ICS 13.200
A 90

中华人民共和国国家标准

GB/T 38299—2019/ISO 22318:2015

公共安全　业务连续性管理体系
供应链连续性指南

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

(ISO 22318:2015,IDT)

2019-12-10 发布　　2020-06-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准使用翻译法等同采用ISO 22318:2015《公共安全　业务连续性管理体系　供应链连续性指南》。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 30146—2013　公共安全　业务连续性管理体系　要求(ISO 22301:2012,IDT)

本标准由全国公共安全基础标准化技术委员会(SAC/TC 351)提出并归口。

本标准起草单位：中国标准化研究院、南京卫岗乳业有限公司、中国信息安全认证中心、咸亨国际科技股份有限公司、国网山东省电力公司、北京城市系统工程研究中心、广发银行股份有限公司信用卡中心、北京市劳动保护科学研究所、南方电网科学研究院有限责任公司、英标认证技术培训(北京)有限公司。

本标准主要起草人：秦挺鑫、白元龙、尤其、翟季青、夏剑剑、王晶晶、杨正科、汪彤、周育忠、邢立强、龚浩、孙宏志、孙世军、李俊超、朱伟、张桂明、代宝乾、陆维斌、赵连河。

引　言

GB/T 30146 和 GB/T 31595 为组织如何保持供应链连续性提供了业务连续性指导，本标准对其进行了深入拓展。本标准假设开展供应链连续性管理(SCCM)的组织已了解业务连续性管理的原则，并已建立或准备实施符合相关标准的业务连续性管理体系(BCMS)。此外，本标准涉及未对产品或者服务供应商连续性管理对组织的影响。

本标准供负责采购、管理组织必需产品或者服务的人员使用，并有助于人员按照既定标准实施良好的 BCM 实践。

组织依赖供应商按时交付达成约定质量及标准的产品或者服务。对于组织来说，识别供应链中断对活动的潜在影响非常重要，这也是业务连续性管理的重要环节。供应商未按时交付达到约定质量和成本的产品或者服务可引发业务中断事件。对于相互冲突的目标，可通过降低供应链成本(如减少周期时间和缓冲库存)和管理供应链连续性风险(如单一来源、依赖按时供应)两种方式解决。

本标准适用于同一组织有连续供应关系的外部、内部供应商所提供的产品和服务，和未按时交付造成组织额外的一次采购安排。

依据其产品或者服务供应中断对组织的影响程度对供应商进行分级，供应商级别用于确定供应商与组织的关系。1 级供应商与组织有直接的合同关系，2 级供应商则向 1 级供应商提供产品和服务。同样的供应链连续性关注事项适用于各级供应商。1 级供应商需要确保其供应链关系，并使客户了解 1 级以外的供应链具有足够的韧性，以及 1 级以外供应商的社会责任等因素。

本标准给出的指导有助于供应商满足客户的业务连续性期望，并可分析依赖单一客户产生的脆弱性。

本标准推荐供应商也遵守 ISO 28000 系列标准中关于供应链安全管理的规定。遵守这些标准将有助于组织提高供应链韧性，降低购买产品和服务时的中断风险。

业务连续性管理的要素见图 1。本标准与业务连续性管理的要素的对应关系见表 1。

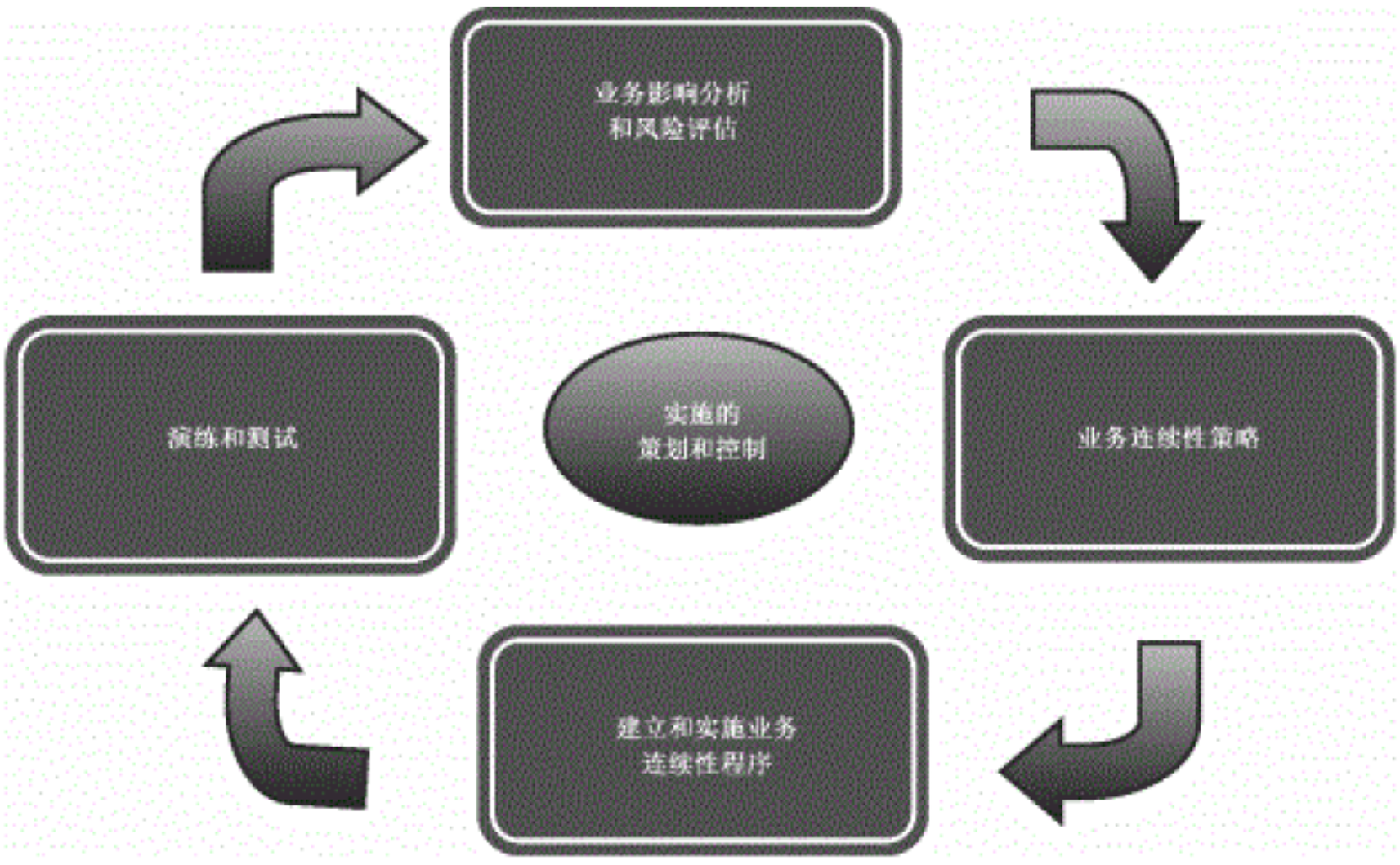

图 1　业务连续性管理(BCM)的要素

表 1　业务连续性管理要素与本标准章节的对应

BCMS 要素	本标准
实施的策划和控制	第 4 章
业务影响分析和风险评估	第 5 章
业务连续性策略	第 6 章
建立和实施业务连续性程序	第 7 章
演练和测试	第 8 章

