PRIVATE CIRCULATION
BCM/1_15_0003
For comment/vote - Action Due Date: 2015/02/13

DRAFT TECHNICAL SPECIFICATION OR TECHNICAL REPORT

Proposed ISO/DTS 22318	
Date 2015-01-12	Reference number **ISO/TC 292 N 15**
Supersedes document	

WARNING: This document is not approved. It is distributed for review and comment. It is subject to change without notice.

ISO/TC 292

Title

Security

Secretariat

SIS

Circulated to P- and O-members, and to technical committees and organizations in liaison for:

☐ discussion at
[venue/date of meeting]

☒ comments by 2015-03-06
[date]

☒ approval for publication as a Technical Specification or Technical Report (as indicated below) by

2015-03-06
[date]

(P-members vote only: ballot form attached)

P-members of the technical committee or subcommittee concerned have an obligation to vote.

Title (English)

Societal security – Business continuity management – Guidance on supply chain continuity

Title (French)

Proposed Technical Specification ☒ or *Technical Report* ☐

Reference language version: ☒ English ☐ French ☐ Russian

Introductory note

Copyright notice

This ISO document is copyright protected by ISO. While reproduction in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed to the secretariat indicated above or to ISO's member body in the country of the requester.

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

© ISO – All rights reserved

1 **ISO/TC 292**

2 Date: 2015-01-12

3

4

5

6 Societal security – Business continuity management — Guidance on 7 supply chain continuity

TS 22318 -CD1- Committee Use Only

© ISO 2013 – All rights reserved

Contents

TS 22318-CD1- Committee Use Only

© ISO 2013 – All rights reserved

TS 22318-CD1- Committee Use Only

© ISO 2013 – All rights reserved

Foreword

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

- An ISO/IEC Publicly Available Specification (ISO/IEC PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

- An ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

lSO/TS 22318 has been prepared by Technical Committee ISO/TC 292, *Security*, Working Group 5, *Resilience and continuity*.

TS 22318 -CD1- Committee Use Only

© ISO 2013 – All rights reserved

Introduction

This Technical Specification (TS) expands the business continuity guidance given in ISO 22301 and ISO 22313 on establishing appropriate levels of continuity management within an organisation's supply chain. It assumes that the organisation seeking to establish Supply Chain Continuity Management (SCCM) is already 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 organisation of suppliers of products or services which do not have adequate continuity arrangements in place.

This guidance is intended primarily to assist anyone buying, managing or responsible for a product or service necessary to an organisation's critical products or services to implement good business continuity practice in line with established standards.

Supply chain management considers the full range of activities concerned with purchase and provision of supplies or services to an organisation as a part of business-as-usual. The scope of this document is less broad in that it specifically considers the issues faced by an organisation which needs continuity of supply of products and services to protect its critical business activities or processes, and the strategies which can be used to mitigate the impact of disruption in the supply chain; this is SCCM. SCCM depends upon business impact analysis (BIA) to identify critical business activities and processes and thus is closely linked with ISO/TS 22317 which provides guidance on conducting a BIA.

Organisations rely on suppliers to deliver critical products or services on time and to agreed quality or standards. It is important, therefore, for an organisation, as part of its wider approach to Business Continuity Management to recognise the potential impact on its activities of a disruption within its supply chain. Failure to deliver a product or service by a supplier may trigger a business disruption event. There are however, conflicting objectives to be managed of maintaining and reducing supply chain cost (for example, by reducing cycle times and buffer stock) while managing the supply chain risk arising from single source and just in time supply approaches.

This TS is relevant to the supply of products and services from external suppliers and internal relationships within divisions of the same organisation, under any type of continuing supplier relationship. It also has applicability to single 'one-off' procurement events such as purchases of long lead items for a major project where failure to deliver could impact the future development of the organisation.

The TS recommends classifying suppliers according to their criticality, which considers the impact on the organisation of a disruption to the supplied products or services, and "supplier tier", which defines the relationship with the organisation (i.e. a tier 1 supplier has a direct contractual relationship with the organisation, while a tier 2 supplier supplies products and services to a tier 1 supplier). This TS recognises that between tiers the same supply chain continuity considerations apply. Tier 1 suppliers would be responsible for assuring their own supply chain relationships; recognising that the customer may need visibility of these relationships both to ensure there is adequate resilience in the supply chain and to take account of factors such Corporate Social Responsibility concerns which may require the customer to understand the end to end supply chain.

The TS focuses on identifying and managing the risks and impacts arising within an organisation from failure of a critical supplier to that organisation The guidance, however, also has relevance to the supplier both so that they can prepare to meet the business continuity expectations of their customer who is dependent upon them, and also to consider vulnerabilities which might arise from dependence on a single customer.

This TS recognises that suppliers may also comply with the requirements of the ISO 28000 series of standards which establish standards for security management within the supply chain. Conformance with these standards will give organisations purchasing goods or services further confidence in the resilience of their supply chain, and potentially reducing the risk of disruption.

The text is mapped to the elements of business continuity management, see Figure 1.

