ICS 03.100.01
A10

团　体　标　准

T/CCFAGS 020-2020

连锁经营企业突发事件应急及业务连续性管理指南

Guidelines for Emergency Response and Business Continuity Management of Chain Enterprises

2020-11-19 发布　　2020-11-19 实施

中国连锁经营协会　发布

目　次

前　言

本标准按照 GB/T 1.1—2020 给出的规则起草。

本标准由中国连锁经营协会提出并归口。

本标准起草单位：中国连锁经营协会、普华永道商务咨询（上海）有限公司、深圳纷来电子商务有限公司、沃尔玛中国投资有限公司、深圳美西西餐餐饮管理有限公司、星巴克企业管理（中国）有限公司、蕾碧裳品牌管理（上海）有限公司、苏宁易购家乐福公司、北京便利蜂连锁商业有限公司、联华超市股份有限公司。

本标准主要起草人：张静、彭建真、姚皓轩、程堂根、臧游、王英、王凌俊、刘江红、李炯、徐颖、陈忠俊、曲强、徐晓一、刘洋、林森。

连锁经营企业突发事件应急及业务连续性管理指南

1 范围

本标准规定了连锁经营企业事件应急及业务连续性的组织架构及职责、业务连续性计划、突发事件监测与预警和准备、应急处置、业务恢复、培训与演练。

本标准适用于连锁经营企业（以下简称：企业）为有效应对自然灾害、事故灾难、公共卫生事件、社会安全事件以及企业运营中断等突发事件的应急及业务连续性管理。

2 规范性引用文件

以下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。

GB/T 30146 公共安全-业务连续性管理体系要求

GB/T 20988 信息安全技术 信息系统灾难恢复规范

SB/T 10806 零售店铺应急处理指南

3 术语和定义

下列术语和定义适用于本文件

3.1

突发事件 emergency

突然发生，没有预警且发生时间短。该事件在现有的业务流程中没有相关现行办法支持商业决策，已造成或者可能造成严重危害，需要在短时间内做出决策采取应急处理措施以应对的事件。

3.2

业务连续管理 business continuity management

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。该过程对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、剩余、品牌和创造价值的活动。

[来源：GB/T 30146-2013 定义 3.4]

3.3

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

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。

[来源：GB/T 30146-2013 定义 3.5]

3.4

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得形成文件的程序。

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。

[来源：GB/T 30146-2013 定义 3.6]

3.5

风险评估 risk assessment

风险识别、风险分析和风险评价的整个过程。

[来源：GB/T 30146-2013 定义 3.50]

3.6

业务影响分析 business impact analysis

分析业务中断可能给组织带来影响的过程。

条目注释 1:结果是对业务连续性要求的陈述和证明。

[来源：GB/T 30146-2013 定义 3.8]

3.7

恢复时间目标 recovery time objective

事件发生后到下列活动完成之间的时间段。

----产品或服务必须恢复，

----或活动必须恢复，

----或资源必须复原。

[来源：GB/T 30146-2013 定义 3.45]

3.8

恢复点目标 recovery point objective

为使活动能够恢复进行，而必须将该活动所用的信息恢复到某时间点。

[来源：GB/T 30146-2013 定义 3.44]

3.9

灾备中心 backup center for disaster recovery

备用站点 alternate site

用于灾难发生后接替主系统进行数据处理和支持**关键业务功能（3.6）**运作的场所，可提供**灾难备份系统（3.3）**、备用的基础设施和专业技术支持及运行维护管理能力，此场所内或周边可提供备用的生活设施。

[来源：GB/T 20988—2007 定义 3.1]

3.10

灾难恢复 disaster recovery

为了将信息系统从灾难(3.8)造成的故障或瘫痪状态恢复到可正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

[来源：GB/T 20988—2007 定义 3.9]

4 组织架构及职责

4.1 日常管理组织架构

企业应在制定业务连续性管理制度，明确业务连续性日常管理的组织构架及职责，并绘制组织架构图，于工作场所显著位置公示。日常管理组织架构应由法定代表人或主要负责人、高级管理层、业务运营部门、信息技术部门、支持保障部门和分支机构组成。