公共安全　业务连续性管理体系
供应链连续性指南

1　范围

本标准给出了理解和扩展 GB/T 30146 和 GB/T 31595 中供应商关系管理的 BCM 原则的方法。

本标准是通用的且适用于所有类型、规模和业务性质的组织(或组织内的部分),适用于组织内外部产品和服务的供应。本标准应用程度取决于组织的运营环境和复杂性。

供应链管理针对向组织供应产品或者服务相关的各项活动。本标准重点关注组织为维持业务活动或者流程而面对的产品和服务连续供应问题,以及供应链中供应商用于降低中断影响的连续性策略,即供应链连续性管理(SCCM)。

GB/T 30146 和 GB/T 31595 给出了制定业务连续性计划和建立业务连续性管理体系的相关指导。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

ISO 22300　公共安全　术语(Societal security—Terminology)

ISO 22301　公共安全　业务连续性管理体系　要求(Societal security—Business continuity management systems—Requirements)

3　术语和定义

下列术语和定义适用于本文件。

3.1

业务连续性　business continuity

组织在中断性意外事件之后仍可以接受的预定义水平继续提供产品或者服务的能力。

[ISO 22300:2012,定义 2.1.10]

3.2

业务影响分析　business impact analysis;BIA

分析活动和业务中断可能带来的影响的过程。

[ISO 22300:2012,定义 2.2.6]

3.3

事态　event

特定情况集合的发生或变化。

注 1:事态可以是一次或多次发生的,可能有多个原因。

注 2:事态可以包括不是正在发生的事情。

注 3:事态有时可发展为“事件”或“事故”。

注 4:未造成后果的事态也可能被称为“未遂”“接近发生”或“紧急”。

[ISO 22300:2012,定义 2.1.8]

3.4

演练　exercise

在组织中训练、评估、实践和提高绩效的过程。

注 1：演练可以用于验证方针、计划、程序、培训、设备和组织间的协议；明确和培训人员的角色和职责；改善组织间的协调和沟通；识别资源上的差距；提升个人绩能；识别改进机会；把握机会提升应变能力。

注 2：测试是演练的一种特殊类型，它包含了对正在计划的演练目标或目的中成功或失败因素的预期。

[ISO 22300:2012，定义 2.4.8]

3.5

事件　incident

可能或将导致中断、损失、紧急状况或危机的情况。

[ISO 22300:2012，定义 2.1.15]

3.6

风险　risk

对于目标的不确定性影响。

注 1：该影响是偏离预期目标的，包括正面的或负面的。

注 2：目标可以有不同的方面(例如财政、健康和安全以及环境)，也可以应用于不同的层次(例如战略、组织范围、项目、产品和过程)。目标可以用其他方式来表示，例如作为预期结果、意图、运行准则、业务连续性目标或用其他意思相近的词来表达(例如目的或宗旨)。

注 3：风险常被描述为潜在事态和后果，或它们的组合。

注 4：风险通常被表述为事态的后果(包括环境的变化)和发生的可能性。

注 5：不确定性是部分或完全缺少与事态的后果和可能性相关信息的状态。

[ISO 22300:2012，定义 2.1.5]

3.7

最高管理者　top management

在最高层指挥和控制组织的一个人或一组人。

注 1：最高管理者有权力在组织内进行授权，并提供资源。

注 2：如果管理体系的范围只涵盖了组织的一部分，那么最高管理者指那些直接指导和操控该部分组织的人。

[ISO 22300:2012，定义 2.2.4]

3.8

活动　activity

由组织(或其代表)为生产或支持一个或者多个产品和服务而执行的过程或者一组过程。

示例：此类过程包括账务、呼叫中心服务、信息技术、生产和配送。

[ISO 22301:2012，定义 3.1]

3.9

业务连续性管理　business continuity management:BCM

识别对组织的潜在威胁以及这些威胁一旦发生可能对业务运行带来的影响的一整套管理过程。该过程为组织建立有效应对威胁的自我恢复能力提供了框架，以保护关键相关方的利益、声誉、品牌和创造价值的活动。

[ISO 22301:2012，定义 3.4]

3.10

业务连续性管理体系　business continuity management system:BCMS

用于建立、实施、运行、监视、评审、保持和改进业务连续性，是一个组织整个管理体系的一部分。

注：管理体系包括组织结构、方针、规划活动、职责、程序、过程和资源。

[ISO 22301:2012，定义 3.5]

3.11

业务连续性计划　business continuity plan

用于指导组织在业务中断时进行响应、恢复、重新开始和还原到预先确定的业务运行水平的形成文件的程序。

注：业务连续性计划通常包括确保关键业务功能的连续性所需的资源、服务和活动。

[ISO 22301:2012，定义 3.6]

3.12

相关方　interested party

对决策或活动产生影响，受到影响，认为被影响的个人或组织。

注：可以是与组织的任何决策或活动有利益关系的个人或团体。

[ISO 22301:2012，定义 3.21]

3.13

最小业务连续性目标　minimum business continuity objective:MBCO

在中断中组织为达到其业务连续性目标可以接受的最低标准的服务和(或)产品。

[ISO 22301:2012，定义 3.28]

3.14

组织　organization

为了实现目标形成的具有自身职能，按照一系列职责、权限和相互关系安排的个人或一组人员。

注 1：组织的概念包括但不限于个体商户、公司、集团、企事业单位、研究机构、合伙企业、慈善机构，或是上述单位的结合体，无论其是否为法人团体，公营还是私营。

注 2：对于拥有一个以上运营单位的组织，可以把每一个单独运营的单位视为一个组织。

[ISO 22301:2012，定义 3.33]

3.15

外包　outsource

把组织的部分职能或过程安排给外部组织。

注：虽然外包的职能和过程属于管理体系的范围，但外部组织则在此范围之外。

[ISO 22301:2012，定义 3.34]

3.16

产品和服务　products and services

组织提供给顾客、服务对象和相关方的有益成果，例如制成品、汽车保险和社区护理。

[ISO 22301:2012，定义 3.41]

3.17

恢复时间目标　recovery time objective:RTO

事件发生后到下列活动完成之间的时间段：

——产品或者服务必须恢复；

——活动应恢复；

——资源应复原。

注：对于产品、服务和活动，恢复时间目标应小于组织不能接受的导致产品/服务停止供应、活动无法执行等负面影响所需的时间。

[ISO 22301:2012，定义 3.45]

3.18

资源　resources

为了运行和实现目标，组织在需要时可供使用的所有资产、人员、技能、信息、技术(包括工厂和设备)、场地、物资和信息(无论是否为电子格式)。

[ISO 22301:2012，定义 3.47]

