing the expense of supply chain risk reduction and the long term payback with the short-term financial rewards of lower supply chain capital and operating costs;

— differences in risk tolerance/appetites between individuals, organizations and cultures;

— shortage of organization and supplier resources to implement preferred strategies;

— single and sole source suppliers;

— cultural differences including consideration of diversity issues;

— different regulatory requirements for the organization and the supplier;

— imbalance of power in the supply chain where a small organization is dealing with a larger supplier with multiple customers;

— obtaining confidence in product or service supply continuity arrangements from suppliers (might a supplier divert supplies to another customer in times of shortage?);

— difficulty in identifying indirect impacts such as when the loss of one supplier makes another supplier critical;

— difficulty understanding the full cost of disruption.

4.7 Key points of Clause 4: Why supply chain continuity is important

a) A supply chain exists wherever an organization's product or service delivery depends on inputs that are not under its direct management or control.

b) Supply chain continuity is important in an increasingly global, interconnected and fast-moving world, in which most organizations spend a significant proportion of their total costs via their supply chains, which are increasingly exposed to new and elevated risks.

c) Disruption to the supply chain can severely impact the ability of an organization to deliver its priority business processes.

d) Supply chains are frequently composed of a large number of suppliers organized in series (like a chain) or networks (like a web). These interrelationships and the transactions between them are dynamic.

e) There are many supply chain stakeholders or interested parties, both within and between organizations, which need to collaborate effectively during supply chain disruption.

f) The responsibility is on organizations (and not their suppliers) to mitigate their supply chain risk and respond to supply chain disruptions.

g) An organization shall manage the conflicting objectives of reducing supply chain cost and reducing supply chain risk.

h) A supplier needs to demonstrate continuity capability following a disruption, to reinstate, within an acceptable timeframe, the supply of product or service to an organization.

5 Analysis of the supply chain

5.1 General

Consistent analysis of all suppliers allows an organization to understand and assess the risk and potential impacts of a disruption in the supply chain. The supplier's criticality to the organization's activities and the level of risk to which they are exposed will determine the depth of analysis. Suppliers are responsible for extending the analysis process to their own supply chains and communicating the outcomes back to the organization.

5.2 Considerations for analysing the supply chain

The following are to be considered when conducting the analysis:

— the depth of analysis required to provide assurance that dependencies, risks and impacts have been identified and understood;

— use of a consistent, auditable approach that can be maintained over time;

— the cost/benefit;

— defining the organization's continuity framework and requirement for sourcing and ongoing supplier relationship management;

— integration of identified supply chain risks into the organization's risk management process;

— identification of the legal or regulatory constraints on the suppliers;

— results of the BIA.

5.3 Define the approach

The organization should identify its operational and environmental needs and consider them when conducting the analysis to ensure consistency across the organization and to create an approach that is sustainable over time. These should include the following:

— assessing supplier criticality, using a ranked approach. As an example, suppliers may be divided into two ranks as follows:

  — "critical": suppliers are those whose failure to deliver products or services on time or to quality or cost would significantly impact the ability of the organization to continue its high priority activities or processes and whose loss could jeopardize the survival of the organization;

  — "non-critical": suppliers, the loss of whose products or services could be tolerated for a limited period without adversely impacting the core activities of the organization;

— consideration of whether two ranks of supplier criticality is sufficient to provide a manageable structure for the programme or if a three ranked approach [strategic (business partners), core (suppliers who provide essential services or products), transactional (suppliers of routine non-critical products)] is required;

— analysis of the impact of an incident and its effect on a number of non-critical suppliers supplying the same product or service, at the same time;

— determination of acceptable business continuity requirements for suppliers:

  — what capability the organization expects for each category of supplier as minimum levels of supply including minimum business continuity objective (MBCO) and recovery time objectives (RTOs);

  — what evidence it requires from suppliers to demonstrate compliance/capability;

— the breadth and depth of analysis considering whether the analysis is to include all suppliers or only some suppliers based on their criticality and how far down the supply chain the analysis should be conducted;

— how frequently the analysis is to be repeated;

— how the requirements will be incorporated into current supplier relationship management and development of any future sourcing strategies.

The organization should fully document the approach and ensure it is agreed to by top management.

