ICS 35.080
CCS L 77

中华人民共和国国家标准

GB/T 43046—2023

信息技术服务　应对突发公共安全事件的信息技术应急风险管理

Information technology service—Information technology emergency risk management in public security emergency response

2023-09-07 发布　　2024-04-01 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

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：上海谷航信息科技发展有限公司、中国电子技术标准化研究院、上海计算机软件技术开发中心、北京国家会计学院、上海市卫生健康委员会、上海市网络与信息安全应急管理事务中心、北京太极华保科技股份有限公司、北京同创永益科技发展有限公司、北京赛迪认证中心有限公司、万达信息股份有限公司、神州数码融信云技术服务有限公司、国家工业信息安全发展研究中心、苏州市软件评测中心有限公司、上海交通大学、中科软科技股份有限公司、中福彩科技发展(北京)有限公司、浙江经济职业技术学院、天津天大康博科技有限公司、金税信息技术服务股份有限公司、上海软件产业促进中心、山东正中信息技术股份有限公司、成都市工业互联网发展中心、陕西省信息化工程研究院、中远海运科技股份有限公司、建信金融科技有限责任公司、国网区块链科技(北京)有限公司、太极计算机股份有限公司、上海安言信息技术有限公司、北京德信永道信息技术服务有限公司、嘉兴嘉赛信息技术有限公司、上海软中信息系统咨询有限公司、上海新炬网络信息技术股份有限公司、广州物联网研究院、威海神舟信息技术研究院有限公司、南京云信达科技有限公司、上海云济信息科技有限公司、上海霞安信息科技有限公司、工业互联网创新中心(上海)有限公司、北京赛博昆仑科技有限公司、上海翰纬信息科技有限公司、武汉速云星博信息技术有限公司、帝杰曼科技股份有限公司、湖南创博龙智信息科技股份有限公司、杭州数列网络科技有限责任公司、北京中百信信息技术股份有限公司、黑龙江科技大学、健康云(上海)数字科技有限公司、上海市新能源汽车公共数据采集与监测研究中心、武汉网信安全技术股份有限公司、上海申康医院发展中心、深圳市通商宝科技有限公司、浙江海瑞网络科技有限公司、深圳融昕医疗科技有限公司、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、北京明易达科技股份有限公司、河北微保物流科技有限公司、建标教育科技河北有限公司、河北沃瑞斯供应链管理有限公司、河北标质质检技术服务中心、广东润联信息技术有限公司、武汉东湖大数据交易中心股份有限公司、河北鸿宇通信器材有限公司、河北鹏博通信设备有限公司。

本文件主要起草人：俞文平、张凤玲、郭鑫伟、宋俊典、冯骏、吴恩平、赵勇祥、郑阳、邵庆祥、徐雨清、薛质、方健、郑晨光、肖筱华、栗卓越、马烈、韩飞、张蕾、徐刚、张玮、薛冰玢、聂兴凯、杨烨、王珊珊、谢美程、张建成、王文俊、熊健淞、莊敏、张勇、俞志东、张在丰、石竹玉、赵建华、黄建文、陈申捷、施勇、方轶博、赵丹丹、高敏、郭磊、钱伟峰、杨泉、张晓娟、张明英、梁铭图、陈鲁鑫、郭辉、李帆、赵小敏、王慧芬、潘钢、朱柯、孙诚、王守选、杨德华、卢学哲、赵秋多、潘铮、王成名、俞丽平、吕千千、陈昌杰、门美龄、孙明雷、王萌、李光亚、安特、侯鹏飞、刘敏、丁海元、安淑荻、金开立、鹿全礼、付华茂、赵晓荣、陈振东、何煜翔、李庆、董刚华、付宇、阙志兴、程永新、胡良霖、毛慧丽、黄海峰、柴磊、米登科、徐萍、左有良、赵丹凤、金燕芳、唐泽诚、高金、王承琨、曹川韡、钟鸣荟、朱武振、黄泽锋、陈晗、祝荣荣、赵亮、王猛、蔡未锋、白瑞英、孟繁哲、曹嘉恒、王慧颖、姚敏森、杜乐、闫航飞、高占良、李凯。

引　言

为有效控制突发公共安全事件情况下组织面临的IT应急风险，提高相应的IT应急风险管理能力，促进IT对组织业务的安全、可靠、有效支持，提出应对突发公共安全事件下的IT应急风险管理规范，实现责任落实、风险可控和价值实现的目标。

实施主体可根据应对突发公共安全事件的IT应急风险管理规范要求，明确组织应对突发公共安全事件的IT应急风险管理顶层设计、管理体系等，结合实施环境，规范相应的IT应急风险管理实施过程，明确统筹和规划、构建和运行、监督和评估、改进和优化的目标和基本任务。

信息技术服务　应对突发公共安全事件的信息技术应急风险管理

1　范围

本文件确立了突发公共安全事件情况下IT应急风险管理的总则、框架，并规定了相关的顶层设计、环境、体系、要素及实施等要求。

本文件适用于：

a）　决策层或最高管理者实施相关的IT应急风险管理顶层设计职能；

b）　建立或完善组织相关的IT应急风险管理体系；

c）　明确组织相关IT应急风险管理流程的要求；

d）　规范组织相关IT应急风险管理的实施；

e）　第三方或其他机构开展相关IT应急风险管理咨询业务。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

组织　organization

为实现目标，由职责、权限和相互关系构成自身功能的一个人或一组人。

注：组织的概念包括，但不限于代理商、公司、集团、商行、企事业单位、行政机构、合营公司、协会、慈善机构或研究机构，或上述组织的部分或组合，无论是否为法人组织，公有的或私有的。

[来源：GB/T 19000—2016，3.2.1]

3.2

决策层　decision-making level

负责确定组织(3.1)的目标、纲领和实施方案，进行宏观控制的最高权力机构。

3.3

最高管理者　top management

在最高层指挥和控制组织(3.1)的一个人或一组人。

注：最高管理者在组织内有授权和提供资源的权力。

[来源：GB/T 19000—2016，3.1.1]

3.4

突发公共安全事件　public security emergency

突然发生，造成或者可能造成重大人员伤亡、财产损失、生态环境破坏和严重社会危害，危及公共安全的紧急事件。

注：根据突发公共安全事件的发生过程、性质和机理，主要分为以下四类：自然灾害、事故灾难、公共卫生事件和社会安全事件。

3.5

IT 应急管理　information technology emergency management

组织为应对突发公共安全事件开展的信息技术领域的应急管理。

3.6

IT 应急风险管理　information technology emergency risk management

在突发公共安全事件情况下，组织为控制信息技术应急管理中的风险而进行的一系列管控活动。

注：简称“风险管理”。

4　缩略语

下列缩略语适用于本文件。

BCMS：业务连续性管理体系（Business Continuity Management System）

IT：信息技术（Information Technology）

RPO：恢复点目标（Recovery Point Objective）

RTO：恢复时间目标（Recovery Time Objective）

SWOT 分析法：企业竞争态势[优势（Strength）、劣势（Weakness）、机会（Opportunity）、威胁（Threat）]分析方法

5　总则

5.1　IT 应急风险管理与 IT 应急管理的关系

与一般的 IT 应急管理不同，突发公共安全事件情况下的 IT 应急管理，旨在为应对突发公共安全事件开展的 IT 领域的应急管理。管理主体的 IT 相关应急管理职责不仅仅局限于组织内部，还涉及组织与外部的联防、联动等。

突发公共安全事件情况下的 IT 应急风险管理旨在相关 IT 应急管理基础上，进一步强调与应对突发公共安全事件相关 IT 应急控制措施的合理性和有效性。管理主体的 IT 应急风险管理职责不仅仅局限于组织内部，也涉及组织与外部的联防、联动等。