4.2 日常管理组织架构职责

法定代表人或主要负责人是业务连续性管理工作的责任人，对业务连续性管理工作承担最终责任，其主要职责包括：

a）负责业务连续性管理战略、政策和程序审核和批准；

b）负责高级管理层业务连续性管理职责的审批，定期听取高级管理层关于业务连续性管理工作的报告，并对其履职情况进行监督、评价；

c）负责业务连续性管理工作相关审计报告审批；

d）对经费预算进行审核并批准。

高级管理层负责执行经法定代表人或主要负责人批准的灾难恢复管理政策，其主要职责包括：

a）负责业务连续性管理总体战略、政策和程序的组织制定、定期审查及监督执行；

b）对业务连续性管理策略进行审阅并批准；

c）负责明确各部门职责、报告路线及报告时效，监督业务连续性管理策略的执行情况，督促各部门履职，确保业务连续性管理体系正常运行；

d）确保配置充足资源保障业务连续性管理体系实施。

企业应设立业务连续性管理主管部门具体负责组织协调业务连续性管理事宜。其主要职责包括：

a）负责执行灾难恢复管理总体战略、政策和程序；

b）针对风险评估组织开展并进行审核；

c）协助业务连续性管理主管部门开展业务影响分析；

d）组织制定灾难恢复策略，并提交高级管理层审批；

e）组织制定并审核灾难恢复预案，协调各部门制定并审核专项预案；

f）负责演练计划制定，并组织相关部门执行演练；

g）组织开展并审核灾难恢复工作评估与改进；

h）组织开展业务连续性管理文化建设及相关培训；

i）完成职责范围内其它与业务连续性管理相关的工作。

业务运营部门、信息科技部门、支持保障部门，在业务连续性主管部门的统一组织协调下，负责日常管理工作，其主要职责如下：

业务运营部门：

a）负责对本部门归口管理业务进行业务影响分析和风险评估；

b）在新业务上线前，针对新业务开展业务影响分析工作，对于重要业务应按照相关要求确定恢复目标和恢复策略；

c）确定重要业务恢复策略，负责开发信息系统中断场景下的业务专项应急预案；

d）配合制定演练方案，参与演练实施与总结，对本部门归口管理的重要业务开展灾难恢复演练、评估与改进工作；

e）负责本部门业务连续性管理文化建设及相关培训；

f）完成本部门职责范围内其它与业务连续性管理相关的工作。

信息科技部门：

a）负责分析业务影响分析结论，并结合信息系统现状与规划，确定信息系统恢复目标；

b）负责信息系统资源风险评估，保障信息系统资源有效性和可用性；

c）根据信息系统恢复目标，制定灾难备份中心及系统建设策略与方案，明确信息系统恢复策略；并在灾难恢复预案的框架下，制定并完善信息系统专项应急预案和操作手册；

d）负责进行业务连续性管理资源建设、管理和维护；

e）负责信息科技范畴内的灾难恢复演练、评估与改进工作，并在日常工作和演练中关注与业务运营部门、支持保障部门和分支机构应急预案的有效衔接；

f）负责本部门业务连续性管理文化建设及相关培训；

g）完成本部门职责范围内其它与业务连续性管理相关的工作。

支持保障部门：

负责业务连续性管理工作的相关保障，为日常管理和应急管理提供人力、物力、财力等资源保障及安全保障、媒体公关、法律诉讼等工作。支持保障部门包括办公室、人力资源部门、公共关系部门、财务部门、法律合规部门、后勤部门、保卫部门等。

4.3 应急管理组织架构

灾难恢复应急管理组织架构，应包括应急决策层、应急指挥层、应急执行层。

应急决策层由高层管理者组成，负责重大业务运营中断事件应急预案的启动、应急处置过程中重大事项决策，例如批准灾难恢复方案、批准向上级部门和监管部门的报告、对外通报等。