5.4 Structure of the analysis

The organization may adopt the following framework (see Figure 5):

— collate relevant, available documentation including the BIA, risk assessments and list of suppliers;

— define and document the approach to be used to assess supplier criticality, business continuity arrangements, including the parameters;

— conduct the analysis and risk assessment with each supplier;

— review the results of each supplier's analysis of its own supply chain;

— assess the overall level of risk from each supplier;

— share results with the suppliers and make improvement recommendations, agree an action plan and the process to monitor progress;

— include SCCM in the supplier relationship management process and allocate responsibilities for the periodic review;

— revise the level of risk to the organization from each supplier;

— complete an overall analysis of the supply chain comparing supplier continuity capability and supplier criticality.

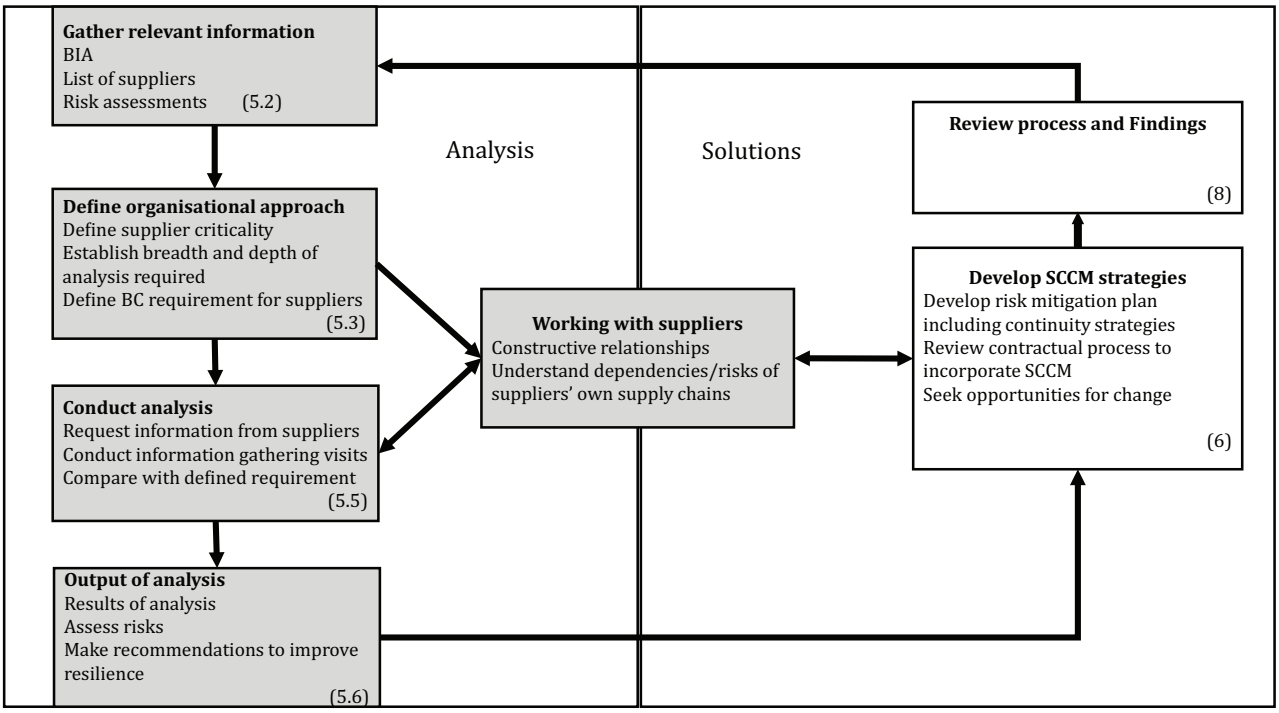

Figure 5 — SCCM flow chart

5.5 Conducting the analysis

The organization should share the rationale for the analysis and its potential benefits with suppliers explaining the organization's requirements and the expectations of each supplier.

The organization should identify the tiers of the supply chain (see Figure 2), drawing on information from the BIA to identify its high priority activities or processes, the MBCO and RTOs and the suppliers it depends on to meet them. The effect on the organization of any disruption to supply should be evident when the results of the BIA and the supply chain analysis are considered together.