应对突发公共安全事件情况下的 IT 应急风险管理，有利于各级各类组织树立 IT 应急风险管理意识，完善 IT 应急管理机制，提高应对突发公共安全事件的 IT 应急处理能力，并达到如下效果：

a）遇到突发公共安全事件时，在政府的统筹领导下，加强与外部的联防、联动，沉着应对各种 IT 应急风险，提升组织 IT 应急相关资源的统筹与调配能力，避免无序和失控情况的发生；

b）在日常的 IT 管理中，将 IT 应急风险管理意识贯穿于价值、制度、机制和能力等方面，建立和完善应对突发公共安全事件的 IT 应急风险管理体系，提高组织的预期管理能力，并增强社会责任意识；

c）突发公共安全事件情况下的 IT 应急风险管理属于组织风险管理体系一部分，通过加强对相关 IT 应急管理合理性、有效性的监督和评价，促进 IT 应急管理能力的持续提升，确保组织业务的持续运营。

5.2　风险管理原则

IT 应急风险管理原则包括如下内容。

a) 整体性原则。在突发公共安全事件情况下，作为整体的有机组成部分，组织充分配合国家、地方、行业或领域等开展IT应急风险管理，履行社会责任，并建立与外部的联防、联动机制。

b) 全面性原则。IT应急风险管理覆盖IT应急应用领域的各个方面，贯穿决策、执行和监督全部管理环节。

c) 标准化原则。通过实施标准化的IT应急风险管理，提供更稳定、更可靠的IT应急风险管控服务。

d) 前瞻性原则。组织建立IT应急风险管理机制，确保IT应急风险管理目标与组织战略发展目标一致性，并具有超前意识，预判潜在的IT应急风险，提前进行干预和制定对策。

e) 预防性原则。坚持预防为主，建立预防、预警与演练机制，将日常管理与应急处置有效结合。

f) 可执行性原则。组织开展的IT应急风险管理切实符合当前能力，确保IT应急风险管理的可执行性。

g) 适应性原则。IT应急风险管理机制与IT应急风险状况、信息化或数字化程度等相适应，并根据应急环境变化、内外部要求进行调整。

h) 人性化原则。坚持以人为本，重点保障人员安全与健康，并需考虑无障碍服务。

5.3 风险管理文化

组织建立应对突发公共安全事件的IT应急风险管理文化，包括但不限于：

a) 加强与国家、地方、行业或领域等的协同与沟通，提升社会责任意识；

b) 与组织文化建设相结合，使其成为组织日常运营管理的有机组成部分；

c) 提升全员的IT应急风险管理意识，遵守公共安全秩序；

d) 形成与组织相适应的价值准则、职业操守；

e) 建立IT应急风险管理文化培训与传达机制；

f) 建立IT应急风险管理文化的评价、考核、监督及奖惩机制。

5.4 风险管理策略

组织将应对突发公共安全事件的IT应急风险管理纳入IT总体风险管理体系，并根据内外部环境等情况，围绕组织IT发展战略，明确相关的IT应急风险管理策略，包括如下内容。

a) 总体策略。应对突发公共安全事件的IT应急风险管理是组织IT总体风险管理体系有机组成部分，并与国家、地方、行业或领域等的IT应急风险管理体系相协调。

b) 具体策略。内容包括但不限于：

- 组织对IT应急风险进行分类分级管理，为各类突发公共安全事件制定相应的IT应急风险管理策略；
- 根据突发公共安全事件的IT应急风险特点，采用风险规避、风险转移、风险减轻以及风险接受等措施；
- 采用应对措施时，需要考虑的事项包括关注成本、承担的责任（含社会责任等）和义务、自愿承诺和利益相关方的观点；根据组织的目标、风险准则和可用资源进行分析；结合价值观、认知和潜在涉及的利益相关方，以及与他们沟通和咨询的最佳方式进行分析；效果相同的方案，因利益相关方偏好不同而采用结果不同。

5.5 风险管理技术

IT应急风险管理技术包括但不限于下述内容。

a) 风险识别技术。识别可能影响一个或多个目标的不确定性，包括德尔菲法、头脑风暴法、检查表法、SWOT 分析法及图解技术等。
b) 风险分析技术。对风险影响和后果进行评价和估量，包括定性分析和定量分析。
c) 风险评价技术。在风险分析的基础上，通过相应的指标体系和评价标准，对风险程度进行划分，以揭示影响成败的关键风险因素，包括单因素风险评价和总体风险评价。
d) 风险应对技术。IT 技术体系中为特定风险制定的应对技术方案，包括云计算、冗余链路、冗余资源、系统弹性伸缩、两地三中心灾备、业务熔断限流、数据备份和副本数据管理等。
e) 风险监测技术。监测应急风险演化为事件的特定触发条件、发展过程，包括 IT 基础设备监控、日志分析、物联网技术、实时数据分析、舆情分析等。
f) 风险预警技术。对应急风险的产生与发展进行提前预测和预警方面的技术，包括人工智能、大数据分析、趋势预测、容量管理、渗透性测试、入侵检测系统等。

5.6 风险管理对象

突发公共安全事件情况下的 IT 应急风险为 IT 应急风险管理对象。IT 应急风险类型包括 IT 应急管理总体风险与 IT 应急管理专项风险(见 10.2、附录 A、附录 B)。

6 风险管理框架

IT 应急风险管理框架是组织 IT 总体风险管理框架的有机组成部分，是组织应对突发公共安全事件的 IT 应急风险管理框架，主要包括顶层设计、风险管理环境、风险管理体系、风险管理要素和风险管理实施五部分，见图 1。

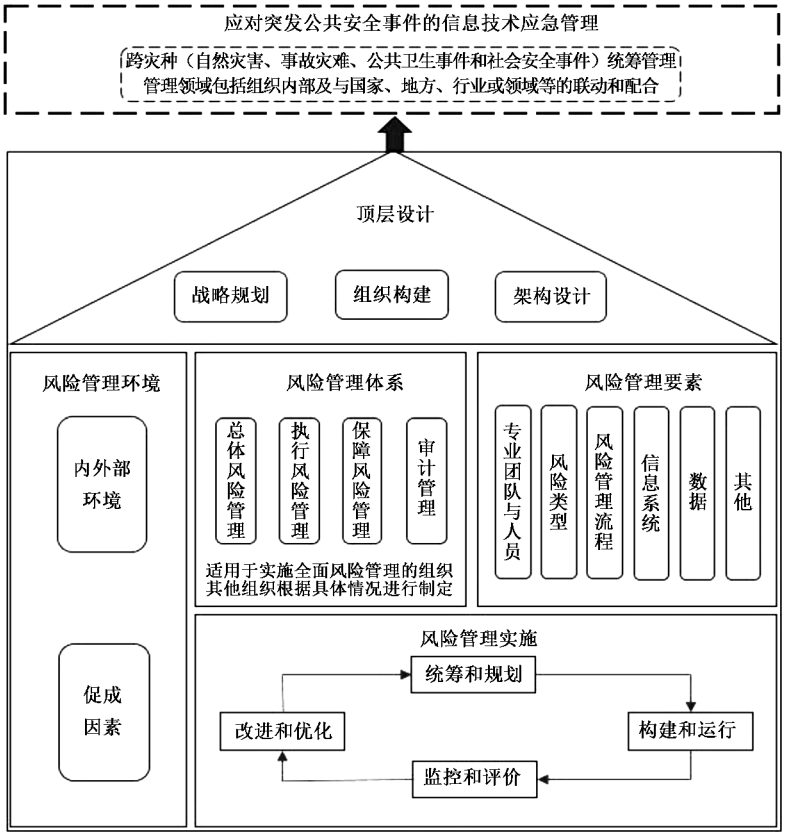

图 1　风险管理框架

在 IT 应急管理过程中引入 IT 应急风险管理机制（见第 7 章～第 11 章）。当突发公共安全事件时，可有效管控 IT 应急管理的相关风险（见附录 A、附录 B），提升组织内部以及与国家、地方、行业或领域等的联防、联动 IT 应急管理能力，避免无序和失控情况的发生，确保相关 IT 应急管理工作的成效。