4.4 应急管理组织架构职责

应急指挥层由企业各相关部门负责人组成，主要职责如下：

a）负责指挥和组织协调应急处置工作，督导应急处置措施的具体实施；

b）处置过程中向应急决策层报告处置进展情况，处置结束后向高级管理层报送总结报告；

c）其他处置过程中需领导和指挥的事项。

应急执行层由业务运营部门、信息科技部门、支持保障部门和分支机构工作人员组成，其主要职责如下：

业务运营部门：

a）按照业务专项应急预案，开展业务应急处置工作，尽量降低业务运营的负面影响；

b）组织一线或分支机构业务人员做好客户安抚和解释工作，防范和消除客户负面情绪和过激行为；

c）向应急指挥层报告业务应急处置进展情况和事态发展情况；

d）其他需执行小组参与处置的事项；

e）预估事件的影响时间，以及所产生的额外费用。

信息科技部门：

a）负责开展信息系统中断问题排查、抢修和调整等具体处置工作；

b）负责执行信息系统灾难恢复预案；

c）向应急指挥层报告信息系统应急处置进展情况和事态发展情况；

d）收集分析突发事件处置过程中的数据信息和日志；

e）其他需执行小组参与处置的事项。

支持保障部门：

a）提供突发事件处置过程中所需人力、物力、财力等资源保障；

b）及时、准确向监管机构、股东、客户、媒体、社会公众等报告或披露事件信息；

c）配合业务运营部门、一线及分支机构对受影响客户进行解释和安抚工作；

d）做好秩序维护、安全保障、法律咨询和支援等工作；

e）其他为降低突发事件负面影响或损失提供的支持保障等。

分支机构：

a）根据应急指挥层的要求及应急预案处置流程，开展突发事件的应急处置工作；

b）做好客户安抚和解释工作，防范和消除客户负面情绪和过激行为；

c）向主管部门报告应急处置进展情况和事态发展情况；

d）记录突发事件处置过程中的数据信息和日志；

e）其他需参与处置的事项。

4.5 组织架构优化

4.5.1 评估和更新

企业建立业务连续性管理体系后，应每年定期进行评估和更新，对体系中各环节进行持续改进。

4.5.2 临时变更

当企业内、外部环境发生变化时，应根据变化及时更新业务连续性管理体系。可能引起业务连续性管理制度临时变更的情景包括但不限于：

a）上游供应链监管制度发生变化，并可能影响供应链稳健性，或可能导致与供应商合作关系发生变化；

b）监管制度或行业质量控制文件发生变化，可能影响业务开展模式；

c）外部突发事件出现，且在短时间内无法消除，对业务开展造成影响并预计短时间内无法消除。

4.5.3 组织架构变更

企业应在组织构架发生变更时，应及时更新业务连续性管理体系组织构架，以保持业务连续性管理体系与整体管理的兼容。

5 业务连续性计划

5.1 需求分析

5.1.1 总则

企业宜建立、实施和保持一个正式和文件化的业务影响分析和风险评估过程。通过业务影响分析和风险评估过程来了解企业，对企业的了解为有效的业务连续性提供了基础。

企业通过向客户交付产品和服务来达成其目的。因此，认识到这些产品和服务（及相关活动）随着中断时间对企业的目标和运行产生的负面影响是非常重要的。理解互相关系和支持产品和服务的活动的资源要求以及他们所受的威胁也是很重要的。

5.1.2 风险评估

企业应建立风险评估过程，对组织优先活动和支撑这些活动的过程、体系、信息、人员、资产、供应商和其它资源中断的风险进行系统的识别、分析和评估。

5.1.2.1 确定风险分析目标

明确支持重要业务开展的关键资源，评估其可能面临的风险场景，为业务连续性管理策略、体系规划与实施提供科学依据。

可能的风险场景包括但不限于：

a）自然灾害：地震、海啸、火灾、洪涝、泥石流等；

b）人为损害：黑客攻击、恐怖袭击等；

c）外部服务中断：供应商、物流等第三方无法合作或提供服务、国家或区域政策限制导致服务不能提供等；

d）内部运营中断：如信息系统故障、配套设施和资源不可用、内部人力等资源无法调用运营中断等；

e）公共卫生突发事件：大型传染病疫情、动物疫情、中毒等。

5.1.2.2 确定风险评估范围

风险分析范围为连锁经营企业所有业务和内部管理流程。

风险分析对象为业务运营的所依赖的关键资源，是在风险发生后应当保护的对象。关键资源主要包括：数据中心基础设施，网络及通讯线路、硬件、软件、数据、文档、人员、办公场地、办公设备以及外部服务商等。

5.1.2.3 风险评估方法

企业应根据不同的商业场景和业务需求，选择符合自身的标准，如《信息安全技术-信息安全风险评估规范》（GB/T 20984—2007）、《中央企业全面风险管理指引》（国资发改革[2006]108 号）、《Risk Management - Guidelines》（ISO30000）等，并根据所选标准中提出的风险评估的基本概念、要素关系、分析原理、实施流程和评估方法开展风险评估工作。

企业在采用新技术时，应着重评估新技术服务和设备提供商的风险管控能力，并根据新技术架构特点评估可能导致企业运营中断或服务能力下降的风险场景，制定相应的防控措施。

5.1.2.4 风险评估结果

风险评估工作应以书面报告形式体现，报告应当包括以下内容：

a）分析关键资源所面临的各类威胁以及资源自身脆弱性，确定资源面临的风险；

b）根据风险类型制定降低、缓释、转移等应对策略。依据防范或控制风险的可行性和残余风险的可接受程度，确定风险防范和控制措施。

5.1.2.5 持续改进

企业应根据业务连续性管理体系建设要求，确定风险分析周期，至少每三年进行一次全面风险分析。当关键资产发生重大变化，或发生重大灾难事件后，应立即启动风险分析工作。

5.1.3 业务影响分析

5.1.3.1 确定业务影响分析目标

通过深入理解组织业务环境，评估业务运营中断造成的影响，判断对中断的容忍程度，分析业务活动业务连续性管理需求，评估信息系统恢复优先等级和恢复指标，确定支撑关键业务基本运营的必要技术资源，为业务连续性管理策略制定和资源建设提供基础数据输入。

5.1.3.2 确定业务影响分析范围

企业应将所有对外提供服务的业务活动作为业务影响分析范围。

5.1.3.3 业务影响分析方法

5.1.3.3.1 业务基本情况调研

收集、分析业务活动情况,包括:

a）业务活动的开展情况、职能部门、正常处理流程等相关信息;

b）业务活动的政策法规要求;

c）业务服务渠道、客户类型、业务上下游外部机构;

d）业务活动所需数据及其分布和存放情况;

e）业务运营时段、特点、时效性要求、业务量及峰值时间;

f）业务活动之间的关联关系等。

5.1.3.3.2 评估业务中断影响

针对业务基本情况，评估业务中断造成的影响。影响类型包括财务损失和非财务损失：

a）财务损失包括：业务中断对企业造成的直接财务损失和间接财务损失；

b）非财务损失包括：业务中断对企业造成的业务量降低、客户投诉、企业声誉、合同违约、监管和行业影响等；

c）分析信息系统业务数据丢失对业务运营造成的影响，评估业务活动对数据丢失的容忍程度。

5.1.3.4 业务影响分析结论

业务影响分析工作应当以书面报告形式体现，其结论包括：

a）确定信息系统恢复优先级和恢复指标:根据业务中断影响评估，结合信息系统架构特点，确定信息系统恢复优先等级和恢复指标恢复时间目标、恢复点目标；

b）确定重要业务活动所必须的最小资源和获取渠道:根据业务中断影响评估，确定重要业务活动所要求的最小资源，资源类型包括：数据中心基础设施，网络及通讯线路、硬件、软件、数据、文档、人员、办公场地、办公设备以及外部服务商等。