The organization should evaluate for each supplier

— the criticality of the product or service they provide,

— whether this supplier is the only source for that product or service,

— the risk of disruption to their ability to deliver products and services to the organization,

— whether the supplier has effective business continuity arrangements in place,

— the extent to which the supplier has already assessed its own supply chain risks,

— the priority assigned to the organization by the supplier on its list of critical customers, and

— whether the supplier's MBCO/RTO is aligned with those of the organization for the activity or process they support.

An evidence-based approach to assessment of suppliers should be used to support maintenance of an SCCM including

— suppliers' documented BIAs, risk assessments and business continuity plans,

— suppliers' documented processes for maintaining and updating their continuity arrangements, and

— suppliers' documented exercise plans and post-exercise and post-incident reports.

For the most critical suppliers, review of documentation will rarely give sufficient confidence in the continuity capability and should be backed up with site visits and observation of exercises to validate documentation.

5.6 Output of analysis

The organization should ensure that output of the analysis is an auditable, evidence-based report for each supplier. At a minimum, the report should identify the following:

— the supplier's continuity arrangements and evidence that its BCM arrangements give confidence in their ability to recover within required MBCO/RTO;

— how these arrangements compare with the organization's expectations;

— how continuity in suppliers' supply chain is managed;

— threats to supply of the relevant product or service;

— recommendations for improvements.

5.7 Key points of Clause 5: Analysis of the supply chain

a) Supply chains are often broad, complex and interdependent, with multiple tiers.

b) It is essential to understand the supply chain and the risks it poses to the organization before selecting continuity strategies for supplies.

c) Any analysis should be undertaken jointly with suppliers, who in turn should be responsible for cascading the analysis to their suppliers.

d) The analysis should be based on a set of core criteria developed by the organization giving a common organizational approach.

e) These criteria should encompass the analysis process and the business continuity requirements for suppliers.

f) Key outputs from the analysis process include an overall assessment of the level of risk posed by the supply chain and by specific suppliers within it.

g) Supply chains are dynamic so business continuity requirements should be built into sourcing strategies and supplier relationship management processes.

h) The overall analysis process should be repeated periodically.

6 SCCM strategies

6.1 General

The organization should identify an appropriate SCCM strategy (see 6.2) for each supplier taking into account the challenges to SCCM identified in 4.6. The organization should use the results from the analysis (see 5.5) to identify the following:

— preferred suppliers;

— the impact on the business should the supply of product or services be disrupted;

— the criticality of each supplier and impact over time of disruption;

— an understanding of the continuity arrangements each supplier has in place both for itself and its own supply chain.

Strategy options are not mutually exclusive and mitigating the risk arising from an individual supplier may require more than one approach to be implemented. Achieving an optimum solution will take time; it may be necessary to adopt interim approaches with some suppliers until the opportunity arises to implement the preferred solution, particularly where the supply contract/agreement in place has a considerable time to run and there is limited opportunity to negotiate any change of conditions.

The organization should quantify the cost of disruption in terms of lost output, cost of customer compensation, likely scale of fines for breaching regulations, or price of purchasing alternative products or services to justify the cost of putting SCCM measures in place. The intangible costs of disruption, such as damage to reputation leading to loss of market share, loss of share value, or loss of competitiveness, so the case for implementing mitigation measures should also be considered.

6.2 Continuity strategy options

6.2.1 Option 1 — Accept status quo

This “Do Nothing” option may be suitable for non-critical suppliers. It might be appropriate to take out insurance to cover loss of profit (this is not a BC option as payments can lag significantly behind any incident and in some cases, they arrive too late to save the organization and are used merely to pay creditors).

6.2.2 Option 2 — Reduce dependency

The organization may reduce dependence on a supplier(s) by

— ensuring two or more sources of supply at all times (see Option 3),

— increasing stock holding on site or with distributors to lengthen the time before a disruptive event affects the organization, and

— establishing alternative solutions: pragmatic responses to managing risks arising from critical suppliers which the organization is unable to influence, e.g. providing a standby generator to cover for loss of power supplies or developing multichannel communications systems to reduce dependence on a single channel or supplier.