顶层设计包含应对突发公共安全事件的 IT 应急风险管理战略规划、组织构建和架构设计，决策层或最高管理者通过评估、指导和监督对相关的 IT 应急风险管理层进行管控。

管理环境包含内外部环境和促成因素，其中促成因素是应对突发公共安全事件的 IT 应急风险管理实施的保障。

管理体系包含应对突发公共安全事件的总体风险管理、执行风险管理、保障风险管理及审计管理。

管理要素包含应对突发公共安全事件的专业团队与人员、风险类型、风险管理流程、信息系统、数据等。管理体系与管理要素是相关 IT 应急风险管理实施的核心。

风险管理实施包含应对突发公共安全事件的统筹和规划、构建和运行、监控和评价、改进和优化，是相关 IT 应急风险管理的实际应用并促进相关 IT 应急管理提升的过程。

7　顶层设计

7.1　战略规划

组织应结合突发公共安全事件情况下的风险特点，根据内外部环境及促成因素制定独立的 IT 应急风险管理战略规划，明确 IT 应急风险管理战略规划实施的策略。IT 应急风险管理规划属于组织战略规划的一部分，应与组织战略规划中的业务应急管理规划、业务风险管理规划保持一致，包括但不

限于：

a） 分析突发公共安全事件情况下的风险特点、相关内外部环境及促成因素，理解业务应急规划、业务风险管理规划和IT应急规划等，调研需求并评估突发公共安全事件情况下的IT应急风险管理现状、技术现状、应用现状和环境；

b） 制定应对突发公共安全事件的IT应急风险管理战略规划，指导IT应急风险管理体系的建立，并明确IT应急风险管理要素；

c） 明确应对突发公共安全事件的内控、合规、绩效和审计等要求，对相关IT应急风险进行管控；

d） 监控和评价应对突发公共安全事件的IT应急管理规划制定与实施，确保IT应急管理规划的持续改进和优化。

7.2 组织构建

组织构建应聚焦突发公共安全事件情况下的IT应急风险管理责任主体与分工，通过完善组织机制及与外部的联防、联动机制，获得相关方的理解和支持，制定相应的IT应急风险管理制度和流程，以支撑突发公共安全事件情况下IT应急风险管理的实施，包括但不限于：

a） 建立与外部的联防、联动机制，配合国家、地方、行业或领域等在突发公共安全事件情况下IT应急风险管理的开展；

b） 建立突发公共安全事件情况下支撑IT应急风险管理战略的组织机制，明确相关的实施原则和策略；

c） 明确突发公共安全事件情况下的IT应急风险管理决策、实施及监督机构，建立相应的IT应急风险管理组织架构（见附录C），明确管理者和成员角色，确保责权利一致；

d） 建立突发公共安全事件情况下的IT应急风险管理决策、授权和沟通机制，保证利益相关方理解、接受相应的职责和权利；

e） 实现突发公共安全事件情况下的IT应急风险管理决策、执行、控制和监督等职能，评估运行成效并持续改进和优化。

7.3 架构设计

在设计组织层面的IT应急风险管理架构时，应关注突发公共安全事件下的业务架构、应用架构、数据架构、技术架构和架构管理体系等风险，通过持续的评估、改进，不断完善IT应急管理架构，包括但不限于：

a） 建立与突发公共安全事件情况下IT应急风险管理战略、业务战略及组织战略一致的IT应急风险管理架构，针对突发公共安全事件情况下IT应急管理架构的风险（如技术方向、管理策略和支撑体系等风险）提出管控要求；

b） IT应急风险管理架构宜考虑与外部IT应急风险管理架构的联动与控制、技术能力及资源等；

c） 监控和评价组织级突发公共安全事件情况下IT应急管理架构的设计风险，以及组织级相应IT应急管理架构实施、应用的成效，确保IT应急管理架构的持续改进和优化；

d） 监控和评价组织级突发公共安全事件情况下的IT应急管理架构机制运行风险，确保相关管理工作的持续改进和优化。

8 风险管理环境

8.1 内外部环境

组织应分析内外部环境要求，明确突发公共安全事件情况下IT应急风险管理实施的策略。内外

部环境要求包括但不限于：

a） 国家、地区、行业及领域等应急管理规范；

b） 内外部审计、监督及评估等；

c） 组织战略和业务战略的变化；

d） 疫情、地缘冲突、战争及灾难等变化；

e） 新技术变革和IT应用创新发展趋势。

8.2 促成因素

组织应识别突发公共安全事件情况下IT应急风险管理的促成因素，保障风险管理的实施，包括但不限于：

a） 与外部的联防、联动机制；

b） 决策层或最高管理者的授权和支持；

c） IT应急风险管理文化；

d） IT应急风险的分类分级管理；

e） IT应急所需的各类资源保障。

9 风险管理体系

实施全面风险管理的组织应建立突发公共安全事件情况下的IT应急风险管理体系，并将IT应急风险管理纳入全面风险管理体系。IT应急风险管理体系（见附录C）包括但不限于以下内容。

a） 总体风险管理。明确应对突发公共安全事件的IT应急总体风险管理主管部门（如风险管理部门或其他综合管理部门）、职责、权限、人员配备、安全与健康、持续监控并开展风险评估等。

b） 执行风险管理。明确应对突发公共安全事件的IT应急执行风险管理主体（包括业务部门和IT部门）、职责、人员配备、安全与健康、政策和程序的执行、自评估及持续改进等。

c） 保障风险管理。明确应对突发公共安全事件的IT应急保障风险管理主体（如办公室、人力资源部门、财务部门、法律合规部门、公共关系部门、后勤部门等）、职责、权限、人员配备、安全与健康、政策和程序的执行、自评估及持续改进等。

d） 审计管理。明确应对突发公共安全事件的IT应急风险管理审计主体（如内部审计部门）、职责、权限、人员配备、安全与健康、制度和流程的制定及审计活动的开展等。

注：其他未实施全面风险管理的组织依据上述要求并考虑所处行业和自身实际，建立本组织应对突发公共安全事件的IT应急风险管理体系（见附录D）或将IT应急风险管理理念融入具体的IT应急管理领域（见附录E）。

10 风险管理要素

10.1 专业团队与人员

突发公共安全事件情况下，组织的IT应急风险管理专业团队与人员应满足下列要求：

a） IT应急风险管理专业团队，包括但不限于团队内部协同能力、与外部的协同能力、综合救援风险管控能力、人力资源储备与部署能力等；

b） IT应急风险管理专业人员，包括但不限于社会责任、职业道德、知识、技能、资质和经验、专业胜任能力、人员安全与健康等。

注：人力资源储备与部署能力，包括明确领导与决策人员、应急团队、备份人员；特殊情况下的人员备份考虑（如疫

情可能对同一场所或区域人员的不利影响等)；建立关键岗位的应急储备，两套班子互为备份，部署在不同区域(如常规场所、应急备用场所)。

10.2 风险类型

突发公共安全事件情况下的IT应急风险类型包括IT应急管理总体风险与IT应急管理专项风险。IT应急管理总体风险是突发公共安全事件情况下，影响组织IT应急管理总体目标实现的综合性风险(见附录A)；IT应急管理专项风险是突发公共安全事件情况下，组织未满足外部要求及内部特殊需要面临的风险。对IT应急管理专项风险的管控可作为独立项目实施，或作为IT应急管理总体风险管控项目的组成部分实施(见附录B)：

a) IT应急管理总体风险包括IT应急战略风险、IT应急组织风险、IT应急架构风险、IT应急运行体系风险、业务影响分析和风险评估实施风险、应急信息系统风险及IT应急全过程控制风险等；