ISO/TS 22318:CD - Committee use only

© ISO 2013 – All rights reserved

1

Element	Clauses in ISO/TS 22318
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

2 **Figure 1 – Elements of business continuity management (BCM) – see ISO 22313 Figure 5**

3

4

TS 22318 _CD1- Committee only

© ISO 2013 – All rights reserved

Societal security – Business continuity management — Guidance on supply chain continuity

1 Scope

This Technical Specification (TS) gives guidance on continuity management within the supply chain. Guidance is given on practical methods for understanding and extending the principles of business continuity management (BCM), as embodied in ISO 22301 and ISO 22313, to the management of supply relationships. This TS addresses relationships throughout the supply chain, between suppliers and customers. The guidance is generic and intended to be applicable to all organisations (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. Usually there will be an ongoing relationship governed by contractual agreements (including Service Level Agreements (SLA) for external outsource arrangements and Operational Level Agreements (OLA) governing internal service arrangements) between the organisation and the supplier but it may also be applicable to single event relationships, for example if there is a long lead time (i.e. a significant time gap between placing the order and delivery of the good or service). The extent of application of the guidance depends on the organisation's operating environment and complexity.

The TS does not give guidance on developing a business continuity plan or business continuity management system which is the subject matter of the parent standards ISO 22301 and ISO 22313.

2 Normative references

No normative references are applicable to this document. Important source documents are listed in the Bibliography. This clause is included to retain clause numbering similar to other management standards.

3 Terms and definitions

3.1 Terms included in ISO 22300

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

3.1.1
business continuity

3.1.2
business impact analysis

3.1.3
event

3.1.4
exercise

3.1.5
incident

3.1.6
mutual aid agreement

© ISO 2013 – All rights reserved

3.1.7
prioritised activities

3.1.8
risk

3.1.9
top management

3.2 Terms defined in this Technical Specification

The following Terms and Definitions are applicable to this technical specification:

3.2.1
activity
process or set of processes undertaken by an organisation (or on its behalf) that produces or supports one or more products and services

Note 1 to entry: Such processes include accounts, call centres, IT, manufacture, distribution.

3.2.2
business continuity management
holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organisational 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]

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 organisational structure, policies, planning activities, responsibilities, procedures, processes and resources.

[SOURCE: ISO 22301]

3.2.4
business continuity plan
documented procedures that guide organisations 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]

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]

3.2.6
critical customer
a customer the loss of whose business would jeopardize the survival of the organisation

© ISO 2013 – All rights reserved

3.2.7
critical supplier
provider of critical products or services

Note 1 to entry: This includes an “internal supplier”, which is a supplier that is part of the same organisation as its customer.

3.2.8
critical products or services
products or services, obtained from a supplier, which if unavailable would disrupt the organisation’s critical activities and would jeopardize the survival or the organisation.

3.2.9
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 organisation’s objectives

3.2.10
interested party - stakeholder
person or organisation 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 organisation.

[SOURCE: ISO 22301]

3.2.11
organisation
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 organisation 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 organisations with more than one operating unit, a single operating unit can be defined as an organisation.

[SOURCE: ISO 22301]

3.2.12
outsource (verb)
make an arrangement where an external organisation performs part of an organisation’s function or process

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

Note 2 to entry: An outsource provider is a supplier of a product or service within the context of SCCM. Any threat which could lead to a disruptive event affecting the outsource provider is a risk to the organisation.

[SOURCE: ISO 22301]

3.2.13
products and services
beneficial outcomes provided by an organisation to its customers, recipients and interested parties, e.g. manufactured items, car insurance and community nursing

© ISO 2013 – All rights reserved

[SOURCE: ISO 22301]

3.2.14
resources
all assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organisation has to have available to use, when needed, in order to operate and meet its objective

[SOURCE: ISO 22301]

3.2.15
supply chain
network of organisations that are involved, through upstream and downstream linkages, in the different processes and activities that produce value in the form of products and services in the hands of the ultimate consumer

[SOURCE: Christopher 1998]

3.2.16
supply chain continuity management (SCCM)
application of business continuity management to the supply chain

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

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

3.2.17
supplier tier
measure of the distance of a supplier from the organisation

Note 1 to entry: A tier 1 supplier directly supplies products or services to the organisation usually through a contractual arrangement. A tier 2 supplier provides products or services to an organization indirectly and through a tier 1 supplier.

3.2.18
supplier criticality
result of an assessment to identify suppliers whose failure to deliver contracted products or services would significantly impact on the organisation; failure of a critical supplier to deliver products or services in accordance with an agreement would and materially affect the ability of the receiving organisation to conduct its business

Note 1 to entry: The organisation needs to define the criteria to be used when evaluating the criticality of suppliers

4 Why supply chain continuity is important

4.1 Introduction

This clause considers the factors which provide the structure within which SCCM is conducted. Supply chains are becoming increasingly complex and extended (often extending internationally), exposing the organisation to new and additional risk of supply chain interruption. In addition, the supply chain can be in a state of change. A supply chain is always subject to potential disruption, hence the requirement for SCCM.

© ISO 2013 – All rights reserved

4.2 Describing the supply chain

For the purpose of this document a broad view of a supply chain is considered which includes both the manufacturing and distribution of products, and services, outsourcing and off-shoring. It is applicable to organisations of all types and sizes. Figure 2 provides a simple supply chain model.