3.19

关键客户　critical customer

一旦丧失其业务则会威胁组织生存的个人或者实体。

3.20

关键供应商　critical supplier

提供关键产品或者服务的个人或者实体。

注：包括“内部供应商”，也是具有客户关系的同一组织的一部分。

3.21

关键产品或者服务　critical products or services

从供应商获得的资源，如果无法获取此类资源，则会中断组织的关键活动并且威胁组织的生存。

注：关键产品或者服务是支持其 BIA 中识别的组织最高优先级别活动以及流程必不可少的资源。

3.22

中断　disruption

无论属于预期(比如罢工或者飓风)或者非预期的(比如大停电或者地震)的事态均会导致与组织目标预计交付的产品或者服务存在计划外的不利偏差。

3.23

供应链　supply chain

涉及通过上下游联系，向最终客户以产品和服务的方式提供价值的过程和活动的组织网络。

3.24

供应链连续性管理　supply chain continuity management;SCCM

在供应链中实施业务连续性管理。

注 1：BCM 宜应用于组织的各级供应链。

注 2：实际上，组织通常仅将其应用于 1 级供应商，通过影响关键供应商以对其供应商实施 SCCM。

3.25

1 级供应商　Tier 1 supplier

通常通过合同安排直接向组织供应产品或者服务的个人或实体。

3.26

2 级供应商　Tier 2 supplier

间接通过 1 级供应商向组织提供产品或者服务个人或实体。

4　供应链连续性的重要性

4.1　总则

本章关注的是与 SCCM 实施架构相关的各项因素。随着供应链的日益复杂、范围扩大(经常延展到国际)以及频繁变更，组织会不断面临额外的供应链中断风险。由于供应链总会有潜在中断，因此需要 SCCM。

通常情况下，通过合同协议来管理客户—供应商关系，包括组织与供应商之间针对外包的服务水平协议(SLA)和针对内部服务的运营水平协议(OLA)，这同样也适用于一次性采购。

4.2　供应链描述

广义的供应链包括产品和服务的生产与配送、外包与离岸外包。它适用于各种类型和大小的组织。图 2 给出了一个简单的供应链模型。

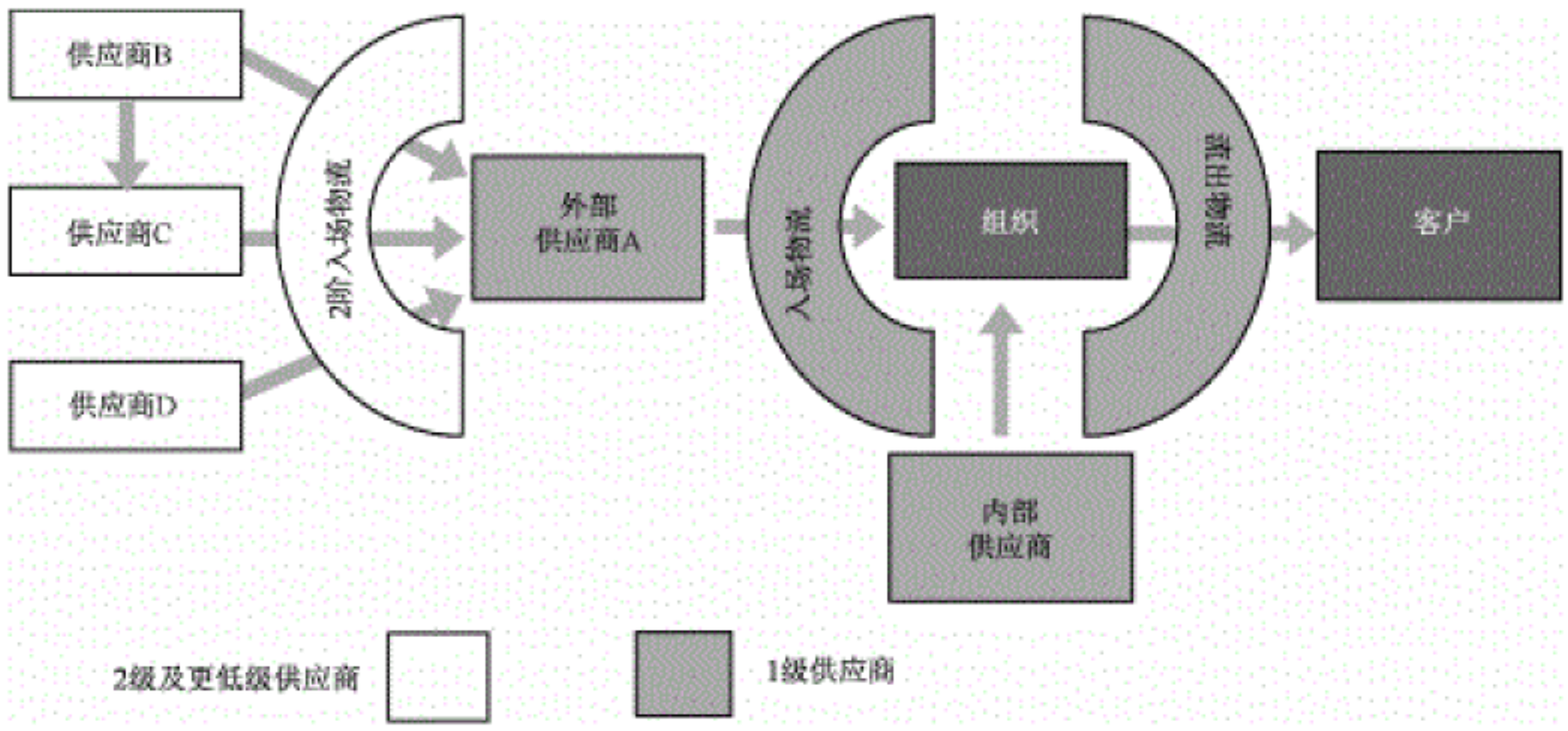

图 2　供应链模型

注 1：实际的供应链更为复杂。

注 2：外部供应商 A 可提供产品或者外包服务。

注 3：内部供应商包括组织从其更大的业务组购买服务或者设备所涉及的任何关系。

供应链存在于不受运营单位(组织)直接管理或者控制的产品或者服务的供应过程中，包括内部与外部供应关系。不同供应商的关系因组织控制这种关系的灵活程度与能力的不同而不同(见图 3)。