b) IT应急管理专项风险包括人员类风险、资源类风险、技术应用类风险、过程类风险及管理类风险等。

10.3 风险管理流程

IT应急风险管理流程是组织针对突发公共安全事件，开展IT应急风险管理活动所采取的系列行动和步骤，包括如下内容。

a) 准备工作。协助利益相关方理解IT应急风险，明确作出决策的依据，需采取特定行动的原因及需要承担的社会责任等，针对性地设置突发公共安全事件情况下IT应急风险管理流程，实现有效的IT应急风险评估和恰当的风险应对。

b) 风险评估。针对突发公共安全事件开展IT应急风险评估，及时发现IT应急管理中存在的风险隐患和管理漏洞，持续提高IT应急管理的有效性。风险评估包括：

- 风险识别，发现、识别和描述可能有助于或妨碍组织实现突发公共安全事件情况下IT应急目标的风险；
- 风险分析，理解包括突发公共安全事件情况下IT应急风险水平在内的风险性质和特征；
- 风险评价，将突发公共安全事件情况下IT应急风险分析的结果与既定的风险准则进行比较，以确定需要采取何种应对措施。

c) 风险应对。选择和实施应对突发公共安全事件情况下IT应急风险的方式。

d) 监督和检查。保证和提升突发公共安全事件情况下的流程设计、实施与结果的质量和有效性。

e) 记录和报告。需在组织内传达应对突发公共安全事件的IT应急风险管理活动和成果，为决策提供信息、改进相关的IT应急风险管理活动，以及协助与利益相关方的互动等。

10.4 信息系统

突发公共安全事件情况下的应急风险管理信息系统用于支持决策层或最高管理者、应急风险管理相关部门(或机构)及咨询机构人员完成相关工作，该信息系统需与内外部应急管理系统实现联动，包括但不限于：

a) 建立应对突发公共安全事件的应急风险管理信息系统，并实现与应急管理系统(如远程办公系统、远程运营系统、应急全过程控制系统等)的联动与控制；

b) 与外部应急管理系统资源进行整合、实现信息共享；

c) 建立应对突发公共安全事件的应急风险管理信息系统管理制度和流程；

d) 明确应对突发公共安全事件的网络与信息安全管理要求；

e) 明确应对突发公共安全事件的IT远程研发支撑要求；
f) 建立应对突发公共安全事件的应急风险管理信息系统的应急预案，并对演练组织管理和实施过程进行控制及监督；
g) 对应对突发公共安全事件的应急风险管理信息系统生存周期进行管控，包括信息系统的建设、运维、使用及下线等。

10.5 数据

组织应对突发公共安全事件情况下IT应急风险管理过程中使用和形成的数据进行管理，包括但不限于：

a) 明确相关的IT应急风险数据管理范围，包括内部数据及与外部共享的数据等；
b) 明确相关的IT应急风险数据管理目标和策略；
c) 明确相关的IT应急风险数据组织管理，包括组织架构、责任人、角色、职责和权限等；
d) 制定相关的IT应急风险数据管理制度和流程，包括一般应急数据和共享数据的管理；
e) 建立相关的IT应急风险数据安全管理机制；
f) 建立相关的个人信息保护管理机制；
g) 开展相关的IT应急风险数据生存周期管控，包括数据的收集、存储、使用、加工、传输、提供、公开等。

10.6 其他

对于本文件未明确的其他要素（如无形资产、实物资产等），组织在提出应对突发公共安全事件的IT应急风险管理要求时，宜依据相应的标准规范进行确定。

11 风险管理实施

11.1 统筹和规划

组织进行应对突发公共安全事件的IT应急风险管理实施时，宜充分考虑此情况下IT应急管理的状况，在决策层或最高管理者的领导下，充分发挥IT应急风险管理的作用，包括但不限于：

a) 充分配合国家、地方、行业或领域等突发公共安全事件下的IT应急风险管理工作，履行社会责任，并实施与外部的联防、联动；
b) 明确组织应对突发公共安全事件的IT应急风险管理目标和任务，营造必要的IT应急风险管理环境，做好IT应急风险管理与IT应急管理有效对接的准备；
c) 评估应对突发公共安全事件的IT应急风险管理资源、环境和人员能力等现状，分析现状与法律法规、行业监管、业务发展以及利益相关方等要求的差距，为相应IT应急风险管理方案的制定提供依据；
d) 指导应对突发公共安全事件的IT应急风险管理方案制定，包括组织机构和责权利的规划、管理范围和任务的明确以及实施策略和流程的设计；制定IT应急风险管理方案时，宜充分考虑应对突发公共安全事件下IT应急管理的实际情况及与外部的协同；
e) 监督应对突发公共安全事件的IT应急风险管理统筹和规划过程，保证现状评估的客观性、组织机构设计的合理性及IT应急风险管理方案的可行性等。

11.2 构建和运行

结合应对突发公共安全事件的IT应急管理实施，构建相应的IT应急风险管理实施机制和路

径，确保 IT 应急风险管理实施的有序运行和成效，包括但不限于：

a） 评估应对突发公共安全事件的 IT 应急风险管理方案与现有资源、环境和能力的匹配程度，为应对突发公共安全事件情况下 IT 应急风险管理与 IT 应急管理的有效对接提供指导；

b） 制定应对突发公共安全事件的 IT 应急风险管理实施方案，包括组织机构和团队的构建、职责与分工的明确、内外部实施路线图的制定、实施方法的选择以及管理制度的建立和执行等；

c） 监督应对突发公共安全事件的 IT 应急风险管理构建和运行过程，确保相应 IT 应急风险管理实施过程与方案的符合、管理资源的可用和管理活动的可持续等。

11.3 监控和评价

监控应对突发公共安全事件的 IT 应急风险管理实施过程以及与 IT 应急管理的对接情况，评价相关工作的合规与成效，保障 IT 应急风险管理目标的实现，包括但不限于：

a） 构建必要的应对突发公共安全事件 IT 应急评估体系、内控体系或审计体系，制定相应的评价机制、制度和流程；

b） 评估应对突发公共安全事件的 IT 应急风险管理相关工作成效与目标符合性，为应对突发公共安全事件的 IT 应急风险管理方案改进和优化提供参考，必要时可聘请外部机构进行评估；

c） 定期监控和评价突发公共安全事件情况下 IT 应急风险管理相关工作实施的有效性、合规性，确保相关工作符合法律法规和行业监督要求。

11.4 改进和优化

持续改进应对突发公共安全事件的 IT 应急风险管理实施过程以及与 IT 应急管理的对接工作，包括但不限于：

a） 持续评估应对突发公共安全事件的 IT 应急风险管理相关资源、环境、能力、实施和绩效等，以支撑应对突发公共安全事件的 IT 应急风险管理体系建设；

b） 指导应对突发公共安全事件的 IT 应急风险管理方案改进，优化相应 IT 应急风险管理的实施策略、方法、制度和流程，促进相应 IT 应急风险管理体系、资源和基础工作的完善；

c） 监督应对突发公共安全事件的 IT 应急风险管理相关工作改进和优化过程，为 IT 应急风险管控和 IT 应急管理价值的实现提供保障。

附 录 A
（资料性）
IT 应急管理总体风险

A.1 IT 应急战略风险

组织应开展突发公共安全事件情况下 IT 应急战略风险的管控，风险类型包括但不限于：

a） 与外部（国家、地方、行业或领域等）协同的相关 IT 应急战略风险；
b） 决策层或最高管理者对相关 IT 应急战略评估、指导和监督的风险；
c） 相关 IT 应急战略目标管理风险，包括未能根据组织业务发展的总体目标、经营规模以及风险控制的基本策略和风险偏好，确定适当的 IT 应急战略；未确定重要业务及其恢复目标等；
d） 相关 IT 应急战略预算管理的风险；
e） 相关 IT 应急战略管理体系建设和运行风险；
f） 相关 IT 应急战略规划制定、实施、监控和改进风险；
g） 相关 IT 应急战略与业务战略一致性风险；
h） 相关 IT 应急战略技术选择风险，与业务需求匹配的风险；
i） 相关 IT 资源保障的风险。