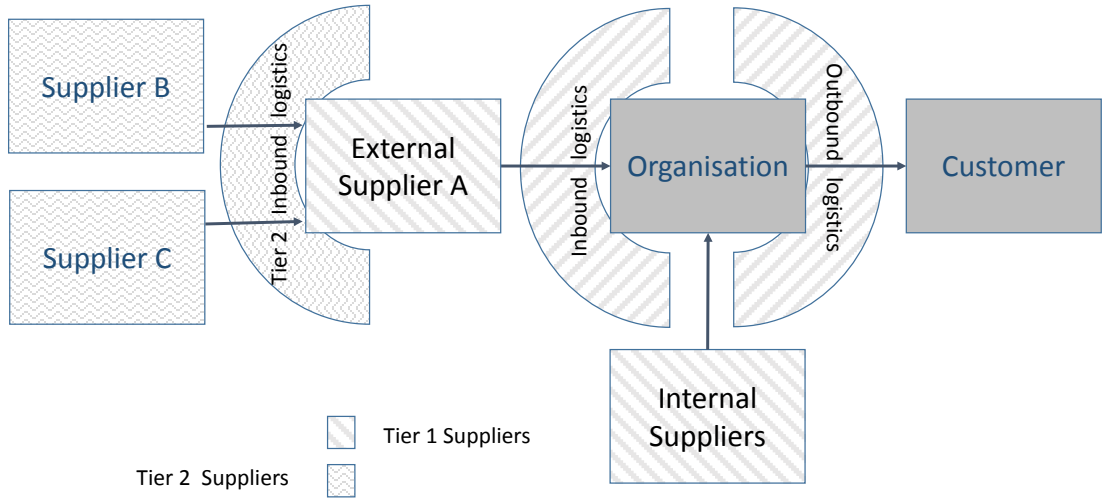

Figure 2 – Supply chain model

A supply chain exists wherever a product or service delivery depends on inputs that are not under the direct management or control of the operating unit (the organisation). 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 organisation to control the relationship, see Figure 3.

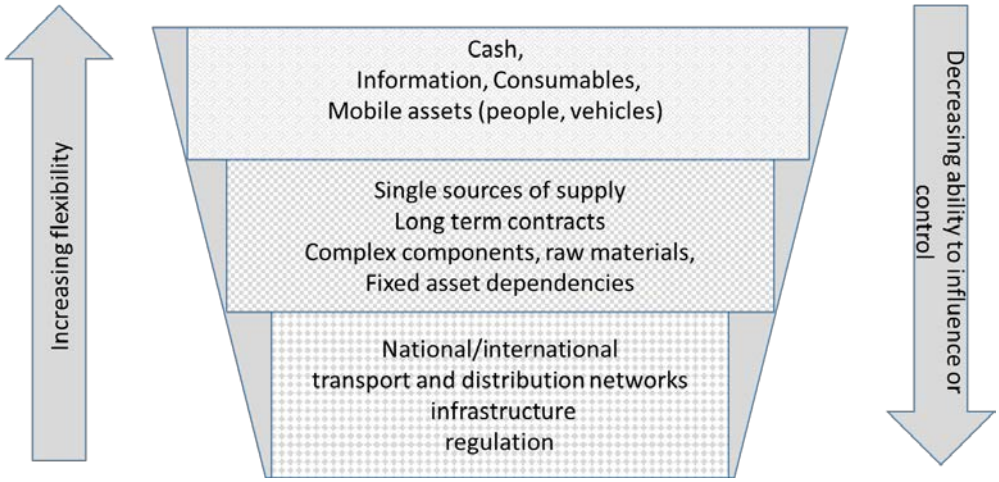

Figure 3 – Supply chain influence and control

There is a range of potential customer relationship types, including:

- business-to-business (some of whom may be distributors, wholesalers, etc.);
- business-to-consumer; and

© ISO 2013 – All rights reserved

- third-party served (where customers are served or supplied indirectly, for example, via subcontractors or agents).

There is also a range of potential supplier relationship types, including:

- recurring product or service suppliers (providing components, raw materials, financing, property rental, essential fixed asset maintenance, etc.);
- one-off or infrequent product or service suppliers (perhaps to provide a new piece of capital equipment);
- outsourced or contracted out (off-site service or business process providers, such as payroll bureau, IT services, contact centres, logistics or distribution);
- strategic partners (such as franchises, distributors and joint ventures); and
- co-operative relationships or interdependencies between suppliers.

In addition to customers and suppliers, other stakeholders might be involved in and impacted by supply chain interruptions, including local communities (for example, the community from which the work force is drawn), informal community network members, trade bodies, contracted consortium partners, partial competitors or “buddies” with reciprocal arrangements, etc.

Supply chain relationships may be based on a number of factors, including:

- people: personal relationships;
- formal agreements: contracts, work orders, service level agreements, operating level agreements, etc.;
- information: electronic or paper; purchase orders, design specifications;
- processes: workflow; product/service creation and delivery;
- infrastructure: transportation systems, Internet;
- culture: business networks, trading relationships; and
- environment: political, meteorological, economic (e.g. foreign exchange rates), etc.

NOTE These are examples only and the list is not intended to be exhaustive.

4.3 Dynamics of supply chains

4.3.1 General

The supply chain is important to organisations of all types and sizes, particularly as organisations seek to lower cost and enhance efficiency. Driving out inventory, time and other forms of “waste” means that goods, services, information and money are moving faster, 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 for many organisations, presenting both a risk and an opportunity. Poor supply chain management can destroy value and jeopardize brand and reputation.