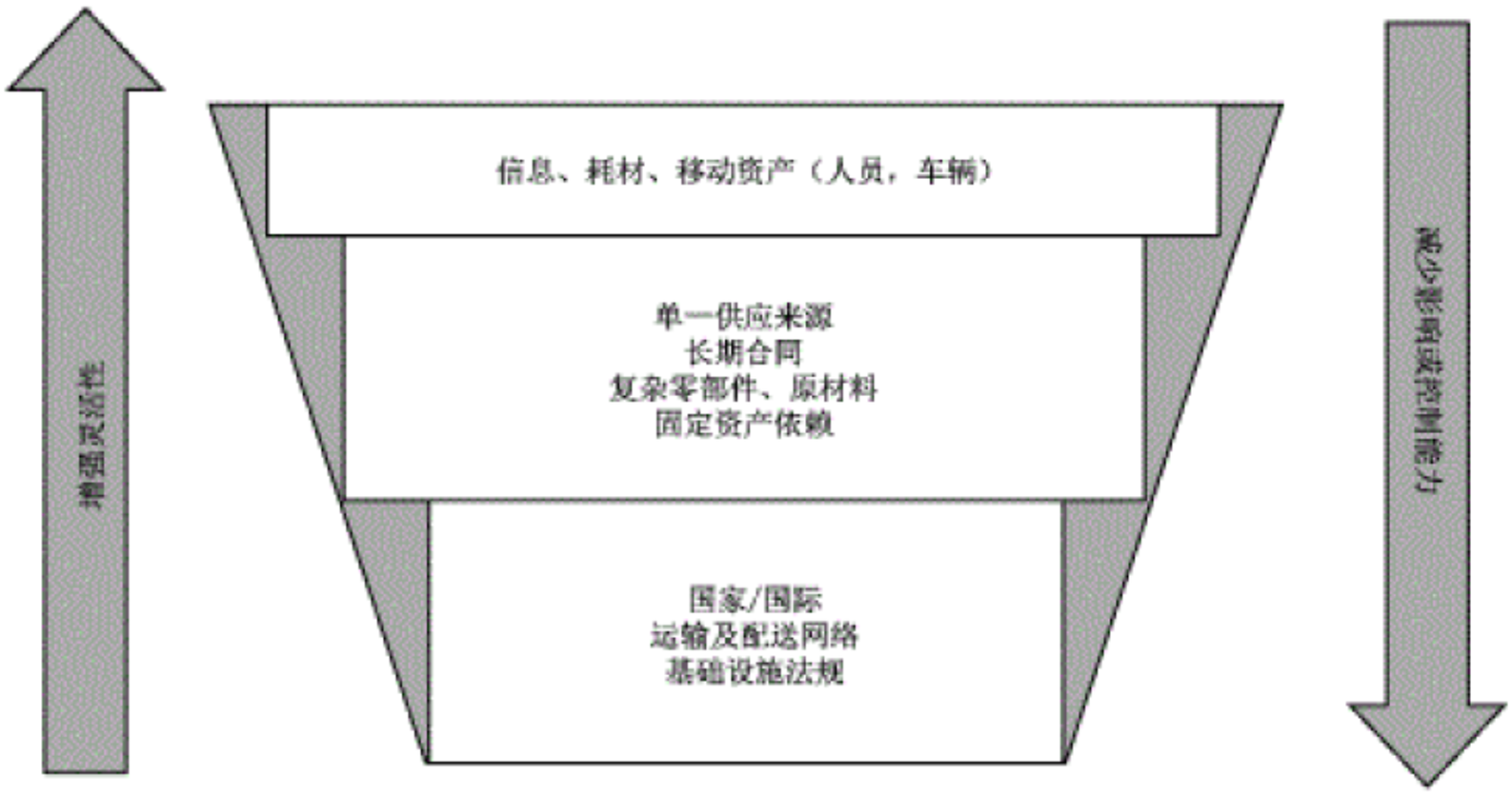

图 3　供应链——灵活性、影响和控制

供应链中一系列潜在的客户关系类型包括：

——公司对公司(包括分销商、批发商等)；

——公司对顾客；

——第三方服务(客户受到间接服务，例如，通过分包商或代理)。

同时也有如下的一系列潜在的供应商关系类型，包括：

——常用的产品、服务的供应商(提供组件、原材料、融资、房地产租赁、重要固定资产维护等)；

——一次或少量产品、服务供应商(可提供一种新的固定设备)；

——外包、契约服务或业务流程的提供者(如薪酬管理服务机构、IT 服务、联系中心、物流或配送)；

——战略合作伙伴/联盟(如特许经营、分销商和合资企业)；

——与供应商之间是合作关系或相互依赖关系。

除客户和供应商外，可受到供应链中断牵连和影响的其他利益相关者，包括当地社区（例如，社区的工人被抽调）、非正式的社会网络成员、贸易机构、签约的联盟伙伴、部分竞争对手等。

可构成供应链关系基础的因素至少包括：

——人与人际关系；

——合同、工作指令、服务水平协议、运营水平协议等正式协议；

——采购订单或设计规范等的电子或纸质信息；

——对工作流、产品/服务创建和交付等过程的描述；

——运输体系、互联网等基础设施；

——商业网络、贸易关系等文化因素；

——环境：政治、经济、法规等。

4.3 供应链的动力

4.3.1 通则

供应链对不同类型和规模的组织来说都很重要，尤其是在组织寻求降低成本和提高效率的时候。消除库存、时间和其他形式的“无效率”意味着商品、服务、信息和资金的流动更高效，反过来意味着供应链一旦中断，其影响将会更强烈、更敏感、更频繁。对于许多组织来说，逐渐加大投资于供应链的成本比例，既有风险也有机会。糟糕的供应链管理会摧毁价值观、危及品牌和声誉。

无论是地理分布还是供应商的数量与类型，供应链已经超出了组织的直接控制。导致这一局面的驱动力因素包括：

——通过互联网可实现相对低成本的全球访问；

——国际贸易壁垒的减少和资本的自由流动；

——受过教育和相对低成本的技术工人的大量增加；

——组织将管理重点放在核心增值活动，倾向于将非核心业务流程外包，如物流、配送、薪酬管理、餐饮服务、保洁、安保与IT服务，使组织更加相互依赖；

——随着全球需求超过了供给，某些特定的供应，包括一些自然资源，只存在于世界某些地区，这导致了资源受到限制。

由于组织之间的关联与依赖性正在增加，并且供应链所达范围更加全球化，新的脆弱点正在不断出现，暴露程度不断提高，通过水平扫描识别变更风险状况（见第7章）正在变得更加具有挑战性。由于供应链更加一体化和相互依赖，任何影响其中一个链接的事件都可能会影响到供应链中的其他链接。业务影响分析可以揭示供应链的整体相互依存关系，但可能不会深入到供应链内部越过一级（直接）供应商开展分析，而组织通过这些1级供应商与2级供应商、1级供应商的直接供应商以及其他组织具有了合同关系。

4.3.2 供应商和合同生命周期

供应商合同存在于供应和服务的采集、操作和中止的生命周期内（见图4）。签订新合同或者更新现有的合同给组织提供了一个机会，使其可以通过合同与服务水平变化来影响未来供应商行为。相反，长期合同承诺与高供应商转换成本会改变组织与其供应商之间的权力平衡，产生对改变供应商行为的抵制（见图3）。在这种情形下，应实施SCCM。供应链分析（见第5章）将有助于识别实施SCCM的高优先级关系、需求与机会。