6.2.3 Option 3 — Increase resilience

The organization may develop recovery strategies which are independent of the supplier(s) by

— developing ways to mitigate loss of service by bringing the manufacture or delivery back into the organization (insourcing),

— identifying alternative suppliers able and prepared to meet the organization's demand at minimal notice, and

— establishing mutual support arrangements with competitors.

6.2.4 Option 4 — Work with the supplier

The organization may work with each supplier to improve resilience/recoverability by

— developing relationships and forming partnerships with critical suppliers based on mutual trust which will assist the organization to understand their arrangements and facilitate speedy recovery,

— defining the performance standard required and the process by which this will be assessed,

— helping and encouraging the supplier to improve its resilience, and

— including SCCM requirements into contract terms.

6.2.5 Option 5 — Ending the relationship

If a suitable provision for SCCM with a critical supplier cannot be found, consider ending the contractual relationship.

6.3 Including SCCM capability into a supply contract

The organization should include the continuity requirement within the sourcing process to ensure suppliers have adequate BCM arrangements for the product or service being provided in order to deliver SCCM over the longer term. Continuity requirements within the sourcing process include the following:

— defining the organization's BC requirement in the request for offers;

— seeking documentary evidence of BC arrangements and assessing the quality of the responses during the supplier selection process;

— establishing a standard contract clause to deliver the chosen continuity strategy to be applied immediately to new contracts and, at the earliest opportunity, for existing contracts;

— including escalation triggers and measures for notification and incident management in contract terms and service level agreements;

— specifying a requirement in contracts to notify key events and information, including invocations, plan reviews, exercises and document revisions;

— incorporating arrangements for joint exercises and sharing of learning points into contracts;

— requiring contracts include provisions for management review and/or audit of BC arrangements;

— encouraging suppliers to make visible their approaches to assessing the impact of disruption within their supply chains and the measures being taken to mitigate their supply chain disruption risk;

— requiring early notification of changes to the supply market which could jeopardize the BCM arrangements;

— specifying the effect on contracts of not achieving required SCCM criteria such as an escalation process and potential contract termination;

— limiting force majeure clauses that can be invoked by the supplier instead of implementing effective SCCM arrangements.

NOTE Force majeure is a clause commonly included in contracts that free both parties from liability or contractual obligation when an extraordinary event or circumstance beyond the control of the parties occurs. An extraordinary event or circumstance may be a war, strike, riot, crime, or an event legally described as an act of God such as hurricane, flooding, earthquake, or volcanic eruption. Most force majeure clauses do not excuse a party's non-performance entirely but only suspends it for the duration of the force majeure.

6.4 Ownership of SCCM

The organization should identify those with responsibility for supplier relationship management and for securing and monitoring supply chain continuity assurance. The responsibility should be closely linked to the wider arrangements for BCM within the organization.

The organization should require that the responsibility for managing the SCCM is turned over by those who bought the products or services (purchasing) to those who are going to manage the contract or run operations.

The organization should ensure that the control measures put in place do not degrade over time. For example, having placed contracts with two suppliers to achieve resilience, it is important to guard against the number of suppliers being reduced to one as a cost-saving measure.

6.5 Key points of Clause 6: Considering options: developing strategies

a) There is a range of potential strategies for building greater resilience in the supply chain. The choice of the best strategy(ies) depends on identifying and highlighting the most critical suppliers.

b) Where cost effective, choose strategies which allow the organization to reduce the impact of disruption independently of the supplier, e.g. setting up more than one source of supply and/or increasing stockholding of resources.

c) Where it is not possible to mitigate the impact independently of the supplier, a continuity solution should be developed in cooperation with the supplier.

d) The requirement for suppliers to put in place an effective business continuity solution for themselves and their supply chain needs to be incorporated within the supply contract. Critical suppliers need to provide evidence of this both at the time the contract is awarded and as part of ongoing performance evaluation.

e) The contract/agreement needs to define information exchange and plan invocation procedures to be used between suppliers and customers.

f) It is necessary to recognize that it will take time to implement the best possible approach and that it might be necessary to accept partial solutions to mitigate the risk in the short to medium term.

7 Managing a disruption in the supply chain

7.1 General

Having conducted the analysis of the supply chain as defined in Clause 5 and put appropriate strategies in place in accordance with Clause 6, the organization should ensure that appropriate processes are in place to manage any disruption.