A number of drivers have enabled and accelerated the extension of supply chains well beyond the organisation’s direct control, both in terms of geographical spread and the number and type of suppliers, including:

© ISO 2013 – All rights reserved

- the rise and development of the Internet, its global accessibility and relatively low cost;
- the reduction of international trade barriers and the free movement of capital;
- the addition of hundreds of millions of educated and relatively low-cost skilled workers;
- a management trend for organisations to focus on core, value-adding activities and outsource an increasing range of peripheral business processes, such as logistics, distribution, payroll, catering, cleaning, security and IT, making organisations more interdependent and extending impact of disruption across entities; and
- the emergence of resource constraints as global demand exceeds supply, so that certain supplies, including some natural resources, are only available in particular parts of the world.

Organisations are therefore increasingly interconnected and interdependent. As supply chains become more global in their reach, new vulnerabilities are created and exposure is increased, while horizon scanning to identify changing risk profiles (see Clause 7) becomes more challenging. Furthermore, as supply chains become more integrated and lean, the more likely it is that any event affecting one link may ripple through, affecting other links in the chain. Business impact analysis should uncover interdependence across a supply chain, but often does not extend into the supply chain past Tier 1 (direct) suppliers (those with whom the organisation has contractual relations) to those in Tier 2 (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. The point of entering into a new contract or renewing an existing contract presents the organisation with an opportunity to influence future supplier behaviour through contract and/or service level changes. Conversely, longer-term contractual commitments and high supplier switching costs can shift the balance of power between the organisation and its supplier, creating resistance to changing future supplier behaviour. (Figure 3). Implementing SCCM has to be achieved within this environment. The analysis of the supply chain (Clause 5) will help to identify both the critical relationships and the requirements for, and opportunities to implement SCCM.

4.3.3 Who owns the risk?

The fact that the organisation might be unable to deliver its products or services to its customers as a consequence of a disruption in its supply chain is a risk that the organisation itself retains. The onus is therefore on the organisation to mitigate this risk in line with its risk management policy and approach and be prepared to respond to supply chain interruptions. Customers (backed by legislation) expect the organisation to take responsibility for its supply chains and can be expected to hold the organisation (rather than its suppliers) responsible for failure to deliver products or services. Therefore, an organisation's brand is at risk of damage in the event of a problem in its supply chain or by the actions of a supplier.

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

4.4 The essentials for SCCM

The essential requirements for effective SCCM are:

- top management support for an SCCM initiative/project to set the priorities and standards required; to allocate resources for conduct of the analysis; and to evaluate the impact of supplier/supply failure on the organisation's critical activities;
- analysis to understand the organisation's supply chain and the risk to the organisation arising from its disruption;

© ISO 2013 – All rights reserved

- establishing continuity strategies to be applied to each supplier;
- procedures for gaining assurance from suppliers that appropriate SCCM is in place;
- a programme for ongoing management; and
- a long-term strategy to build a resilient organisation.

4.5 Benefits of effective SCCM

Potential benefits arising from effective SCCM include:

- mapping of the supply chain gives a better understanding of where and how to improve the organisation's supplier management, which in turn can increase efficiency and reduce the likelihood and impact of supply chain interruptions;
- improved response to supply chain interruptions, including more effective collaboration with suppliers and customers;
- more frequent identification and mitigation of supply chain risks before they happen or before the organisation is impacted;
- improved business-as-usual supplier management, planning, due diligence, assurance and working relationships with suppliers; and
- the organisation can gain new customers by distinguishing itself from competitors who do not have in place effective SCCM arrangements.

4.6 Challenges to effective SCCM

Supply chain continuity management presents a number of challenges, including:

- scale and complexity (especially large organisations that can have many thousands of suppliers);
- distance and visibility of suppliers in the supply chain (geographic separation and number of links along the chain);
- convincing suppliers that SCCM adds value to the relationship and persuading them to participate openly and transparently;
- existing contractual relationships might present infrequent "moments of change" when the service is open to alteration;
- lack of structured approach (to determine where to start, how to proceed and overcome apathy or inertia);
- lack of business case, top management commitment and necessary resources, including trained people;
- defining and embedding responsibility for SCCM across stakeholder functions within the organisation, and between organisations in the supply chain;
- striking a balance between the expense of supply chain risk reduction that pays off over a longer time period and the short-term financial rewards of lower supply chain capital and operating costs in "business-as-usual";

© ISO 2013 – All rights reserved

- differences in risk tolerance/appetites between individuals, organisations and cultures;
- shortage of resources to implement preferred strategies(both for the organisation and the supplier);
- cultural and legal differences including consideration of diversity issues;
- balance (or lack) of power in the supply chain (such as a small organisation dealing with a much larger supplier with multiple customers);
- obtaining firm and meaningful product or service supply continuity commitments from suppliers (might a supplier divert supplies to another more important customer in times of shortage?);
- difficulty in identifying indirect impacts: the loss of one supplier can make another critical; and
- difficulty understanding the full cost of disruption.

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

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

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

3) Disruption to the supply chain can severely impact the ability of an organisation to deliver its critical business processes.

4) 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 subject to constant change.

5) There are many supply chain stakeholders or interested parties, both within and between organisations, which need to collaborate effectively during supply chain stress situations if continuity is to be achieved.

6) The onus is on organisations (and not their suppliers) to mitigate their supply chain risk and respond to supply chain interruptions.