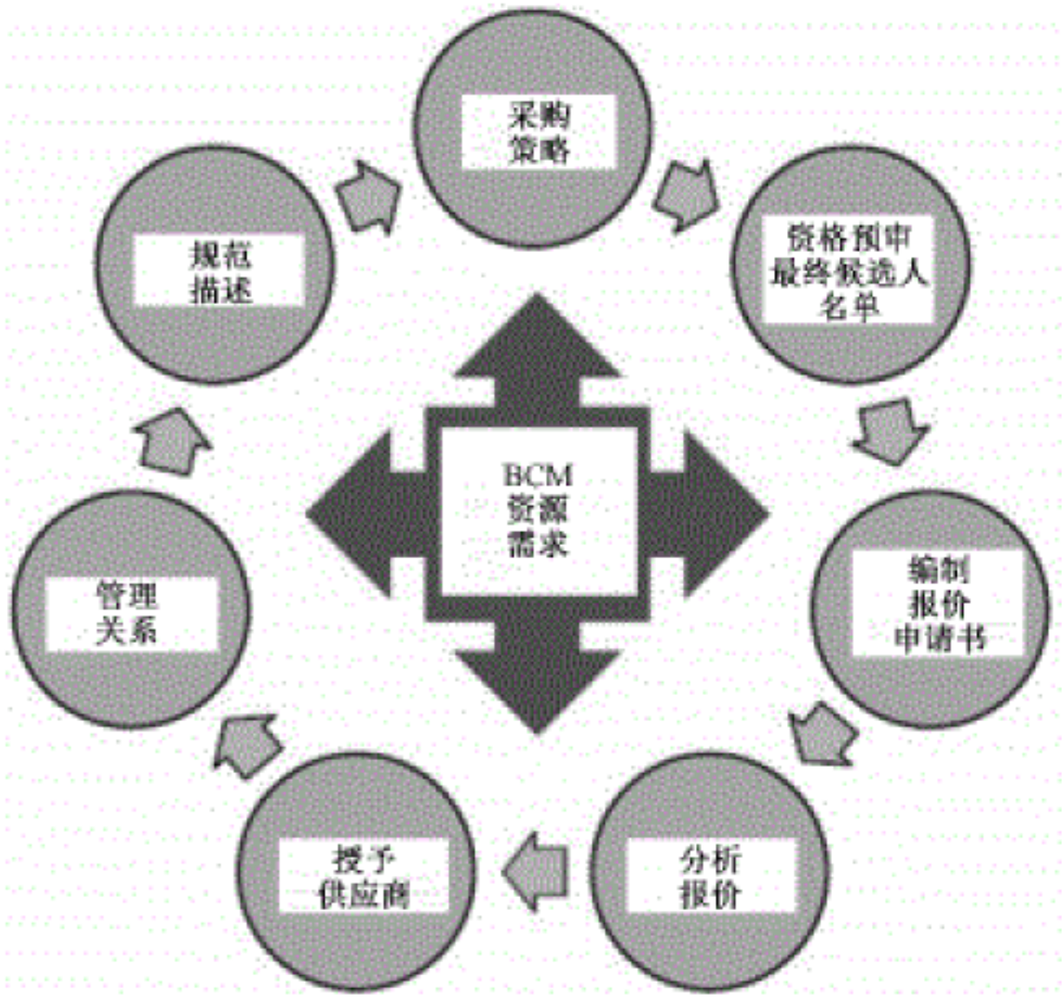

图 4　将 SCCM 整合到供应链生命周期之中

4.3.3　风险承担者

组织本身具有因供应链中断而无法提供其产品或者服务给客户的风险。因此组织宜承担适合的风险管理政策和方法以减轻风险的责任，并做好供应链中断的预防措施。客户(合法的)期望组织负责它的供应链，也期望组织(而不是其供应商)负责按时交付产品或者服务。因此，一个组织的品牌可能因其供应链发生问题或被供应商的行为所损害。

在某些极端情况下，供应链中断可能会影响一个行业、市场部门或更广泛的经济、政府和公众的利益。

4.4　SCCM 的基本要素

有效 SCCM 的关键要求包括如下：

a)　最高管理者支持整合的 BCM 与 SCCM 方案：
　　1)　设定必要的优先级别与标准；
　　2)　分配资源以便开展分析；
　　3)　评估供应链或者各个供应商失效对于组织高优先级活动或者流程的影响。
b)　分析了解组织的供应链，及供应链中断对组织造成的风险。
c)　针对每个供应商而采用适当的连续性策略。
d)　用于确认供应商已经采取适当连续性措施的程序。
e)　供应商关系管理方案。
f)　构建更具恢复力供应链的长期策略。

4.5　有效的 SCCM 的效益

有效 SCCM 的潜在效益包括以下各项：

——更好地理解供应链以及潜在威胁；

——改进供应商关系管理以减少供应链中断影响；

——通过有效与供应商以及客户开展合作，改进供应链中断的响应方式；
——在供应链风险发生之前或者在组织受到影响之前，识别以及减缓此类风险；
——改进计划工作、尽职调查、保险和与供应商的工作关系；
——对不具有有效 SCCM 的对手形成竞争优势。

4.6 实施有效的 SCCM 所面临的挑战

SCCM 提出了大量的挑战，其中包括以下各项：
——规模与复杂性，尤其涉及具有数千供应商的大型组织；
——供应商在供应链中的距离与可见性(地理位置分散以及供应链中存在的级数)；
——说服供应商以开放且透明的方式参与其中，其原因是 SCCM 会令关系增值；
——僵化的合同关系导致服务面向变革开放的程度较低；
——采用无结构化的方式描述了何处开始、如何进行以及如何克服冷漠或惰性；
——无法开发业务案例以及确保最高管理者的承诺与必要的资源，其中包括经过训练的人员；
——在组织内部跨越相关方职能和在供应链中跨越组织去定义并嵌入有关 SCCM 的责任；
——缓解供应链风险支出带来的长期回报与较低的供应链资金使用与运营成本带来的短期财务收益的平衡；
——个人、组织与文化在风险容忍和偏好方面的差异；
——缺乏实施最优策略的组织以及供应商资源；
——单个与唯一来源供应商；
——文化差异，其中包括多样化问题的考虑事项；
——不同的组织与供应商法规要求；
——小型组织面对具有多个客户的大型供应商时的供应链内部权力失衡问题；
——从供应商获得产品或者服务供应连续性安排方面的信心(供应商是否在出现短缺的情况下将供应品转移至其他客户)；
——识别间接影响的困难，如丧失某位供应商令其他供应商处于危急状态的时刻；
——理解中断全部成本的困难。

4.7 保持供应链连续性的重要性

包括如下内容：

a) 一旦组织依赖不在其直接管理或控制下的输入交付产品或者服务时，供应链即存在。
b) 在全球化程度不断提高、联系性紧密和快速变化的世界里，通过供应链的支出在大多数组织的总成本中占据了显著的比例，而这种情况面临新的和更高的风险，因此供应链连续性是十分重要的。
c) 供应链中断可能会严重影响组织执行关键业务流程的能力。
d) 供应链通常是由大量的供应商组织成线(如链)或网(如网状)。这些相互关系以及它们之间的交易处于动态变化中。
e) 组织内和组织间的许多供应链利益相关者需要有效协作，实现供应链连续性。
f) 组织负责(而不是供应商)减轻其供应链风险和应对供应链中断。
g) 在组织目标产生冲突的时候，应降低供应链的管理成本和减少供应链风险。
h) 供应商需要证明其在一次中断事件后，在可接受的时间框架内，恢复向一个组织提供产品或者服务的连续性能力。

5 供应链分析

5.1 总则

对所有供应商进行一致的分析可以使组织理解和评估供应链中断所带来的风险及潜在影响。供应商对于组织活动的关键程度以及其面对的风险级别将决定分析的深入程度。供应商有责任将这种分析过程推进到其自己的供应链中,并将分析结论反馈给组织。

5.2 分析供应链的注意事项

执行分析时,需要考虑以下情况:

——所要求的分析深度,应对依赖性、风险和影响已被识别和理解提供保证;

——使用一个一致的、可审核的、随时间推移仍可保持的方法;

——成本/收益;

——为引入和持续供应商关系管理而定义组织的连续性框架和要求;

——将已识别出的供应链风险整合进组织的风险管理过程;

——识别对供应商有约束力的法律法规;