It is important to maintain engagement with critical suppliers to ensure continuity management arrangements are available and effective. This is best achieved through supplier relationship management by ensuring regular and open discussion between the parties to create a partnership between the organization and the supplier.

It is easy to make assumptions about how each side will respond in the event of an incident; these assumptions need to be validated.

7.2 Before an incident happens

The organization should include the following in its business continuity plans:

— limitations or changes arising from a supplier disruption affecting the organization such as interruption in the supply of goods or services;

— supplier's expectation of support from the organization;

— the action plan for the organization's immediate response.

The organization should

— invite suppliers to take part in BC exercises that relate to the products/services they supply,

— help suppliers to understand the criticality of the supply of their goods and services and enable them to identify any delivery issues in supplying to an alternative site,

— attend supplier exercises relating to the products/services supplied to it to gain objective assurance of the supplier's ability to continue to supply in the event of an interruption,

— use horizon scanning to alert the organization to emerging risks which may affect the supply chain, and

— consider the indirect effect of disruptions caused by external events such as a transport disruption caused by a fuel shortage brought on by industrial action or movement restrictions imposed by a disease outbreak.

7.3 Incident detection and notification

Early detection of a disruptive event enables an effective, timely and appropriate response. This requires that the organization maintains an open relationship with suppliers, encouraging them to raise issues immediately and to identify any problems and the potential impact on the supply of products or services to the organization.

Where the relationship is less transparent, the supplier may be reluctant to inform customers of a disruption or potential disruption due to optimism about its ability to resolve problems without impact to the customer. The impact of delayed notification potentially increases the risk of a minor problem becoming a major issue for the organization. This is particularly true if the supplier does not have a full understanding of their importance to the affected activity.

7.4 During an incident

The organization should consider the following factors during an incident:

— coordinating incident management between a critical supplier and the organization to reduce the likelihood of wrong assumptions about the supplier's response and to minimize the impact to the organization;

— any impact arising because of the supplier's operating location with respect to geography, cultural or political differences;

— procedures for regular communication with the supplier throughout the incident about the current situation and the return to normal working conditions;

— the supplier's approach to external communications to avoid "mixed messages" being released and any consequential reputational damage;

— the reciprocal nature of the arrangement where the organization is the source of the incident and suppliers need to manage their own business operations affected by disruption and also to provide support to facilitate the organization's recovery.

7.5 Return to business as usual

Returning to business as usual will take time and will need the organization to coordinate activities with suppliers whose operations have been affected.

The organization should take the opportunity to learn lessons from the disruption and make improvements both to lessen the impact of future events on the supplier and the organization and to improve the information flow between suppliers and the organization.

The organization should manage suppliers' concerns about sharing sensitive information with other suppliers involved in the review and deal with suppliers who are reluctant to accept follow-up actions without changes to contracts and consequent charges.

The organization should require where possible access to information on the actions resulting from the incident and track progress toward their completion.

7.6 Key points of Clause 7: Managing a disruption in the supply chain

a) Include details of supply chain continuity management arrangements into BC Plans.

b) Exercise with suppliers to improve coordination and understanding of each other's issues.

c) Ensure there is an agreed procedure in place for suppliers to alert the organization to incidents or potential incidents as early as possible.

d) During an incident, ensure that command and control is integrated.

e) Coordinate external communications plans.

f) Post event conduct a thorough, shared review of what happened, the lessons to be learnt and the resulting improvement actions.

8 Performance evaluation

8.1 General

The organization should undertake performance evaluations with its critical suppliers at agreed intervals as part of routine supplier relationship management.

The performance evaluation should cover the ongoing management of the SCCM and include monitoring, verification, validation and review of SCCM arrangements to stimulate continuous improvement and provide assurances in the supply chain.

Monitoring and review help to ensure that critical suppliers continue to have in place robust business continuity arrangements by

— utilizing the regular meetings with suppliers to gain an early understanding of any changes to the supplier's operation or their continuity plans that relate to the goods or services provided,

— monitoring supply chain performance and identifying potential issues,

— establishing escalation triggers and procedures for suppliers to report failures,

— identifying any "hidden" risks with its critical suppliers in the event that they suffer a disruption, and

— facilitating the alignment of suppliers' MBCO and RTO with the requirements of the organization.