7) Within an organisation conflicting objectives must be managed of reducing supply chain cost (for example, by reducing cycle times and buffer stock) and reducing supply chain risk.

8) What matters is a supplier's demonstrated continuity capability to reinstate the supply of product or service to an organisation and its commitment to supply that organisation rather than another.

5 Analysis of the supply chain

5.1 Introduction

Analysis of the supply chain allows an organisation to understand and assess the risk to their operation of a disruption in that supply chain. Achieving consistency in approach is central to the analysis. The depth of analysis of any given supplier needs to reflect their criticality to the organisation's activities and the level of risk to which they are exposed.

Suppliers are responsible for cascading the process of analysis to their own supply chains and communicating the outcomes back to the organisation.

© ISO 2013 – All rights reserved

5.2 Considerations for analysing the supply chain

In carrying out the analysis, the following need to be considered.

a) Depth of analysis required to provide assurance that dependencies and risks have been identified and understood.

b) Developing an approach which is consistent, auditable and can be maintained over time.

c) Cost/benefit analysis of the process

d) Setting standards and a framework which can be incorporated into procurement and ongoing supplier management processes.

e) Including risks identified into the organisation's risk management process.

f) identifying any legal or regulatory constraints on the suppliers.

5.3 Structure of the analysis

5.3.1 General

An organisation may adopt the following broad structure, see Figure 4.

a) Assemble relevant documentation currently available within the organisation, e.g. business impact analyses, risk assessments and supply chain map.

b) Define and document the approach, including defining parameters which will be used to assess supplier criticality, business continuity requirements, etc. (see 5.3.2).

c) Define a supplier engagement plan and allocate responsibilities for the review and completion timescales.

d) Undertake the analysis and risk assessment with each supplier.

e) Assess the overall level of risk from each supplier.

f) Share results with the appropriate supplier (gap analysis), make improvement recommendations, agree an action plan and the process to monitor progress.

g) Review the results of suppliers' analyses of their own supply chain.

h) Revise the level of risk from each supplier based on this and any common dependencies between suppliers.

i) Produce an overall analysis of the supply chain mapping supplier capability against their criticality.

© ISO 2013 – All rights reserved

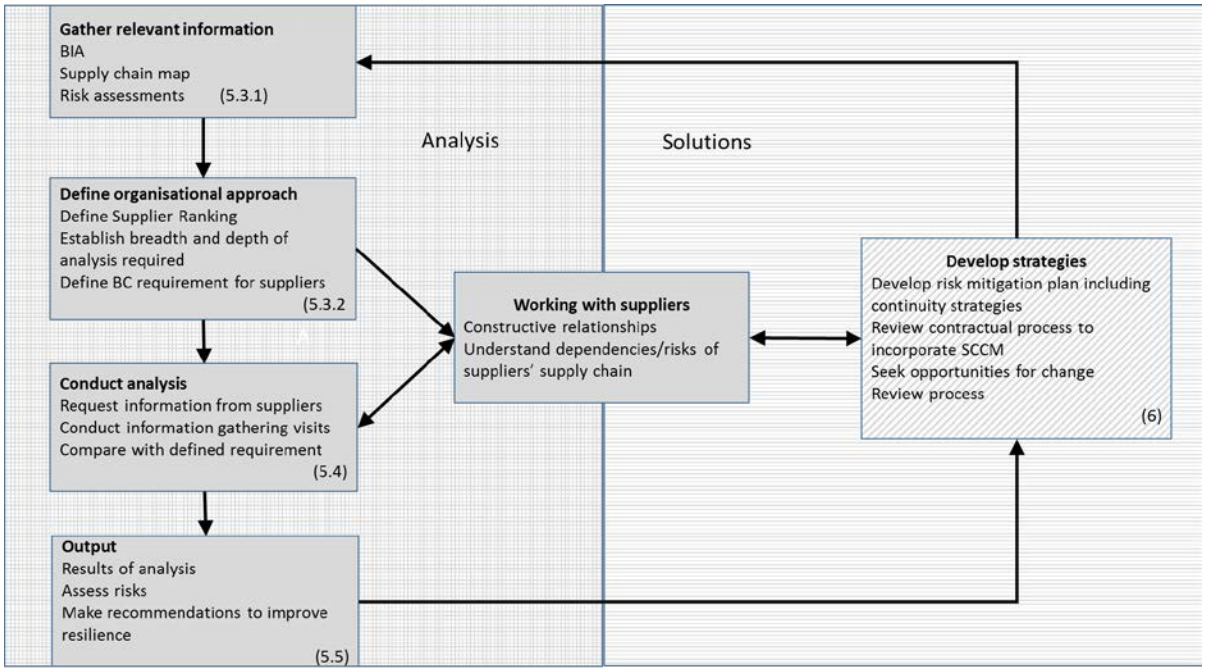

Figure 4 – Supply chain analysis flow chart

5.3.2 Define organisational approach

In undertaking the analysis it is important to achieve consistency across the organisation and to create an approach that is sustainable over time. To help achieve this, a set of core organisational approaches should be developed. These approaches should be specific to the organisation, and tailored to meet the operational and environmental needs. They should include:

- definition of supplier criticality, for example a two tier approach (see Note 2 below):

  a) "critical": suppliers whose products or services are essential for the organisation to continue its critical activities and their loss would jeopardise the survival of the organisation; or

  b) "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 organisation;

NOTE 1 Analysis needs to consider 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.