5.1.3.5 持续改进

企业应明确业务影响分析周期要求，至少每三年开展一次全面的业务影响分析。当开发新业务、新产品，或业务和系统发生重大变化时应当同步开展业务影响分析工作。

5.2 业务连续性策略

企业应根据业务影响分析和风险分析结论，制定差异化的业务恢复策略，主要包括关键资源恢复、业务替代手段、信息系统数据追补和恢复优先级别，及其他需列明的重要事项。

5.3 计划框架

企业应依据业务恢复目标，制定覆盖所有重要业务的业务连续性计划。主要包含如下内容：

a）计划的目标、定义和使用场景；

b）应急人员及职责，企业应根据业务连续性应急管理的组织架构明确具体应急人员及其职责；

c）计划覆盖的经营范围，企业应结合风险评估和业务影响分析结果，结合风险偏好和风险承受能力，确定业务连续性计划覆盖的经营范围；

d）计划未覆盖的剩余风险，企业应明确现行业务连续性管理体系未覆盖的剩余风险，并确保该剩余风险有相应的应急预案；

e）业务连续性计划的执行时间表，企业应制定总体业务连续性计划的执行时间表，明确关键节点，在企业层面推进业务连续性管理体系建设。

5.4 评估与更新周期

在制定业务连续性计划时，企业应明确对计划的定期审核评估时间，同时应在计划中明确，当发生内、外部环境、监管等的重大变化时，对业务连续性计划的及时更新。临时更新触发条件包括但不限于：

a）整体组织架构发生变化；

b）主要业务发生重大变化；

c）供应链结构发生重大调整；

d）相关法律法规发生重大变化；

e）外部重大突发事件发生，并预计在短时间内无法结束。

5.5 评估与更新程序

企业应在业务连续性计划中明确对计划更新调整的程序，确保计划的调整和更新具有相应的授权和审批，保证业务连续性计划的实施和业务连续性目标的实现。

5.6 预案开发与测试

5.6.1 预案体系

应急预案是为确保在发生运营中断事件时关键业务能够快速恢复而事先制定的一系列工作流程、措施、程序或操作手册的总称。

应急预案体系一般分为总体预案、业务专项恢复预案、信息系统专项恢复预案以及保障类应急预案。

总体应急预案是企业应对运营中断事件的总体方案，应当包括总体组织架构、风险描述、应急预案体系、运营中断事件分级、各层级预案的定位和衔接关系及对运营中断事件的预警、报告、分析、决策、处理、恢复等处置程序以及应急保障和应急预案的管理。主要内容应包括：

a）整体应急管理体系组织构架及职责分工；

b）应急预案启动及停用适用条件；

c）应急处置原则和策略；

d）突发事件通用响应流程；

e）内、外部沟通危机沟通机制。

专项应急预案应根据风险评估的结论，选取突发事件场景，明确在不同场景下的应急流程和措施。业务条线的专项应急预案，应当注重调动内部资源、采取业务应急手段尽快恢复业务，并和科技部门、支持保障部门的应急预案有效衔接。主要内容应包括：

a）应急组织架构及各部门、人员角色、权限、职责分工；

b）信息传递路径和方式；

c）运营中断事件处置程序，包括预警、报告、决策、指挥、响应、回退等；

d）运营中断事件处置过程中的风险控制措施；

e）运营中断事件的危机处理机制；

f）运营中断事件的内部、外部沟通机制和联系方式；

g）应急完成后的还原机制；

h）预案的生效时间与实施成本。

5.6.2 预案开发和测试要求

预案的开发和执行是持续改进的过程，应当进行定期地维护和审核。同时，为保障预案的可用性和可操作性，应进行测试和演练。

5.6.2.1 预案保存与分发

a）经过审核和批准的预案，应由专人负责保存与分发；预案应当以多种形式的介质拷贝并保存在不同安全地点，确保突发事件发生后能够快速获取。

b）预案的调用需进行严格授权。

5.6.2.2 维护和变更管理

a）建立预案的定期演练、评审和修订制度；

b）预案涉及的内容发生重大变更后，应立即更新预案；

c）演练后应根据演练评估结论，立即更新预案；

d）每年应至少组织一次预案的审查和批准工作；

e）预案的教育和培训应贯穿业务连续性管理规划和实施的全过程。

6 突发事件监测与预警、准备

6.1 事件监测

企业应在业务连续性管理体系中建立事件监测机制，及时发现可能导致突发事件发生的信息。事件监测主要包括：

a）可能导致企业现行运营机制、产品或服务在未来不合规的外部监管制度、法律法规变化；

b）可能影响企业运营的外部事件，如大规模地震灾害、上游供应商被监测机构监测判定为质量安全不合格、地区局部动乱等；

c）在重大业务和社会活动等关键时点，或在业务功能、关键资源发生重大变更时，应当加强风险监控和预警。

6.2 事件初始响应

6.2.1 通知通报

企业应在突发事件管理中建立通知通报制度，在突发事件发生时，相关部门、人员应按照通知通报制度流程及时进行上报。通报人员职责及通报内容包括但不限于:

a）突发事件发生时，应在及时实施人员及财产抢救同时，第一时间进行通知通报；

b）突发事件的发生及相关情况；

c）相关部门及人员应根据应急预案及时联络相关部门协作部门，寻求相关资源支持；

d）当涉及外部相关方时，应急管理层应及时决定是否通知相关方相关信息，是否寻求外部协助；

e）当威胁供应链稳健性时，应急管理层及时进行处置，如启用备用供应商储备、第三方紧急供货等；

f）当涉及向监管报送报告时，有关管理层应及时向有关监管机构就突发事件的发生及处置进行报告。

6.2.2 人员及财产抢救

企业应在突发事件管理中建立人员及财产抢救制度，在突发事件发生时，相关部门、人员应在保障人员安全前提下，依照人员及财产抢救制度，对重要资产进行抢救，降低损失。

6.3 事件分级与预判

企业在建立应急预案体系时，应根据风险评估和业务影响分析结果对突发事件进行分级，明确不同级别突发事件的相应管理层级，以便当突发事件发生时，相关部门及人员遵循“统一

指挥、分类管理、分级处置、快速响应”的原则，对突发事件级别和影响程度进行预判，提高突发事件发生时的决策、反应速度。

突发事件应该按照相关法律法规，行业要求和国家标准进行突发事件分级，分级方式应选择符合自身实际情况和行业特点的模式：

a）按照公共事件分级进行处置：当应急事件涉及公共事件时，事件分级标准应当参照政府公共事件分级进行评估并执行应急预案制定；

b）按照受影响的业务条线和店面数量：事件分级标准应当根据受影响的业务条线或店面数量评估突发事件级别制定；

c）按照财务损失计量：事件分级标准应当根据财务损失评估突发事件级别制定；

d）按照受影响的客户数量：事件分级标准应当根据受影响的客户数量评估突发事件级别制定。

7 应急处置

7.1 人员安全保障

7.1.1 人力保障策略

总体预案中应规定人力保障措施，确保人力资源充足。人力保障措施包括但不限于：应急人员响应制度、职责分工、备用专家召集名单及召集计划和人员调度授权流程等。

7.1.2 安全保障策略

总体预案中应规定安全保障措施，明确突发事件发生时人员在救治、疏散、集合、转移和安置过程中的安全措施；

7.2 重要财产保障

总体预案中应规定重要财产保障措施，规定重要财产如楼宇场地、重要信息资产等财产的保障措施，确保重要财产安全。

企业应提前制定突发事件中，紧急财务资金审批流程，设立突发事件备用金，确保财务资金充足。

7.3 品牌保护保障

总体预案中应规定品牌保护保障措施，通过提前对可能发生的突发事件制定相应的对公、对客公告模板，加快突发事件发生时的反应速度，设立舆情监测措施，及时发现潜在舆论威胁等方式确保品牌价值不受影响或降低损失。

7.4 危机沟通

企业应当将危机沟通纳入应急事件管理，以便及时控制外部舆情或获得内外部援助等。危机沟通对象应涵盖所有受影响利益相关方沟通策略包括，

a）编制紧急联络手册，明确利益相关方的联络方式及沟通内容；

b）当应急情景涉及客户时，应制定相应通知或公告模板；

c）当应急事件情景涉及外部监管或政府机构时，企业应当明确与监管或政府的沟通方式、内容及报送要求等，以保证自身应对措施符合法律法规及监管要求，并在必要时获得相关协助。

7.5 舆情控制

7.5.1 媒体公关保障策略

在突发事件发生时，企业应当按照应急处置预案，开展合理宣传解释工作，防止不实信息导致声誉受损，消除社会疑虑，化解纠纷。媒体公关保障策略包括但不限于：

a）加强和公众、政府、组织、媒体的沟通，由公关指定负责人及时通过媒体通报突发事件处置进展，进行舆情控制；

b）及时就突发事件与受影响客户进行沟通，提出解决方案；

c）制定突发事件公示模板，及时向社会公告。

7.5.2 第三方机构保障策略

企业应与第三方专业机构建立危机公关相关合作，利用第三方专业知识及渠道，开展合理宣传解释工作，防止不实信息导致声誉受损，消除社会疑虑，化解纠纷。

7.6 损失评估与决策

企业应根据突发事件的性质和状态，组织评估人员对受影响的区域或业务进行损害性评估并进行记录，确定损害造成的业务中断影响区域、影响范围和影响时间。

应急决策层应根据突发事件的评估结论、性质特征和判定标准进行突发事件的等级评估，并根据已制定的相应的应急处置措施，进行相应的决策分工，降低突发事件造成的经济及非经济损失。