8.2 Engaging with suppliers

The organization should include SCCM assurance as an item for regular discussion with suppliers through

— inclusion on the agenda for supplier review meetings,

— shared education and training tools,

— the sourcing strategy,

— monitoring of performance metrics,

— exercising of incident plans,

— well-rehearsed trigger and escalation plans,

— shared understanding of command and reporting structures in the event of an incident, and

— collaborative exercise programmes.

8.3 Implementing an SCCM performance evaluation programme

The organization should maintain an SCCM performance evaluation programme which includes the following:

— review of the organization's criteria for the SCCM capability required from suppliers; this will depend on the assessment of supplier criticality and the chosen BCM strategy for each supplier;

— an assurance process that includes the following:

  — maintaining the analysis (see 8.4);

  — ongoing monitoring using key performance indicators (KPIs)/metrics;

  — design and use of questionnaires/checklists/self-evaluation;

  — use of an escalation process when suppliers do not meet the criteria;

  — review of the organization's procurement process to ensure BCM requirements are included;

  — review of standard SCCM contract and schedule clauses to ensure they continue to meet the organization's needs;

— the inclusion of the right to carry out performance evaluation in the contracts and agreements. If the right to undertake performance evaluation is not in the agreement, it should be added, if possible.

8.4 Maintaining the analysis

The supply chain and the risks it faces are always changing. To maintain its SCCM, the organization should

— establish a repeatable process to analyse the supply chain and monitor changing risks,

— keep the analysis up-to-date and identify opportunities for continuous improvement,

— implement a continuous review process to monitor supply chain changes and implementation of improvements,

— identify individuals responsible for the review process and for incorporating it into the existing supplier relationship management process,

— build SCCM requirements into sourcing strategy, and

— include the supplier SCCM performance evaluation process into the scope of BCM audits.

8.5 Outcomes of performance evaluation

Performance evaluation should be outcome-focused. When assessing a supplier's ability to meet the organization's requirements, the following should be examined:

— supplier's documented BIAs, risk assessments and business continuity plans;

— documented processes for maintaining and updating suppliers' continuity plan;

— supplier's exercise plans and post-exercise and post-incident reports;

— documented notification process is in place that includes key organizations likely to be impacted;

— documented communications plan that includes joint communications and statements that take into consideration the organizations impacted.

The following are the benefits of the process:

— 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 each supplier meets the organization's BCM requirements;

— early indication of changes likely to affect the supply relationship;

— identification of gaps in capability which the supplier needs to address;

— supplier monitoring and performance measurement against targets.

The organization should review the relationship and/or the SCCM strategy (see Clause 6) when there are significant issues with a supplier's BCM arrangements.

In conducting performance evaluation, the organization should take the following into account:

— a supplier may have many customers who wish to validate their BCM and this could be both costly and disruptive to the supplier;

— performance evaluation is an indicator that provides a view at a particular point in time so the programme needs to be reviewed regularly;

— the potential that the performance evaluation process and implementing remedial actions could result in increased costs.

8.6 Key points of Clause 8: Performance management

a) The responsibility is on the organization to ensure that SCCM provisions required to protect its high priority activities or processes are maintained.

b) Owners of supplier relationships need to have appropriate triggers and escalation pathways in place to alert and deal quickly with changes to critical supplier performance.

c) Regular engagement with suppliers through review meetings is essential to maintaining the supplier relationship.

d) Including suppliers in exercises can highlight previously unknown risks which can be added to an action log for both to work through.

e) Performance evaluation includes monitoring, verification, validation and review of SCCM arrangements, stimulates continuous improvement and provides performance evaluation in the supply chain.

Bibliography

[1] ISO 28000, *Specification for security management systems for the supply chain*

[2] ISO 28002, *Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use*

[3] ISO 22313:2012, *Societal security — Business continuity management systems — Guidance*

[4] ISO 31000, *Risk management — Principles and guidelines*

[5] BS PAS 7000:2014, *Supply chain risk management — Supplier prequalification*

[6] BS 65000:2014, *Guidance on organizational resilience*

[7] BS 13500:2013, *Code of practice for delivering effective governance of organizations*

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™