NOTE 2 The example above only defines two levels of supplier criticality businesses with many suppliers may need to define more supplier criticality groupings to provide a manageable structure for the programme; for example a three tier approach: strategic (business partners), core (suppliers who provide essential services or products), transactional (suppliers of routine non critical products).

- defining acceptable business continuity requirements for suppliers:

  1) what capability the organisation expects for each category of supplier, e.g. minimum levels of supply and recovery time objectives (RTOs), and

  2) what evidence it expects from suppliers to demonstrate compliance/capability;

- breadth and depth of analysis – is the analysis to include all suppliers or only certain categories of supplier based on their criticality? How far down the supply chain should the analysis be conducted?

© ISO 2013 – All rights reserved

- how frequently the analysis is to be repeated; and

- incorporating the requirements into any tender/procurement process and the ongoing supplier management and development.

The overall approach should be fully documented and signed-off within the organisation by top management.

5.4 Conducting the analysis

The organisation should share with suppliers the rationale for the analysis and its potential benefits to them, including an explanation of its requirements and the expectations of each supplier.

Working within the structured approach which has been defined, the organisation should map the various layers of the supply chain (see Figure 2), drawing on any business impact analysis (BIA) undertaken to identify the organisation's critical activities , their respective RTO's and the suppliers on which it depends in order to deliver these. The results of the BIA and the supply chain analysis together, should describe the effect on the organisation of any disruption to supply

For each supplier there should be evaluation, with respect to the organisation of:

a) the criticality of the product or service they provide;

b) whether this supplier is the only source for that product or service;

c) the risks facing the supplier with respect to the critical product or service provided to the organisation;

d) whether the supplier has in place effective business continuity arrangements;

e) the extent to which the supplier has already assessed its own supply chain risks;

f) what priority the organisation has in the supplier's list of critical customers; and

g) whether the supplier's recovery time objectives will allow the organisation to continue to conduct its critical activities.

To support maintenance of SCCM an evidential approach to assessment of suppliers should be used including material such as:

1) documented BIAs, risk assessments and business continuity plans;

2) documented processes for maintaining and updating suppliers' continuity plans; and

3) documented exercise plans and post-exercise and post-incident reports.

NOTE 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.

5.5 Output of Analysis

The output of the analysis is an auditable, evidence based report for each supplier which as a minimum identifies:

- continuity provisions which supplier has in place and evidence that supplier's BCM approach is fit for purpose

© ISO 2013 – All rights reserved

- how these provisions compare with the organisations expectations
- how continuity in suppliers' supply chain is managed
- threats to supply of the relevant product or service
- recommendations for improvements.

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

1) Supply chains are often broad, complex and interdependent, with multiple layers of dependencies.

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

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

4) The analysis should be based on a set of core criteria developed by the organisation: giving a common organisational approach.

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

6) 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.

7) Supply chains are dynamic so business continuity requirements should be built into tender/procurement and supplier management processes, and the overall analysis process should be repeated periodically.

6 SCCM Strategies

6.1 Introduction

An appropriate recovery strategy (section 6.2) should be identified for every supplier. In choosing the most appropriate strategy, or combination of strategies, account needs to be taken of the challenges to SCCM identified in section 4.6 which may limit the options available. The results from the analysis should have identified:

- the suppliers;
- the impact on the business should the supply of product or services be disrupted;
- the criticality of each supplier and hence the tolerance over time of disruption; and
- an understanding of the continuity measures each supplier has in place both for itself and its own supply chain.

The options described here are not mutually exclusive and mitigating the risk arising from an individual supplier may require more than one approach to be implemented. Achieving the final solution will take time; it might be necessary to adopt interim approaches with some suppliers until the opportunity arises to implement the optimum 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.

© ISO 2013 – All rights reserved

Where it is possible to 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, it is relatively straight forward to justify the cost of putting risk mitigation measures in place. It is not so easy to measure the intangible costs of disruption, such as damage to reputation or loss of competitiveness, so the case for implementing mitigation measures might be less clear, but the risk assessment/BIA should emphasize the importance of suppliers to delivery of critical activities or processes.

6.2 Continuity Strategy Options

6.2.1 Option 1 Accept status quo

This 'Do Nothing' option is more likely to be adopted 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 organisation and are used merely to pay creditors).

6.2.2 Option 2 Reduce dependency

Reduce dependence on a supplier(s) by, for example:

1) having two or more sources of supply at all times (see Option 3);

2) lengthening the time before a disruptive event affects the organisation by measures such as increasing stock holding on site or with distributors; and

3) establishing alternative solutions: pragmatic responses to managing risks arising from critical suppliers which the organisation 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

Develop recovery strategies which are independent of the supplier(s) for example:

1) developing workarounds (to mitigate loss of services);

2) identifying alternative suppliers who are able/prepared to pick up the demand at minimal notice; and

3) agreeing mutual support arrangements with competitors.

6.2.4 Option 4 Work with the supplier

Work with each supplier to improve resilience/recoverability by:

1) developing relationships with critical suppliers to understand their arrangements and form partnerships based on mutual trust which will faciltate speedy recovery;

2) clearly defining the performance standard required and the process by which this will be assessed;

3) helping/encouraging the supplier to improve its resilience; and

4) include SCCM requirements into contract terms.