A.2 IT 应急组织风险

组织应开展突发公共安全事件情况下 IT 应急组织风险的管控，风险类型包括但不限于：

a） 组织环境分析风险，包括未对内外部环境进行全面分析、未充分识别相关方与法律法规要求、未明确管理体系的范围等；
b） 内外部联动机制风险，包括未能有效配合国家、地方、行业或领域等的 IT 应急管理工作、未能有效统筹组织内的 IT 应急管理工作等；
c） 应急领导力风险，包括组织的各级管理者未能证明其在实现相关 IT 应急管理方针和目标方面的承诺和领导力、决策层或最高管理者未能证明其在相关 IT 应急管理体系方面的承诺、决策层或最高管理者对相关 IT 应急管理方针的管理不规范及相关 IT 应急管理组织的角色、职责和权力方面存在问题等；
d） 组织分工和工作流程的风险；
e） IT 应急团队人员安全与健康风险，包括各级各类人员因隔离、死亡、异动，无法参与 IT 应急管理等；
f） 相关合作伙伴、供应商、外包商等响应能力及人员安全与健康的风险。

A.3 IT 应急架构风险

组织应开展突发公共安全事件情况下 IT 应急架构风险的管控，风险类型包括但不限于：

a） IT 应急架构与外部应对突发公共安全事件的 IT 应急管理架构协同联动的风险；
b） 决策层或高级管理层对相关 IT 应急架构评估、指导和监督的风险；
c） IT 应急架构与相关 IT 应急管理战略一致性的风险；
d） IT 应急架构规划、设计、实施、服务等过程控制的风险；
e） IT 应急架构评估与持续改进的风险。

A.4 IT 应急运行体系风险

组织应开展突发公共安全事件情况下 IT 应急运行体系风险的管控，风险类型包括但不限于：

a) IT 应急运行环境风险，包括未对内外部运行环境进行分析或分析不充分等；
b) IT 应急运行规划风险，包括 IT 应急管理运行规划未制定或无法实施等；
c) IT 应急机构与队伍建设体系风险，包括 IT 应急机构设置不合理、IT 应急管理队伍专业能力有限及经验不足等；
d) IT 应急制度体系风险，包括 IT 应急管理制度制定不合理或未执行等；
e) IT 应急合规管理风险，包括违反应对突发公共安全事件的相关方针与政策、未遵守网络安全法、数据安全法、个人信息保护法及未满足网络安全等级保护等要求；
f) 业务连续性管理风险，包括未完善业务连续性管理机制、灾备中心管理不规范及未建立应用级或者数据级灾备机制等；
g) IT 应急预案管理风险，包括未对应急预案进行分类管理（如总体应急预案、专项应急预案）、应急策略不合理、未实施差异化管理、预警和信息报告渠道不通畅、应急预案缺乏针对性和可操作性、未根据业务风险评估及组织架构适应性调整应急预案等；
h) IT 应急演练与验证管理风险，包括未进行 IT 应急演练、演练范围有限、未对演练过程进行记录或记录不充分及未根据演练结果更新完善 IT 应急预案等；
i) IT 应急宣传教育管理风险，包括应急宣传教育目标未明确、应急宣传教育制度与流程管理不规范及应急宣传教育未满足要求等；
j) 新技术应用管理风险，包括云计算技术、大数据技术、物联网技术、信息通信技术、健康码技术、远程诊疗技术及无人技术（含无人系统、无人机系统方面的智能化技术、人工智能）等在应用管理方面存在的各种风险；
k) IT 应急综合保障管理风险，包括 IT 应急保障规划未建立或不完善、IT 应急保障制度不健全、IT 应急资源（如人、财、物、技术、信息及通信等）不足或覆盖度有限等；
l) 网络舆情管理风险，包括未建立合理的网络舆情风险管理机制、未通过培训提高网络舆情风险意识、公关部门未及时与外部（如国家相关主管部门、行业监管机构等）进行沟通、汇报等；
m) 放弃执行 IT 应急运行管理的风险，包括公共安全事件风险级别已超出 IT 应急运行体系能够承受的范围，导致决策层或最高管理者放弃执行 IT 应急运行体系后的风险等；
n) 外部供应商 IT 应急管理的风险，包括 IT 应急预案的制定、演练的组织管理和实施过程的控制及监督等风险；
o) 因客户或用户因素导致的风险，包括系统使用不当、未就系统服务重建需要的业务条件与客户达成一致并得到有效配合等。

A.5 业务影响分析和风险评估实施风险

组织应开展突发公共安全事件情况下业务影响分析和风险评估实施风险的管控，风险类型包括但不限于：

a) 内外部环境变化带来的业务影响的风险；
b) 技术变更带来的业务影响的风险，如自动化或硬件更换；
c) 产品或服务变更带来的业务影响范围的风险；
d) 资源变化带来的恢复活动所需要时间的风险，如人员减少等；
e) 风险评估不足或未及时处置风险带来的业务影响的风险；

f） 风险处置后的残余风险带来的新风险。

A.6 应急信息系统风险

组织应开展突发公共安全事件情况下应急信息系统风险的管控，风险类型包括但不限于：

a） 应急信息系统规划风险，包括未对突发公共安全事件情况下的远程办公系统、远程运营系统、应急全过程控制系统等进行统筹规划或实施过程中存在问题和不足等；
b） 应急信息系统组织架构及人员配备的风险；
c） 应急信息系统管理制度和流程的风险；
d） 应急信息系统供方管理风险；
e） 应急信息系统生存周期管理风险，包括应急信息系统的建设、运行与维护及应用等存在问题和不足；
f） 应急信息系统网络与安全风险；
g） 数据管理风险，包括数据管理组织架构、制度、流程及数据生存周期管理等存在问题和不足；
h） 个人信息保护风险；
i） 应急信息系统远程研发支撑风险；
j） 应急信息系统无障碍风险；
k） 应急信息系统业务连续性风险，包括应急预案的制定、演练的组织管理和实施过程的控制及监督等风险；
l） 应急信息系统全部或部分损失的风险；
m） 应急信息系统风险评估机制与实施的风险。

A.7 IT 应急全过程控制风险

组织应开展突发公共安全事件情况下 IT 应急全过程控制风险的管控，风险类型包括但不限于：

a） 预防与应急准备阶段风险，包括 IT 应急救援队伍组建、与外部的联防联动、综合保障能力、资源投入、应急预案管理（包括应急预案的制定、演练的组织管理和实施过程的控制及监督等）、风险分析管理等存在问题和不足；
b） 监测与预警阶段风险，包括监测与预警总体管理（如组织管理、人员的配备、与外部的联防联动、安全与健康、制度与流程等）、监测与预警平台（如突发事件监测系统、突发事件预测系统、突发事件预警系统、突发事件信息报告系统、突发事件统计分析系统等）管理、网络与信息安全及数据资源整合和安全保护等存在问题和不足；
c） 应急处置与救援阶段风险，包括应急处置救援总体管理（如组织管理、人员配备、与外部联防联动、安全与健康、制度与流程等）、应急处置与救援平台（如应急值守系统、决策指挥系统、事件处置系统、疏散救援系统、资源管理系统、信息舆情系统、应急通信保障系统等）管理、网络与信息安全及数据资源整合和安全保护等存在问题和不足；
d） 事后恢复与重建阶段风险，包括善后处置、调查与评估（如针对特别重大突发公共安全事件的起因、性质、影响、责任、经验教训和恢复重建等）、恢复重建（如制定灾后重建计划、组织实施恢复重建工作等）等方面存在问题和不足。