8 业务恢复

8.1 业务运营恢复

8.1.1 线上、线下运营恢复策略

企业制定线上及线下运营的恢复策略，内容包括但不限于：

a）业务运营恢复的启动及停用条件、职能部门及相关负责人职责分工、内、外部沟通流程、资源需求清单等；

b）涉及供应链、物流等第三方供应商时，应制定相应的供应商服务及供货中断情景下的紧急供货制度及备用物流制度，保证配送的及时性；

c）制定人力资源保障制度，在线下运营受到突发事件，冲击且短时间内无法恢复正常运营时，保障企业人力资源利用率。

8.1.2 IT 恢复策略

在信息系统中断时，评估是否进行本地恢复或启用灾备中心进行信息系统灾难恢复的原则：

1．不考虑灾备恢复，一般只考虑启用本地恢复

a）对数据中心主机房场地不造成破坏，只造成生产系统短时间不能运行或系统资源不能被访问；

b）在短时间内可以由本地恢复的事件，如计算机主机设备、网络通讯设备、供电设备的某一部件损坏等；

c）由应用软件错误造成的系统中断；

d）黑客攻击。

2. 优先考虑启用本地恢复

a）短时间的局部电力故障、短时间的局部通讯故障；

b）设备故障、数据库系统故障、操作系统故障；

c）人为操作失误、人为蓄意破坏、病毒。

3. 考虑启用灾备中心进行恢复

a）较长时间的局部电力故障、较长时间的局部通讯故障；

b）设备故障、数据库系统故障、操作系统故障；

c）人为操作失误、人为蓄意破坏、生产中心机房场所倒塌、盗抢、爆炸、恐怖袭击。

8.2 场地恢复

8.2.1 场地恢复策略

企业应在相关应急预案中，制定场地恢复策略，当场地恢复到可正常使用状态时，实行场地回迁。场地恢复策略包括：

a）在办公场地与备用场地间转场流程；

b）支持场地恢复所需最小资源清单；

c）职能部门及相关负责人职责分工；

d）内、外部沟通流程；

e）备用场地具体地址及情况；

f）场地回迁流程，如业务信息备份及回迁、业务验证和数据追补等；

g）资料的形成及存档等。

8.2.2 物资保障策略

企业应建立物资保障制度，以保障在突发事件发生时，物资充足，能及时反应并控制风险的扩散。物资保障制度包括业务恢复所需的最小物资支持清单、基础资源恢复措施、第三方短期供货计划和备用物流服务计划。

8.3 供应链恢复

企业应制定供应链恢复策略，降低突发事件导致供应链中断对业务的影响。供应链恢复策略包括：建立供应商紧急联系机制、第三方短期供应协议、建立备用供应商储备计划和供应链恢复流程。

9 培训与演练

9.1 培训

a）企业应为所有员工提供业务连续性的专业培训。培训形式可根据企业的自身条件选择内部培训或聘请外部机构培训；

b）应按照业务连续性日常管理及应急管理要求为关键岗位和关键角色提供特殊的岗位培训；

c）应对每次培训的结果进行记录和评估。

9.2 演练的目标及形式

9.2.1 演练的目标

d）验证应急预案的有效性，并进行完善；

e）提高业务、信息科技及保障团队等参演人员的应急处置能力和实际切换能力。

9.2.2 演练组织形式

演练应当根据演练内容的复杂程度、演练目的以及实际情况选择桌面演练、模拟演练和实战演练等方式，控制演练风险。演练计划应当采取事前通告的计划性演练或非事前通告的非计划性的演练。

a）桌面演练。组织相关人员，以会议形式模拟各种突发事件场景，参与人员集中讨论应急响应和恢复流程中的管理与指挥协调，而不进行实际操作，以验证应急预案的决策和指挥能力；

b）模拟演练。模拟突发事件场景，利用灾难备份系统、备用场地、备用设施等恢复资源，按照应急响应及恢复预案，模拟系统切换恢复操作，在模拟演练期间模拟系统通常不对外提供真实服务，一般在非营业时间进行；

c）实战演练。模拟突发事件场景，利用灾难备份系统、备用场地、备用设施等恢复资源，按照应急响应及恢复预案，实际完成系统切换，并恢复业务运营的演练，以验证各类资源在应急状态下的可用性。

9.2.3 演练频率

演练应当定期展开，频率要求至少三年覆盖全部重要业务。

9.3 演练过程管理

9.3.1 制定演练方案

演练方案主要内容应包括但不限于下列事项：

a）演练组织。明确参与演练的所有人员及其职责。演练参与人员一般包括演练领导小组、演练指挥小组、演练执行小组、演练保障小组等，还应当包括演练观摩、评估等其他人员；

b）演练场景设计。设计演练场景，确定演练方式，明确演练的范围，演练场景应参考应急预案的场景进行设计；

c）演练评估方法。通过观察、体验和记录演练活动，比较演练实际效果与目标之间的差异，总结演练效果和不足；

d）演练实施方案。应包含演练实施的时间、地点、实施流程及详细的实施步骤。对于重大综合性演练，应编写演练脚本，描述演练事件场景、处置过程、执行人员等；

e）演练风险分析。演练方案中应对演练实施过程中的潜在风险及可能导致的结果进行识别和分析。并针对性的制定应对风险和处置风险的措施和机制；

f）演练准备。演练实施要求具备的技术、后勤保障、经费保障、基础设施（如：演练场地、演练工具等）、安全保障等。

9.3.2 演练培训

在演练开始前由演练牵头方组织演练动员和培训，确保所有演练参与人员掌握演练规则、演练情景和各自在演练中的任务。

a）培训发起方为演练牵头部门，负责根据演练方案制定演练培训与动员计划。明确培训开展的时间、地点、培训内容和培训对象；

b）培训对象为演练参与人员；

c）培训内容是由培训发起方根据演练方案制定的内容，应包括演练的目标、演练场景、演练实施方案，演练参与人员的角色和职责、应急技能及个人安全保护的说明，演练操作流程、话术等演练相关内容。