——业务影响分析(BIA)结果。

5.3 方法定义

组织宜识别其运行环境需求,并且在开展分析的时候考虑此类需求,以确保在组织范围内实现一致性,并且创建在一定时间范围内的可持续方案。其中应包括以下内容:

a) 采用分级方案评估供应商关键性。如可按照下列方式将供应商分为两级:
   1) "关键":供应商如未能按时交付产品或者服务,或者未能达到相关质量或成本,则会显著影响组织继续开展高优先级活动或者流程的能力,而且一旦失去此类供应商,则可能会危及组织的生存;
   2) "非关键":一旦失去供应商的产品或者服务,则在有限时间周期内是可以忍受的,而且不会对组织的核心活动造成不利影响。
b) 考虑两个层级供应商是否足以为项目提供可管理的结构,或者是否需要采用三个层级的方案:策略性(业务伙伴)、核心(提供重要服务或者产品的供应商)、交易性(常规非关键产品的供应商)。
c) 分析意外事件的冲击及其对于同时供应相同产品或者服务的大量非关键供应商的影响。
d) 确定可接受的供应商业务连续性要求:
   1) 组织期望各类供应商在最低供应水平,包括最低业务连续性目标(MBCO)以及恢复时间目标(RTO),所具有的能力;
   2) 供应商证明合规性/能力所需的具体证据。
e) 分析的广度需要考虑根据关键性判断分析全部供应商还是部分供应商,分析的深度需要考虑深入到供应链的什么程度。
f) 需要重复分析的具体频率。
g) 在当前供应商管理以及今后任何采购策略中采纳的具体要求。

组织宜全面记载方案,并且确保其获得最高管理者的同意。

5.4 分析的结构

组织可使用供应链分析流程图(见图 5)进行如下分析:

——收集整理有关可用文件，包括业务影响分析、风险评估和供应商清单；
——确定用于评估供应商重要性、业务连续性安排的方法(包括参数)，并使之文件化；
——与各供应商进行分析和风险评估；
——评审各个供应商对其供应链的分析结果；
——综合每个供应商评估风险的总体水平；
——与合适的供应商分享结果(差异分析)，提出改进建议，协定一个行动计划和监测的过程；
——将 SCCM 纳入供应商关系管理过程，分配定期评审的职责；
——修订各个供应商对于组织的风险级别；
——通过对比供应商连续性能力与供应商关键性，完成供应链的总体分析。

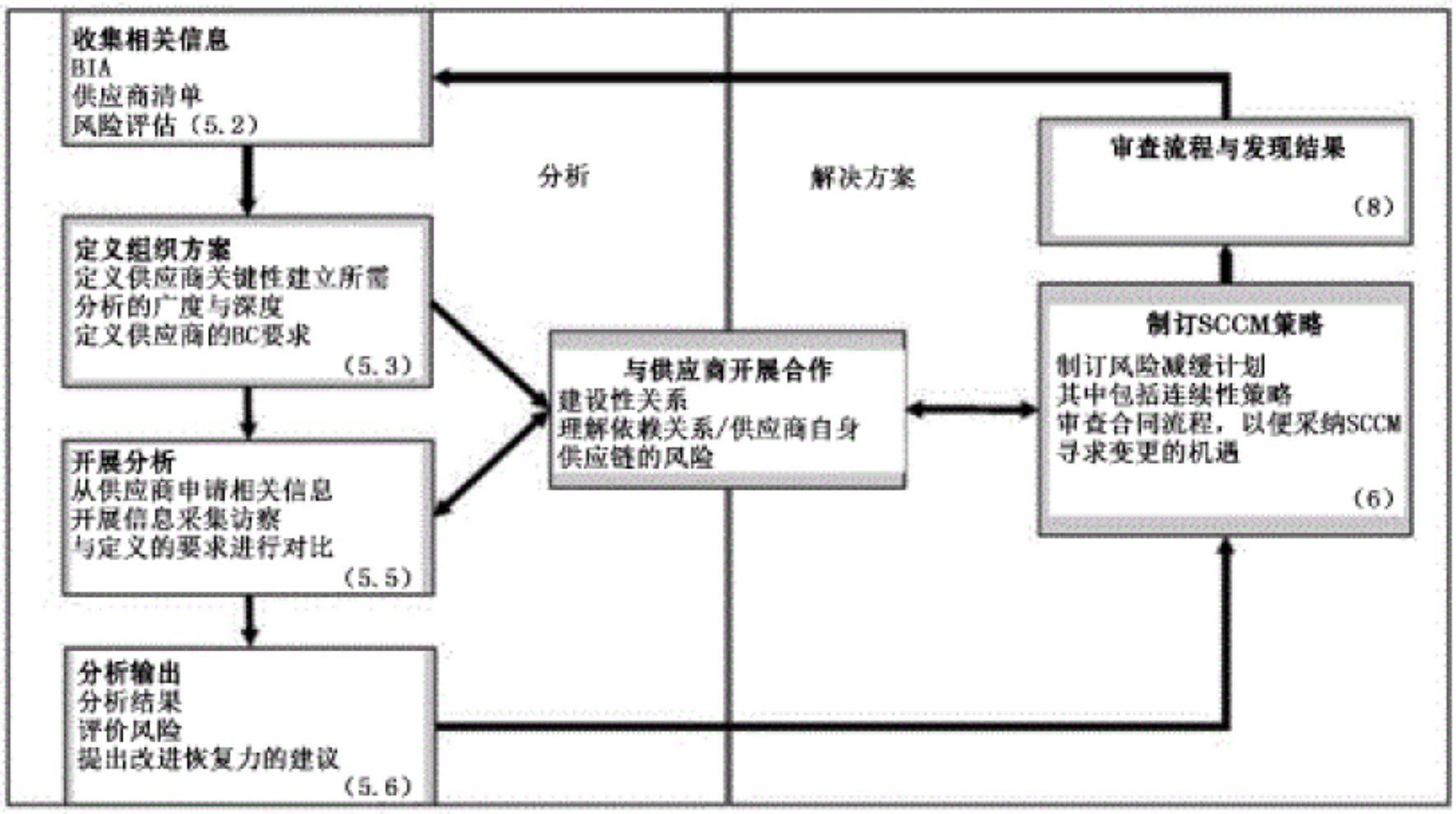

图 5　供应链分析流程图

5.5　开展分析

组织宜与供应商分享分析的基本原理及其潜在的好处，解释组织的需求和每个供应商的期望。

组织宜识别供应链的级别(见图 2)，从 BIA 中获取信息去识别高优先级活动或过程，MBCO 与 RTOs 及其依赖的供应商。如果综合考虑 BIA 以及供应链分析结果，那么任何供应中断对于组织造成的影响均宜是显而易见的。对于组织的每个供应商宜有如下评价：

——供应商提供产品或者服务的临界；
——供应商是否是该产品或者服务的唯一来源；
——供应商向组织交付产品和服务的能力中断的风险；
——供应商是否有到位有效的业务连续性安排；
——供应商对自身供应链风险的评估程度；
——组织在供应商的关键客户名单中的排名；
——供应商的 MBCO/RTO 是否与支持活动或进程的组织相一致。

宜采用基于证据的供应商评估方法，以支持维护 SCCM，其中包括：

——供应商文件化的 BIA、风险评估以及业务连续性计划；
——供应商文件化的保持与更新其连续性安排的过程；

——供应商文件化的演练计划与演练后报告以及事后报告。

对于大多数关键供应商而言，评审文档不足以证明连续性能力，宜连同现场考察以及演练观察结果，以便证实文档。

5.6 分析的输出

组织宜确保分析的输出是面向每位供应商的可以审计的、基于证据的报告。报告宜至少识别以下各项内容：

——供应商的连续性安排并证明其 BCM 安排对于被要求的 MBCO/RTO 范围内恢复能力是可信的；

——规定与组织预期是否相符；

——如何管理供应商供应链的连续性；

——对相关产品或者服务的威胁；

——改进建议。

5.7 供应链分析关键点

包括如下内容：

a) 供应链往往是广泛、复杂且相互作用、多层次的；

b) 选择供应连续性策略之前，有必要理解供应链及其对组织的风险；

c) 组织宜与供应商一起进行分析，同时该供应商应负责分析他们的下一级供应商；

d) 分析宜基于组织开发的同一套核心标准；

e) 标准应包括分析过程和对供应商的业务连续性要求；

f) 分析过程的主要输出包括对供应链和特定供应商带来的风险水平的整体评估；

g) 供应链是动态的，业务连续性需求宜内置采购策略和供应商关系管理流程；

h) 整个分析过程宜定期重复。

6 SCCM 策略

6.1 总则

一个适当的恢复策略(见 6.2)宜能被每个供应商辨识。选择最合适的一个或多个策略时 SCCM 需要考虑 4.6 所确定的挑战。组织宜使用分析结果(见 5.5)来确定以下内容：