© ISO 2013 – All rights reserved

6.2.5 Option 5 Exit the relationship

If a suitable provision for SCCM with a critical supplier cannot be found consider exiting the contract.

6.3 Including SCCM capability into a supply contract

To deliver SCCM over the longer term the organisation should include the continuity requirement within the tender process to ensure suppliers have adequate BCM provision for the product or service being provided:

- defining the organisation's BC requirement in the invitation to tender (ITT) and assessing the quality of the responses during the supplier selection process (this would include seeking documentary evidence of BC arrangements);
- establishing a framework solution (e.g. a standard contract clause) to deliver the chosen continuity strategy, which can be applied immediately to new contracts and for which early opportunities can be sought to apply it to existing contracts;
- including escalation triggers and measures for notification and incident management in contract terms and SLAs;
- specifying in contracts a requirement to notify key events and information, including invocations, plan reviews, exercises and documents;
- arrangements for joint exercises and sharing of learning points;
- incorporating into contracts provision for management review and/or audit of BC arrangements;
- encouraging visibility of a supplier's approach to assessing the impact of disruption within the supplier's own supply chain and measures being taken to mitigate this risk;
- early notification of changes to the supply environment which could jeopardize the BCM arrangements;
- effects on contract of not achieving required BCM criteria, including escalation process and potential contract termination; and
- excluding force majeure clauses which can be easily invoked by the supplier instead of implementing effective BCM arrangements.

NOTE Force Majeur is a common clause in contracts that essentially frees both parties from liability or obligation when an extraordinary event or circumstance beyond the control of the parties, such as a war, strike, riot, crime, or an event described by the legal term *act of God* (such as hurricane, flooding, earthquake, volcanic eruption, etc.), prevents one or both parties from fulfilling their obligations under the contract. In practice, 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 organisation should identify those with responsibility for supplier management and for securing/monitoring supply chain continuity assurance. It should also be closely linked to the wider arrangements for BCM within the organisation.

Those who bought the products or services (purchasing) should hand over the responsibility for managing the SCCM to those who are going to manage the contract or run operations. It is important to ensure that the control measures put in place do not degrade over time, e.g. having secured two suppliers to achieve resilience, it is important to guard against the potential for the number of suppliers to be reduced to one as a cost-saving measure at some time in the future.

© ISO 2013 – All rights reserved

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

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

2) Where cost–effective, choose strategies which allow the organisation 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 critical resources.

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

4) 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 assurance.

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

6) 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 Introduction

This clause assumes that appropriate analysis has been done of the supply as defined in clause 5 and appropriate strategies put in place in accordance with clause 6. However, threats to the supply chain still exist and the organisation needs to have in place the processes required to manage an incident. It is important to maintain engagement with critical suppliers to ensure continuity management arrangements are available and effective. This is best achieved by ensuring regular and open discussion between the parties to create a partnership between the organisation 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

Business continuity plans should include:

- Details of any limitations on the organisation arising from supplier disruption; e.g. breaks in supply of goods or services whilst recovery takes place.
- Supplier expectation of support the organisation may provide them.
- Action plan for the organisation’s immediate response.

Exercise integration. If possible, inviting the suppliers to take part in BC exercises that relate to the products/services they supply will allow the suppliers to understand the criticality of their supply. It would also enable the suppliers to identify any delivery issues that they could experience in supplying to an alternative site. It is also valuable for the organisation to be able to attend supplier exercises relating to the products/services supplied to it. The organisation can gain objective assurance of the supplier’s ability to continue to supply in the event of an interruption.

© ISO 2013 – All rights reserved

Make use of horizon scanning to alert the organisation to emerging risks which may affect the supply chain. Disruptions might arise due to the indirect effect of external events, such as transport disruption caused by a fuel shortage brought on by industrial action or movement restrictions imposed by a disease outbreak. The time taken for a supplier to identify a problem and notify the organisation of the potential impact could cost the organisation potentially valuable response time.

7.3 Incident detection and notification

Early detection of a disruptive event enables an effective and appropriate response. This requires that the relationship between the organisation and each supplier is open and suppliers feel confident that they can raise issues with the organisation.

Where the relationship is less transparent the supplier may be reluctant to inform their customers of a disruption, or potential disruption due to optimism about its ability to resolve the disruption without impact to the organisation. The impact of delayed notification potentially increases the risk of a minor problem becoming a major issue for the organisation. 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

Factors to consider during an incident are:

- Coordinated incident management. If the disruption experienced by the critical supplier impacts the operation it is important to coordinate the incident management of both organisations. This reduces the likelihood of wrong assumptions and minimizes the impact to the organisation.

- Impact of supplier's operating location with respect to geography, cultural and political differences.

- Regular communication with the supplier about the current situation and the potential return to normal working is essential throughout the incident.

- External communications: It is essential that the organisation understands the approach that the supplier will have to external communications to avoid "mixed messages" and the consequential reputational damage.

- Recognise this is a reciprocal arrangement; if the organisation is the source of the incident suppliers need to be engaged to manage both their business operations which may be affected by disruption and/or to provide valuable support to facilitate the organisation's recovery.

7.5 Return to business as usual

A combined approach is required to facilitate recovery to business as usual; this will take time and may require co-ordination with many suppliers whose operations have been affected.