9.3.3 演练实施

a）演练指挥小组负责演练实施全过程的指挥控制。按照演练方案要求，演练指挥小组指挥各参演人员，完成各项演练活动；

b）演练执行、保障小组人员应根据控制消息和指令，按照演练方案规定的程序开展应急演练，完成各项演练活动；

c）演练实施过程中，要安排专门人员，采用文字、照片和音像等手段记录演练过程。记录内容主要包括演练实际开始与结束时间、演练过程实施情况等内容；

d）演练完毕由演练领导小组宣布演练结束，演练实施过程中如出现突发事件，经演练领导小组决定，应当提前终止演练。

9.4 演练的总结及报告

a）现场评估。在演练的一个或所有阶段结束后，由演练评估人员在演练现场有针对性地进行评估。内容主要包括本阶段的演练目标、参演队伍及人员的表现、演练中暴露的问题等；

b）事后总结。在演练结束后，由演练组织者根据演练记录、演练评估、应急预案及演练方案等材料，对演练进行全面总结，并形成演练总结报告，针对演练中发现的问题，制定行动措施，确定负责人和完成时间并定期回顾。

c）演练总结报告。的内容包括:演练目的、时间和地点、参演单位和人员，演练方案概要、发现的问题与原因以及改进有关工作的建议等。对过程中暴露的问题应经过分析原因，确定解决方案并进行相应的整改，演练报告应当经演练组织部门和参与部门审核确认，提交备案。

d）演练归档。演练结束后应将演练计划、演练方案、演练过程记录文件、演练总结报告等资料归档保存。

e）应根据演练评估结论对灾难恢复预案进行维护和更新,并对后续演练策略和计划进行必要的调整。

附录

（资料性）

连锁经营企业典型场景应急处置预案要点见表

序号	突发事件/风险场景分类	突发事件/场景描述	造成影响	影响范围	应急处置要点
1	自然灾害类	台风/暴雨/洪水/山体滑坡/暴雪	运营中断/财产损失/人身伤害	单一/区域门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 安排联络小组与所有员工保持联系，提前发布内部预警信息； ➢ 持续关注天气预警预报； ➢ 准备沙袋防止门店进水； ➢ 采取保护措施保护商品； ➢ 确保应急照明系统正常运作； ➢ 电气设备采取保护措施； ➢ 现金、贵重商品、文件妥善保存； ➢ 相关财产损失向保险公司报备。
2	自然灾害类	地震	运营中断/财产损失/人身伤害	区域门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 远离门窗和易碎物品、堆高商品，靠近承重立柱或在桌子等可承重设施下躲避； ➢ 视情况通过广播或便携设备通知员工和顾客从就近出口撤离； ➢ 相关财产损失向保险公司报备。
3	事故灾难类	火灾	运营中断/财产损失/人身伤害/政府处	单一门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 设置火灾专项应急小组，做好训练和演习； ➢ 使用灭火器、消防水枪等设备扑救初级火灾；

序号	突发事件/风险场景分类	突发事件/场景描述	造成影响	影响范围	应急处置要点
			罚/品牌形象受损		➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 立即通过广播及员工安抚顾客，疏散店内人员，确保所有人员有序撤离； ➢ 疏散后集合清点当班人数； ➢ 根据现场情况，组织工作人员清理消防通道，引导消防车施救； ➢ 围封现场，协助调查事故原因，统计损失，申报保险； ➢ 形成总结报告并制定改进措施。
4	事故灾难类	煤气/燃气泄漏	运营中断	单一门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 发现情况，初步判断问题，并视情况是否疏散顾客及员工； ➢ 配合物业查找泄漏点； ➢ 必要情况下拨打火警电话。
5	事故灾难类	门店营业期间出现停电	运营中断	单一门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 管理人员到位控制好管辖区域，重点控制现金房、收银区和各出入口； ➢ 准备好备用手照明设备； ➢ 安抚员工和顾客情绪稳定，保持走道通畅； ➢ 检查电梯是否有被困顾客； ➢ 关闭所有设备电源及煤气阀门，撤离危险或高温区； ➢ 低温食品、贵重商品采取保护性措施； ➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 通过备用电源及时保存电子文档； ➢ 了解停电、停水原因及时间；