——首选的供应商；

——产品或者服务的供给中断对业务的影响；

——每个供应商的临界，中断的容忍时间；

——理解每个供应商自身和其下级的供应链的连续性措施。

这里描述的选项并不相互排斥，减轻供应商带来的风险可能需要多种方法来实现。实现最终的解决方案需要时间，可能需要与一些供应商共同采用临时方法直到实现最优解决方案的机会出现，尤其在与供应商签订长期供应合同/协议时，在谈判时只有有限的条件去创造机会。

组织宜从丧失输出的角度来量化中断成本、客户补偿成本、违反规章制度可能导致的罚款的规模，或者采购替代性产品或者服务以便证明制订 SCCM 措施的相关成本的合理性。此外，还应当考虑中断的无形成本，比如导致丧失市场份额、丧失股票价值或者丧失竞争力的声望损失，以至于应实施减缓措施。

6.2 连续性策略选择

6.2.1 选择 1——接受现状

更容易被非关键供应商采用。供应商可采用投保来避免利润损失(这并不是业务连续性范畴,因为理赔时间远远落后于事件或者其他情况发生,不足以挽救组织)。

6.2.2 选择 2——减少依赖

减少对供应商的依赖,例如:

——有两个或更多的供应来源(见 6.2.3);

——采取措施延长事件对组织产生破坏性影响前的时间;

——建立替代方案:对关键供应商的风险管理方法落在实处,例如采用备用发电机以避免失去电力供应,开发多通道的通信系统来减少对单一渠道或供应商的依赖。

6.2.3 选择 3 ——增加韧性

开发独立于供应商的恢复策略,例如:

——采取相关方式,通过恢复组织的生产制造或交付能力(内包)来减缓丧失服务造成的损失;

——识别可替代的供应商,有备用的能够满足最小供应需求的供应商;

——与同行达成相互支持协议。

6.2.4 选择 4——与供应商合作

组织与每个供应商合作,提高韧性/可恢复性:

——与关键供应商发展合作关系,了解他们的安排,基于信任形成的伙伴关系将有利于供应链的加速恢复;

——明确地定义所需的绩效标准和评估过程;

——帮助/鼓励供应商改善其韧性/可恢复性;

——合同条款中包括的 SCCM 需求。

6.2.5 选择 5 ——撤销关系

如关键供应商不能提供一个合适的 SCCM,考虑取消合同。

6.3 供应合同包含 SCCM 能力

组织宜在采购流程中包括连续性要求,以确保供应商针对需要提供的产品或者服务而具备充分的 BCM 安排,以便长期交付 SCCM。采购流程中的连续性要求包括以下各项:

——在报价申请书中定义组织的 BC 要求;

——寻求 BC 安排的文档证据,并且在供应商选择流程中评价响应质量;

——建立标准合同条款,以便针对现有合同,尽早交付立即应用于新合同的选定的连续性策略;

——包括提交触发与通知策略,以及合同条款与服务水平协议的意外管理;

——规定合同中的某项要求,以便通知重要事件与信息,其中包括文件调取、计划审查、演习与文档修订;

——采纳联合演习的安排,并且在合同中分享吸取的各项内容;

——要求合同包括管理审查及/或 BC 安排审计等相关规定;

——鼓励供应商提供方案,以便评估其内部供应链中断的影响以及减缓其供应链中断风险所需采

取的措施：

——要求尽早通知供应市场的变化，此类影响可能危及 BCM 安排；

——规定未达成规定的 SCCM 标准而对于合同造成的影响，如提交流程以及可能的合同终止；

——限制供应商可能调用的不可抗拒力条款而非实施有效的 SCCM 安排。

注：不可抗拒力是合同中通常会包括的一种条款，该条款在特殊事件或者环境状况超出订约双方控制范围的情况下，免除订约双方的责任或者合同义务。特殊事件或者环境状况可以是战争、罢工、暴乱、犯罪或者从法律角度被描述为天灾的事件，如飓风、洪水、地震或者火山爆发。大多数不可抗拒力条款均不会完全免除订约一方的未履约责任，而是仅会在不可抗拒力期间暂停此类责任。

6.4 SCCM 所有权

组织宜识别供应商关系管理以及保障和监控供应链连续性保证情况的责任。此类责任宜与组织内部针对 BCM 的更大范围的安排紧密相连。

组织宜要求 SCCM 的管理权由负责购买产品或者服务的人员转交给管理合同或开展运营的相关人员。

组织宜确保采取的控制措施不会随着时间的推移而降级。如与两个供应商签订合同以提高韧性的时候，将供应商减为一个是节约成本的重要措施。

6.5 连续性策略选择关键点

包括如下内容：

a) 有一系列战略来增强供应链的弹性，最好的策略是识别并选择最重要的供应商。

b) 成本效益和选择策略可以减少单独供应商供应中断对组织造成的影响，如设置多个供应来源，增加持有关键资源的供应商的股份。

c) 在组织无法减轻影响的时候，应与供应商一同合作研制连续性解决方案。

d) 供应商应具备一个有效的业务连续性解决方案，供应合同中应包含供应链。在签订合同和现有的保证中，供应商可拿出这方面的凭证，这一点十分重要。

e) 合同/协议需要定义供应商和客户都可调用的信息交换程序和计划。

f) 应认识到最好的方法生效需要一定的时间，在此期间内可能需要采取部分其他方法减轻中断期。

7 供应链中断的管理

7.1 总则

按照第 5 章的规定对供应链进行了分析并按照第 6 章的要求制定适用的策略，为管理任何中断事件的适当过程做好准备。

与关键供应商保持深度合作十分重要，以确保连续性管理安排的可获得及有效。通过供应商关系管理达成这一目标的最有效方法是确保在各方之间进行定期和开放式的讨论以在组织和供应商之间建立伙伴关系。

对一旦意外事件发生各方将如何应对进行假设是一件容易的事情，但这些假设需要得到确认。

7.2 事件发生之前

组织的业务连续性计划宜包括以下各项：

——影响组织的供应商中断事件引发的限制或改变，如产品或者服务中断供应。

——供应商对组织给予支持的期望。

——组织立即做出响应的行动计划。

组织宜：

——邀请供应商参加与其提供的产品/服务相关的业务连续性演练；

——帮助供应商理解其产品或者服务供应的重要性，并使其能够识别出向一个备选场所供应的交付事宜。

——参加供应商提供产品/服务相关的演练，以获得供应商在中断事件发生时连续供应能力的客观保证。

——运用水平扫描，向组织预警可能影响供应链的风险；并且

——考虑由于外部事态引发的中断事件的间接影响，如由于劳工运动或疾病暴发造成行动受限，导致燃油短缺而出现的运输中断事件。

7.3 事件的发现与通报

提前发现具有破坏性的事态可以使响应高效、及时和适当。这要求组织与供应商保持一种开放的关系，鼓励其立即通报问题，识别在向组织提供产品/服务方面存在的任何问题和潜在影响。