附 录 B
（资料性）
IT 应急管理专项风险

B.1 人员类风险

组织应开展突发公共安全事件情况下 IT 应急人员风险的管控，风险类型包括但不限于：

a） IT 应急人员战略管理的风险；

b） IT 应急人员管理目标、方针和策略的风险；

c） IT 应急人员社会责任意识与合规意识的风险；

d） IT 应急人员专业技能的风险；

e） IT 应急人员流失的风险；

f） IT 应急人员能力培养的风险；

g） IT 应急人员安全的风险；

h） IT 应急人员疫情防范与健康的风险；

i） IT 应急人员备用的风险；

j） IT 应急人员监督管理的风险。

B.2 资源类风险

组织应开展突发公共安全事件情况下 IT 应急资源风险的管控，风险类型包括但不限于：

a） IT 应急资源范围界定的风险；

b） IT 应急资源规划制定与实施的风险；

c） IT 应急资源组织管理的风险；

d） 与所需承担社会责任相关 IT 应急资源投入的风险；

e） IT 应急资金预算规划及管理的风险；

f） IT 应急资源管理制度和流程的风险；

g） IT 应急数据的风险，包括数据安全、数据生存周期、数据质量及数据灾备等管理不规范或存在问题；

h） IT 应急资源监督管理的风险；

i） 其他风险，如应用系统、平台资源、虚拟资源、物理资源及机房基础设施等管理不规范或不可用。

B.3 技术应用类风险

B.3.1 新技术应用风险

组织应开展突发公共安全事件情况下应急管理新技术应用风险的管控，风险类型包括但不限于：

a） 与外部（国家、地方、行业或领域等）联防联动新技术应用交流与协同的风险；

b） 应急管理新技术应用战略制定与实施的风险；

c） 应急管理新技术应用目标、方针和策略的风险；

d） 应急管理新技术应用组织建设的风险；

e） 应急管理新技术应用制度和流程的风险；

f） 应急管理新技术应用专业人才的风险；

g） 投入资金预算规划及管理的风险；

h） 密码技术应用的风险；

i） 大数据技术应用的风险；

j） 云计算技术应用的风险；

k） 人工智能技术应用的风险；

l） 区块链技术应用的风险；

m） 边缘计算技术应用的风险；

n） 通信技术应用的风险

o） 物联网技术应用的风险；

p） 应急管理新技术应用监督的风险。

B.3.2 IT 应急应用创新风险

组织应开展突发公共安全事件情况下 IT 应急应用创新风险的管控，风险类型包括但不限于：

a） 与外部（国家、地方、行业或领域等）IT 应急应用创新交流与协同的风险；

b） IT 应急应用创新战略制定与实施的风险；

c） IT 应急应用创新管理目标、方针和策略的风险；

d） IT 应急应用创新组织管理的风险；

e） IT 应急应用创新制度和流程的风险；

f） IT 应急应用创新专业人才的风险；

g） 投入资金预算规划及管理的风险；

h） 灾备中心管理的风险；

i） IT 应急应用创新系统管理的风险；

j） IT 应急应用创新办公终端管理的风险；

k） IT 应急应用创新云服务（如公有云、私有云、混合云等）管理的风险；

l） IT 应急应用创新安全管理的风险；

m） IT 应急应用创新自主可控的风险；

n） IT 应急应用创新系统应急预案的制定、演练的组织管理和实施过程的控制及监督等风险。

B.4 过程类风险

B.4.1 预防与应急准备阶段的 IT 应急风险

组织应开展突发公共安全事件情况下预防与应急准备阶段的 IT 应急风险管控，风险类型包括但不限于：

a） 与外部（国家、地方、行业或领域等）联防、联动机制的风险；

b） IT 应急救援队伍建设的风险；

c） IT 应急管理制度和流程的风险；

d) IT 应急管理投入的风险；
e) IT 应急管理制度和流程的风险；
f) IT 应急预案的风险，包括 IT 应急预案的编制、演练组织管理和实施过程的控制及监督等存在问题和不足；
g) IT 应急培训教育的风险；
h) IT 应急综合保障能力建设的风险；
i) IT 应急平台建设、运维及应用等的风险。

B.4.2 监测与预警阶段的 IT 应急风险

组织应开展突发公共安全事件情况下监测与预警阶段的 IT 应急风险管控，风险类型包括但不限于：

a) 监测与预警总体管理风险，包括组织管理、人员配备、与外部联防联动等风险；
b) 人员安全与健康的风险；
c) 监测与预警制度和流程等存在问题和不足；
d) 监测与预警平台管理风险，包括突发事件监测系统管理、突发事件信息报告系统管理、突发事件统计分析系统管理等存在问题和不足。

B.4.3 应急处置与救援阶段的 IT 应急风险

组织应开展突发公共安全事件情况下应急处置与救援的 IT 应急风险管控，风险类型包括但不限于：

a) 应急处置救援总体风险，包括应急处置救援平台的组织管理、人员配备、与外部联防联动、人员安全与健康及制度与流程等存在问题和不足；
b) 应急处置救援平台管理风险，包括应急值守系统、决策指挥系统、事件处置系统、疏散救援系统、资源管理系统、信息舆情系统及应急通信保障系统等管理存在问题和不足；
c) 应急处置过程中人为操作的风险。

B.4.4 事后恢复与重建阶段的 IT 应急风险

组织应开展突发公共安全事件情况下事后恢复与重建的 IT 应急风险管控，风险类型包括但不限于：

a) 事后恢复与重建的 IT 应急管理目标、方针和策略风险；
b) 事后恢复与重建的 IT 应急组织管理风险；
c) 事后恢复与重建的外部联防联动风险；
d) 事后恢复与重建的 IT 应急人员配备、安全与健康风险；
e) 事后恢复与重建的 IT 应急制度与流程风险；
f) 事后恢复与重建工作中的 IT 评价风险；
g) 事后恢复与重建工作中的 IT 补偿风险；
h) 事后恢复与重建工作中的 IT 救助风险；
i) 事后恢复与重建工作中的 IT 恢复风险；
j) 事后恢复与重建工作中的信息管理风险。

B.5 管理类风险

B.5.1 业务连续性风险

组织应开展突发公共安全事件情况下业务连续性风险的管控，风险类型包括但不限于：

a) 组织环境风险，包括未对内外部环境进行全面分析、未充分识别相关方与法律法规要求、业务应急机制匮乏、与外部的联防、联动不足、未明确 IT 应急管理体系的范围、对风险防控的重要性和价值认识不足、尚未形成有效的 IT 应急风险防控管理体系等；

b) 领导力风险，包括组织的各级管理者未能证明其在实现 IT 应急方针和目标方面的承诺和领导力、决策层或最高管理者未能证明其在 IT 应急管理体系方面的承诺、决策层或最高管理者对 IT 应急方针的管理不规范及 IT 应急组织的角色、职责和权力等存在问题和不足；

c) 策划风险，包括应对风险和机会的措施不合理、业务连续性目标未明确及业务连续性实施计划未有效管理等；

d) 支持风险，包括对 BCMS 资源保障的重要性认识有限、备用资源保障不足、承担 BCMS 工作的人员能力不足、相关人员对 BCMS 缺乏适当的意识、未建立业务连续性文化、沟通和协调机制不健全及存档信息管理不规范等 ；

e) 实施风险，包括业务连续性风险管理实施的策划和控制不完善、业务影响分析和风险评估工作不符合要求、业务连续性策略不合理、业务恢复目标不明确、业务连续性程序的建立和实施存在不足及演练和测试工作不规范等；