序号	突发事件/风险场景分类	突发事件/场景描述	造成影响	影响范围	应急处置要点
					➢ 如发生长时间停电，需有序疏导顾客离店。
6	事故灾难类	漏水	运营中断/财产损失	单一门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 上报物业查找漏水原因及漏水点； ➢ 关闭漏水点下方电源； ➢ 遮挡或移动漏水点下方物品。
7	事故灾难类	建筑物、设施倒塌	运营中断/财产损失/人身伤害	单一门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 安抚致歉，并及时疏散顾客； ➢ 疏散员工； ➢ 安排事故区域警示警戒； ➢ 相关损失及时向保险公司报备。
8	公共卫生事件类	流行疾病或传染病	人员安全/运营中断/品牌形象受损	全/单一/区域门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 发现疫病发生者，由做好防护的专人安排到专门区域，隔离开人群； ➢ 通知医疗机构到场急救； ➢ 追踪并关注密切接触人员； ➢ 清洁并消杀工作区域； ➢ 如有必要，及时上报卫健委及当地疾控中心持续监控预警； ➢ 提前发布内部预警信息，采取个人防护措施。

序号	突发事件/风险场景分类	突发事件/场景描述	造成影响	影响范围	应急处置要点
9	公共卫生事件类	顾客或门店员工受伤/死亡	人身伤害/运营中断/顾客高额索赔	单一门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 接到报告立刻到达现场并组织紧急救治； ➢ 根据伤势及时就医，并跟进陪同； ➢ 做好现场记录拍摄取证报警备案； ➢ 组织专人跟进联系伤者并处理后续事宜； ➢ 相关公众责任险保险公司报备，并划分责任和费用，形成书面文件； ➢ 分析原因避免事故再次发生； ➢ 相关损失及时向保险公司报备。
10	公共卫生事件类	门店发生食品安全事件	品牌形象受损/政府处罚/营业额下降	全国门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 严格执行食品安全相关规定流程，排查隐患； ➢ 配合政府部门调查； ➢ 与政府部门和媒体积极沟通。
11	社会安全事件类	针对顾客或门店商品财物的盗窃	财产损失/顾客投诉	单一门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 出现偷盗行为，立即启动防盗应急系统； ➢ 监控系统及时发现并记录偷盗行为； ➢ 安全部门检查店内容易藏匿赃物地点； ➢ 顾客财务或大量商品丢失需马上报警。

序号	突发事件/风险场景分类	突发事件/场景描述	造成影响	影响范围	应急处置要点
12	社会安全事件类	抢劫	运营中断/财产损失/人身伤害	单一门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 尽量服从抢劫者要求，避免刺激抢劫者情绪； ➢ 拨打报警电话并通知值班经理； ➢ 避免员工跟随抢劫者走出门店； ➢ 疏散相关区域顾客； ➢ 如有人受伤，必须组织必要的施救； ➢ 事后保护作案现场，配合警方调查； ➢ 涉及损失报送保险公司。
13	社会安全事件类	顾客间或顾客和员工间冲突	运营中断/人身伤害/政府处罚/品牌形象受损	单一门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 通知负责人员控制现场； ➢ 尽力安抚涉事者恢复平静； ➢ 分开冲突双方，以免再次发生冲突； ➢ 根据事件情况，适当选择报警，留住当事人，并配合警方调查； ➢ 如有人受伤，应立即救治，或视严重程度送医施救； ➢ 相关损失及时向保险公司报备。
14	社会安全事件类	非法示威抗议	运营中断/财产损失/人身伤害	单一/区域门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 关注针对品牌的舆情； ➢ 及时处理门店纠纷； ➢ 寻求警方支持； ➢ 相关损失及时向保险公司报备。

序号	突发事件/风险场景分类	突发事件/场景描述	造成影响	影响范围	应急处置要点
15	社会安全事件类	不明嫌疑人通过信件/电话威胁/伤害员工或顾客	运营中断/人身伤害/政府处罚/品牌形象受损	全/单一/区域门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 立即保存信件或电话号码等关键证据； ➢ 提醒目击者保持冷静，并了解情况； ➢ 注意信息的保密性； ➢ 及时报警，配合警方调查，并向上级汇报； ➢ 视情形启动门店紧急疏散预案； ➢ 关店涉及营业额损失需上报保险公司。
16	内部运营类	信息系统技术故障、配套设施故障	运营中断/财产损失/顾客投诉/品牌形象受损	全/单一/区域门店	➢ 启动相关预案，若预案缺失需要制定临时处置措施； ➢ 保存重要信息系统数据后及时开展应急处置； ➢ 恢复过程需要与业务运营部门沟通并及时验证数据可用； ➢ 系统从灾备切回生产后，需进行数据同步和验证。

表 A.1

参 考 文 献

[1] 《中华人民共和国突发事件应对法》.

[2] 《国家突发公共事件总体应急预案》.

[3] 应急办函[2009]62 号《突发事件应急演练指南》.

[4] 应急〔2019〕68 号《应急管理标准化工作管理办法》.

[5] GB/T 31595-2015 公共安全-业务连续性管理体系-指南.

[6] GB/T28827.3-2012 信息技术服务 运行维护 第 3 部分：应急响应规范.

[7] GB/T 38645-2020 信息安全技术 网络安全事件应急演练指南.

[8] GB/T 20988-2007 信息安全技术-信息系统灾难恢复规范