如果关系的透明度低，供应商可能对其解决问题而不对客户造成影响的能力较为乐观，而不愿将中断或可能的中断告知其客户。延迟通报可能增加组织面临的轻微问题变成严重问题的风险，特别是供应商没有充分理解自身对于受到影响活动的重要性。

7.4 事件中

在事件过程中考虑的因素：

——在关键供应商和组织之间协调事件管理，以减少对供应商响应错误假设的可能性，并对组织的影响最小化；

——由于供应商的作业地点在地理、文化和政治等方面的差异而导致的任何影响；

——在事件的全过程中就现状和回归正常工作状态与供应商进行定期沟通的程序；

——供应商在外部沟通中避免发布“混乱信息”并导致信誉损害的方法；

——安排的互惠性质是当组织是事件的根源时，供应商需要对其受到中断影响的自身业务运行进行管理，并为促进组织的恢复提供支持。

7.5 业务恢复常态

业务恢复常态需要时间而且需要组织与运行受到影响的供应商协调行动。

组织宜从中断事件中获取经验教训，并且在减少未来事态对供应商与组织影响、改进组织与供应商之间的信息流等两方面得以提升。

组织宜处理好供应商在评审中与其他供应商分享敏感信息的担心，与那些对不涉及合同修改和没有相关费用的后续行动有抵触的供应商进行合作。

组织宜要求获取事件触发的行动信息，并跟踪其进展情况。

7.6 管理供应链中断的关键点

包括如下内容：

a) 将供应链连续性管理安排的细节纳入业务连续性计划；

b) 与供应商共同演练以促进协调和理解各方的事宜；

c) 确保获得议定的、使供应商尽早向组织发出事件或潜在事件预警的程序；

d) 在事件发生过程中确保一体化指挥与控制；

e) 协调外部沟通计划；

f) 事后组织一次关于发生了什么、应当汲取的经验教训并导致改进行动的全面的、共享的评审。

8 绩效评价

8.1 总则

作为常规供应商关系管理的组成部分，组织宜按议定的时间间隔对其关键供应商进行绩效评价。绩效评价宜覆盖持续的 SCCM 管理，并且包括对 SCCM 的监测、验证、确认和评审，以激励持续的改进和为供应链提供保障。

通过以下方法进行监测和评审有助于确保关键供应商一直保持良好的业务连续性安排：

——利用与供应商的定期会议，获得供应商运作或连续性计划相关的产品或者服务的更改情况的早期了解；

——监测供应链性能和识别潜在的事宜；

——建立供应商报告失效的升级触发和程序；

——识别关键供应商遭遇中断时任何“隐藏”的风险；

——促进供应商的最小业务连续性目标(MBCO)和恢复时间目标(RTOs)与组织的一致。

8.2 与供应商深度合作

组织宜通过以下方法将 SCCM 保障列为与供应商例行会商的项目：

——纳入供应商评审会议日程；

——共享的教育和培训工具；

——溯源策略；

——绩效指标的监测；

——突发事件应急预案演练；

——经过充分演练的触发与升级计划；

——突发事件发生时可以相互理解的命令与报告结构；

——协同演练方案。

8.3 实施 SCCM 绩效评价程序

组织宜持续实施一个 SCCM 绩效评价方案，包括：

a) 根据供应商的要求评审组织对 SCCM 能力的准则，这将取决于供应商关键性评估和每个供应商选择 BCM 的策略。

b) 保证过程包括：

1) 持续进行分析(见 8.4)；

2) 使用关键绩效指标(KPIs)/度量标准持续监测；

3) 设计和使用调查问卷/检查表/自我评价；

4) 当供应商不满足准则时使用升级过程；

5) 对组织的采购过程进行评审以确保包含了 BCM 要求；

6) 评审标准 SCCM 合同与附件条款，以确保其持续满足组织的需求。

c) 在合同与协议中应包含实施绩效评价的权利。当协议中不包括实施绩效评价的权利时，如果可能，宜增加。

8.4 持续分析

供应链和它所面临的风险是不断变化的，为了保持它的 SCCM，组织宜：

——建立分析供应链和监控不断变化风险的可重复过程；
——保持分析的及时性并且识别持续改进的机会；
——实施持续审查流程，以监控供应链变化和改进的实施情况；
——识别评审过程和将其纳入现有供应商关系管理过程的责任人；
——在溯源策略中添加 SCCM 要求；
——将供应商 SCCM 绩效评价过程纳入 BCM 审核范围。

8.5 绩效评价的输出

绩效评价宜关注结果。对供应商满足要求的能力进行评估，宜检查以下各项：
——供应商文件化的 BIA 分析、风险评估和业务连续性计划；
——供应商保持和更新连续性计划的文件化过程；
——供应商的演练计划、演练后及事后报告；
——文件化通报过程，包括可能受到影响的关键组织；
——文件化沟通计划，包含考虑到组织所受影响的统一的沟通与声明。
过程的收益：
——由于更好地了解和控制风险而对供应链的韧性信心更强；
——评估每个供应商符合组织 BCM 要求的程度；
——更早发现可能影响供应关系变化的迹象；
——识别供应商需要处理的能力差距；
——根据目标进行供应商监控和绩效测量。
组织宜在与供应商的 BCM 安排有重大事宜时，评审与供应商的关系和/或 SCCM 策略（见第 6 章）。

在实施绩效评价时，组织宜考虑如下：
——供应商可能会有很多希望确认 BCM 的客户，这可能导致高成本和供应商的混乱；
——绩效评价是反映一个特定的时间点的指标，所以项目需要定期回顾；
——绩效评价流程与实现补救措施的潜力可能导致增加成本。

8.6 绩效管理的关键点

包括如下内容：

a) 保护其高优先级活动与过程的 SCCM 条件被保持是组织的责任；
b) 供应商关系的所有者要有适当的触发和升级路径，以在关键供应商绩效产生变动时，及时预警和快速处理；
c) 通过评审会议定期与供应商深度合作是保持供应商关系的基础；
d) 将供应商纳入演练能揭示此前未知的、可以将其添加到双方工作计划中解决的风险；
e) 绩效评价包括 SCCM 安排的监测、验证、确认和评审，激励持续的改进和提供供应链的绩效评价。

参 考 文 献

[1] ISO 22313:2012 Societal security—Business continuity management systems—Guidance

[2] ISO 28000 Specification for security management systems for the supply chain

[3] ISO 28002 Security management systems for the supply chain—Development of resilience in the supply chain—Requirements with guidance for us

[4] ISO 31000 Risk management—Principles and guidelines

[5] BS PASS 7000:2014 Supply chain risk management—Supplier prequalification

[6] BS 13500:2013 Code of practice for delivering effective governance of organizations

[7] BS 65000:2014 Guidance on organizational resilience

中 华 人 民 共 和 国
国 家 标 准
公共安全 业务连续性管理体系
供应链连续性指南
GB/T 38299—2019/ISO 22318:2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019年11月第一版
*
书号:155066·1-64025

GB/T 38299-2019