f) 绩效评估风险，包括监测、测量、分析和评价工作不规范、内部审核未发挥应有的作用及管理评审工作未有效开展等；

g) 改进风险，包括针对不符合项未采取有效措施、BCMS 持续改进工作存在不足等；

h) 业务连续性监督管理的风险。

B.5.2 IT 应急演练风险

组织应开展突发公共安全事件情况下 IT 应急演练风险的管控，风险类型包括但不限于：

a) IT 应急演练目的、原则、形式的风险；

b) IT 应急演练规划的风险；

c) IT 应急演练组织架构的风险；

d) IT 应急演练人员配备的风险；

e) IT 应急演练人员疫情防范与健康的风险；

f) IT 应急演练制度和流程的风险

g) IT 应急演练实施过程的风险，包括准备阶段、实施阶段、评估与总结阶段及成果运用阶段等存在问题和不足；

h) IT 应急演练监督管理的风险。

B.5.3 应急公共服务平台风险

组织应开展突发公共安全事件情况下应急公共服务平台风险的管控，风险类型包括但不限于：

a) 应急公共服务平台规划的风险，包括对随身办、健康云、互助通道、志愿者通道、指挥通道、救援

通道、宣传通道及有限通信资源调度等的统筹规划和实施过程中存在问题和不足；

b） 应急公共服务平台组织架构的风险；

c） 应急公共服务人员配备的风险；

d） 应急公共服务人员疫情防范与健康风险；

e） 应急公共服务平台管理制度和流程的风险；

f） 应急公共服务平台供方管理的风险；

g） 应急公共服务平台生存周期管理的风险，包括公共平台的建设、运营及应用等存在问题和不足；

h） 网络与信息安全及数据资源整合和安全保护的风险；

i） 应急信息无障碍的风险；

j） 应急公共服务业务连续性的风险，包括应急预案的制定、演练的组织管理和实施过程的控制及监督等风险；

k） 应急公共服务平台压力测试风险；

l） 应急公共服务平台监督管理的风险。

B.5.4 应急远程办公和远程运营风险

组织应开展突发公共安全事件情况下应急远程办公和远程运营风险的管控，风险类型包括但不限于：

a） 应急远程办公和远程运营与外部联动、控制的风险；

b） 应急远程办公和远程运营环境的风险；

c） 应急远程办公和远程运营管理组织架构及人员配备的风险；

d） 应急远程办公和远程运营管理制度和流程的风险；

e） 应急远程办公和远程运营人员能力（如知识、技能、经验等）的风险；

f） 应急远程办公和远程运营人员安全的风险；

g） 应急远程办公和远程运营人员疫情防范与健康的风险；

h） 应急远程办公和远程运营人员备份的风险；

i） 应急远程办公和远程运营人员培训教育的风险；

j） 应急远程办公和远程运营人员绩效管理的风险；

k） 应急远程办公和远程运营平台管理的风险；

l） 应急远程办公和远程运营平台供方管理的风险；

m） 网络与信息安全的风险；

n） 数据安全与个人信息保护的风险；

o） 数据资源整合和安全保护的风险；

p） 应急远程办公和远程运营业务连续性的风险，包括应急预案的制定、演练的组织管理和实施过程的控制及监督等风险；

q） 应急远程办公和远程运营通信安全的风险；

r） 应急远程办公和远程运营操作的风险；

s） 应急远程办公和远程运营风险评估机制与实施的风险；

t） 应急远程办公和远程运营监督管理的风险。

B.5.5 IT 应急安全管理风险

组织应开展突发公共安全事件情况下 IT 应急安全管理风险的管控，风险类型包括但不限于：

a） IT 应急安全管理目标、方针和策略的风险；
b） IT 应急安全战略制定与实施的风险；
c） IT 应急安全组织建设的风险；
d） 与外部联防联动安全的风险；
e） IT 应急安全管理制度和流程的风险；
f） 人员安全与健康的风险；
g） 网络与信息安全的风险；
h） 数据安全与个人信息保护的风险；
i） 供方安全的风险；
j） 云计算技术应用安全的风险；
k） 信息系统生存周期安全的风险；
l） 大数据技术应用安全的风险；
m） 人工智能技术应用安全的风险；
n） 终端安全的风险；
o） 供应链安全的风险；
p） 互联网应用安全的风险；
q） 区块链技术应用安全的风险；
r） 移动互联网应用安全的风险；
s） 通信技术应用安全的风险
t） 物联网技术应用安全的风险；
u） 开源软件应用安全的风险；
v） IT 应急安全监督管理的风险。

B.5.6 应急云服务风险

组织应开展突发公共安全事件情况下应急云服务风险的管控，风险类型包括但不限于：

a） 应急云服务管理目标、方针和策略的风险；
b） 应急云服务与外部联防联动的风险；
c） 应急云服务组织管理的风险，包括与组织架构、责任人、角色、职责和权限等存在问题和不足；
d） 应急云服务战略管理的风险；
e） 应急云服务管理制度和流程的风险；
f） 应急云服务人员安全与健康的风险；
g） 应急云服务模式分类及控制机制的风险；
h） 应急云服务供方管理的风险；
i） 网络与信息安全的风险；
j） 应用安全的风险，包括终端用户安全、软件即服务（SaaS）应用安全、平台即服务（PaaS）应用安全及基础设施即服务（IaaS）应用安全等风险；

k) 虚拟化安全的风险，包括虚拟化软件安全、虚拟化服务器安全、软件、服务器还有网络、存储等风险；

l) 云平台业务连续性风险，包括应急预案的制定、演练的组织管理和实施过程的控制及监督等风险；

m) 数据资源整合和安全保护的风险；

n) 云平台数据保存与恢复的风险；

o) 容灾备份的风险；

p) 应急云服务监督管理的风险。

B.5.7 不可抗力风险

组织应开展突发公共安全事件情况下不可抗力 IT 应急风险的管控，风险类型包括但不限于：

a) 不可抗力外部联防、联动的风险；

b) 不可抗力 IT 应急战略管理的风险；

c) 不可抗力 IT 应急管理目标、方针和策略的风险；

d) 不可抗力 IT 应急安全管理的风险；

e) 人员安全与健康管理的风险；

f) 不可抗力相关 IT 应急财产安全管理的风险；

g) 不可抗力相关 IT 应急赔偿的风险。

B.5.8 合作伙伴风险

组织应对突发公共安全事件情况下合作伙伴 IT 应急风险的管控，风险类型包括但不限于：

a) 合作伙伴 IT 应急管理目标、方针和策略的风险；

b) 合作伙伴 IT 应急战略管理的风险；

c) 合作伙伴 IT 应急组织管理的风险；

d) 合作伙伴 IT 应急人员安全与健康的风险。

B.5.9 合规风险

组织应开展突发公共安全事件情况下 IT 应急合规风险的管控，风险类型包括但不限于：

a) IT 应急合规战略制定与实施的风险；

b) IT 应急合规管理目标、方针和策略的风险；

c) IT 应急合规组织管理的风险；

d) 与外部联防、联动的 IT 应急合规风险；

e) IT 应急合规管理制度与流程的风险；

f) IT 应急合规管理实施的风险，如违反网络安全法、数据安全法、个人信息保护法、网络安全等级保护及业务连续性管理等要求的风险。

B.5.10 网络舆情管理风险

组织应开展突发公共安全事件情况下网络舆情风险的管控，风险类型包括但不限于：

a) 网络舆情管理目标和策略的风险；

b） 网络舆情组织管理的风险；

c） 网络舆情管理制度和流程的风险；

d） 网络舆情管理培训教育的风险；

e） 与外部联防、联动机制的风险，如机制不完善，与外部（如国家相关主管部门、行业监管机构等）进行沟通、汇报不及时等；

f） 其他风险，包括未建立合理的网络舆情管理风险评估机制、未实际开展网络舆情管理风险评估活动等。

B.5.11 数字化转型风险

组织应开展突发公共安全事件情况下IT应急管理数字化转型风险的管控，风险类型包括但不限于：

a） IT应急管理数字化转型战略管理的风险；

b） IT应急管理数字化转型目标、方针和策略的风险；

c） 与外部联防、联动数字化转型的风险；

d） IT应急管理数字化转型制度和流程的风险；

e） 网络与信息安全的风险；

f） 数据安全与个人信息保护的风险；

g） 数字化转型平台管理的风险；

h） IT应急管理数字化转型监督管理的风险。

附 录 C
（资料性）
IT 应急风险管理组织架构与管理体系

C.1 概述

实施全面风险管理的组织，应建立突发公共安全事件情况下的 IT 应急风险管理组织架构与管理体系，并将 IT 应急风险管理纳入全面风险管理体系。其他组织（如政府部门、事业单位以及公共服务机构等）参考应用思路说明（见 C.4）。