After any disruption, there is an opportunity to learn lessons and improve matters so that similar events in the future will have less impact on both the supplier and the organisation. These might result in improvements in the organisation or the supplier's operations, or to the information flows between suppliers and the organisation. However, a supplier could be reluctant to share full details, especially where other suppliers are involved in the review. In addition to managing concerns about sharing sensitive information, suppliers might be reluctant to accept follow-up actions without changes to contracts and charges. If possible, the organisation should be allowed to see any actions resulting from the incident and be able to track the status toward their completion.

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

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

© ISO 2013 – All rights reserved

2) Exercise with suppliers to improve co-ordination and understanding of each other's issues.

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

4) During an incident ensure that command and control is integrated

5) Co-ordinate external communications plans.

6) Post event conduct a thorough, shared review of what happened and the lessons to be learnt.

8 Performance evaluation

8.1 Introduction

Performance evaluation covers the ongoing management of the SCCM including monitoring, verification, validation and review of SCCM arrangements stimulates continuous improvement and provides assurances in the supply chain.

Ongoing management and review is a proactive and dynamic process which should be reviewed at agreed intervals with the organisation's critical suppliers. This process monitors and acts as an early detection mechanism for any changes in a supplier's business, e.g. organisational changes, reporting processes, manufacturing location and outsourcing. It should be included as part of the routine management of the contract.

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

a) 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;

b) monitoring supply chain performance and identifying potential issues;

c) establishing escalation triggers and procedures for suppliers to report failures;

d) identify any "hidden" risks with its critical suppliers in the event that they suffer a disruption; and

e) facilitate the alignment of suppliers' RTOs and SLAs with those of the organisation.

8.2 Engaging with suppliers

BCM assurance should be introduced and accepted as a business-as-usual item for discussion through:

a) inclusion as an agenda item for supplier update meetings;

b) shared education and training tools;

c) the procurement and contracts process;

d) monitoring of performance metrics.

e) testing of incident plans and well-rehearsed triggers and escalation plan;

f) shared understanding of command and reporting structures in the event of an incident;

g) collaborative exercise programme

© ISO 2013 – All rights reserved

8.3 Implementing a SCCM performance evaluation programme

To implement a SCCM assurance programme, the following need to be maintained:

a) The organisation's criteria for the SCCM capability required from suppliers; this will depend on the assessment of criticality and the chosen BCM strategy for each supplier.

b) The assurance process should include:

   i. maintaining the analysis, see 8.4;

   ii. key performance indicators (KPIs)/metrics for ongoing monitoring;

   iii. design of questionnaires/checklists/self-evaluations;

   iv. escalation process for suppliers who do not meet the criteria;

   v. review of organisational process from procurement to BCM team;

   vi. review of contract and schedule clauses for use by procurement/supply chain management.

8.4 Maintaining the analysis

The supply chain and the risks it faces are constantly changing so it is important to establish a process to keep the analysis up-to-date and identify opportunities for continuous improvement. The organisation should:

a) implement a rolling review process to monitor supply chain changes, implementation of improvements, etc.;

b) identify individuals responsible for this ongoing work, incorporating it into the existing supplier management process wherever possible;

c) build supplier requirements into tender/procurement processes; and

d) include the supplier SCCM assurance process into the scope of BCM audits.

8.5 Outcomes of performance evaluation

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

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

b) documented processes for maintaining and updating suppliers' continuity plans;

c) supplier's exercise plans and post-exercise and post-incident reports;

d) documented notification process is in place that includes key organisations likely to be impacted; and

e) documented communications plan that includes joint communications and statements that take into consideration the organisations impacted.

The benefits of the process are:

a) greater confidence in the supply chain (i.e. better understanding of the risks and controls);

© ISO 2013 – All rights reserved

b) evaluation of whether each supplier/partner meets the organisation's BCM requirements;

c) early indication of changes likely to affect the supply relationship;

d) identification of gaps in capability which the supplier needs to address; and

e) supplier monitoring and performance measurement against targets.

If there are significant issues with a supplier's BCM provision then the organisation can review the relationship and/or the SCCM strategy, see Clause 6.

In conducting performance evaluation the following should be considered:

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

b) performance evaluation is an indicator, not a guarantee. It is only a snapshot at a particular point in time. Situations can change, so the programme needs to be reviewed regularly;

c) the performance evaluation process and implementing remedial actions could result in increased costs; and

d) the right to carry out performance evaluation should be included in the contract/agreement. If the right to undertake performance evaluation is not in the agreement it should be added, if possible.

8.6 Key points of Clause 8: Performance management

1) The onus is on the organisation to ensure that SCCM provisions required to protect its critical activities or processes are maintained.

2) 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.

3) Regular engagement with suppliers through update meetings or calls, is essential to maintaining supplier relations.

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

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

© ISO 2013 – All rights reserved

Bibliography

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[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 22301 *Societal Security - Business Continuity Management Systems - Requirements*

[4] ISO 22313 *Societal security - Business Continuity Management Systems – Guidance*

[5] ISO 31000 *Risk Management – Principles and guidelines*

[6] BS PAS 7000: 2014 *Supply chain risk management – Supplier prequalification*

[7] BS 65000:2014 *Guidance on organisational resilience*

[8] BS 13500: 2013 *Code of practice for delivering effective governance of organisations ISO/TS 22318 – Societal Security – Business continuity management – Guidance on supply chain continuity*

© ISO 2013 – All rights reserved