C.2 IT 应急风险管理组织架构

组织应建立突发公共安全事件情况下的 IT 应急风险管理组织架构，包括但不限于如下内容。

a） 董事会是组织应对突发公共安全事件的 IT 应急风险管理决策机构，对相关的 IT 应急风险管理承担最终责任。主要职责包括但不限于：

- 遵守并贯彻执行国家有关应对突发公共安全事件的法律、法规和技术标准，落实上级主管部门、监管机构等的相关要求；
- 建立应对突发公共安全事件的 IT 应急风险管理文化；
- 评估配合国家、地方、行业或领域等开展 IT 应急风险工作及与外部联防、联动机制运作的效率和效果；
- 审批应对突发公共安全事件的 IT 应急风险管理战略、政策和程序，评估相关 IT 应急及其风险管理工作的总体成效及合规性；
- 监督高级管理层开展应对突发公共安全事件的 IT 应急风险管理工作；
- 审议应对突发公共安全事件的 IT 应急风险管理报告。

注：董事会可以授权其下设的风险管理委员会履行其应对突发公共安全事件的 IT 应急风险管理部分职责。

b） 高级管理层负责执行经董事会批准的应对突发公共安全事件 IT 应急风险管理政策。主要职责包括但不限于：

- 明确与外部联防、联动工作相关的职责与分工，并建立运行机制；
- 明确业务部门、职能部门、IT 部门以及其他部门有关 IT 应急风险管理的职责与分工，建立部门之间相互协调、有效制衡的运行机制；
- 制定清晰的执行和问责机制，确保相关 IT 应急风险管理战略的充分传达和有效实施；
- 制定相关的 IT 应急风险管理政策和程序，定期评估，必要时予以调整；
- 核查相关的 IT 应急风险管理工作落实和实施情况，督促落实不到位工作的整改；
- 评估相关的 IT 应急风险管理状况并向董事会报告。

c） 风险管理部门或其他综合管理部门牵头应对突发公共安全事件的 IT 应急总体风险管理工作，主要职责包括但不限于：

- 加强与外部相关 IT 应急工作的协同配合；
- 实施相应的 IT 应急风险管理体系建设；
- 指导、评估、监督各部门的相关 IT 应急风险管理工作；
- 持续监控相关 IT 应急风险管理战略、政策和程序执行情况，对违反相应风险管理政策和程序的情况及时预警、报告并提出处理建议；

- 组织开展相关 IT 应急风险评估，及时发现风险隐患和管理漏洞，持续提高风险管理的有效性；
- 对本部门相关 IT 应急风险管理工作的合规和成效负责。

d) 业务条线部门作为应对突发公共安全事件的 IT 应急管理执行部门，同时应承担相应的 IT 应急执行风险管理直接责任。主要职责包括但不限于：
- 执行相应的 IT 应急风险管理政策和程序；
- 对相关风险评估、业务影响分析的合理性和有效性负责；
- 对相关重要业务恢复目标和恢复策略确定工作的成效负责；
- 对相关业务条线重要业务应急响应与恢复工作的成效负责。

e) IT 部门作为应对突发公共安全事件的 IT 应急管理执行部门，同时应承担相应的 IT 应急执行风险管理直接责任。主要职责包括但不限于：
- 执行相关的 IT 应急风险管理政策和程序；
- 对组织的相关 IT 应急响应与恢复工作成效负责；
- 对本部门相关的 IT 应急管理工作合规和成效负责。

f) IT 应急保障管理部门（如办公室、人力资源部门、财务部门、法律合规部门、公共关系部门、后勤部门等）作为应对突发公共安全事件的 IT 应急管理保障部门，同时应承担 IT 应急保障风险管理责任。主要职责包括但不限于：
- 对相关应急处置所需人力、物力和财力等资源保障工作的成效负责；
- 对相关应急处置对外报告、宣告、通报和沟通与协调工作的成效负责；
- 对外媒体公关、秩序维护、安全保障、法律咨询和人员安抚等相关工作的成效负责；
- 对各自内部相关的 IT 应急管理工作合规和成效负责。

g) 内部审计部门应承担组织应对突发公共安全事件的 IT 应急风险管理审计工作。主要职责包括但不限于：
- 审核相关业务影响分析、风险评估、恢复策略及恢复目标的合理性和完整性；
- 审核相关 IT 应急计划的完整性和可操作性；
- 审核相关 IT 应急计划演练过程及报告的真实性和有效性；
- 审核相关 IT 应急风险总体管理工作的合规性、合理性和有效性；
- 审核相关 IT 应急管理执行工作的合规性、合理性和有效性；
- 审核相关 IT 应急保障工作的合规性、合理性和有效性；
- 对本部门相关 IT 应急审计管理工作的合规和成效负责。

C.3 IT 应急风险管理体系

C.3.1 IT 应急总体风险管理

组织应建立突发公共安全事件情况下的 IT 应急总体风险管理机制，包括但不限于：

a) 明确 IT 应急总体风险管理部门（如风险管理部门或其他综合管理部门）的相关 IT 应急风险管理职责、岗位职责和权限；
b) 进行人员配备，并确保人员安全和健康；
c) 持续监控相关 IT 应急风险管理战略、政策和程序的执行；
d) 组织开展相关 IT 应急风险评估工作，并向决策层提交报告。

C.3.2 IT 应急执行风险管理

组织应建立突发公共安全事件情况下的 IT 应急执行风险管理机制，包括但不限于：

a) 明确业务部门和IT部门的相关IT应急风险管理职责、岗位职责和权限；
b) 进行人员配备，并确保人员安全和健康；
c) 要求业务部门和IT部门执行相关IT应急风险管理政策和程序；
d) 要求业务部门和IT部门定期开展相关IT应急风险管理自评估，并持续改进。

C.3.3 IT应急保障风险管理

组织应建立突发公共安全事件情况下的IT应急保障风险管理机制，包括但不限于：

a) 明确应急保障管理部门（如办公室、人力资源部门、财务部门、法律合规部门、公共关系部门、后勤部门等）的相关IT应急风险管理职责、岗位职责和权限；
b) 进行人员配备，并确保人员安全和健康；
c) 要求应急保障管理部门执行相关IT应急风险管理政策和程序；
d) 要求各应急保障管理部门定期开展相关IT应急风险管理自评估，并持续改进。

C.3.4 IT应急风险审计管理

组织应明确突发公共安全事件情况下的IT应急风险管理审计要求，包括但不限于：

a) 明确内部审计部门的相关IT应急风险管理审计职责、岗位职责和权限；
b) 进行人员配备，并确保人员安全和健康；
c) 要求内部审计部门制定相关的IT应急风险管理审计制度和流程；
d) 要求内部审计部门定期开展相关的IT应急风险管理审计活动。

C.3.5 其他IT应急风险管理

对于本文件未明确的其他应对突发公共安全事件的IT应急风险管理内容，组织在提出相关管理要求时，宜依据相应的标准规范建立。

C.4 其他组织的应用思路说明

其他组织（如政府部门、事业单位以及公共服务机构等），应依据相关要求并考虑所处行业、领域和自身的实际，建立本组织突发公共安全事件情况下的IT应急风险管理组织架构与管理体系，加强对IT应急管理合理性、有效性的监督和评价，促进IT应急管理能力的持续提升，确保业务的持续运营。

附 录 D
（资料性）
突发公共安全事件情况下的整体应用场景

D.1 概述

IT 应急风险管理方法论在突发公共安全事件（如新型冠状肺炎疫情等）情况下的整体应用，主要是以实施全面风险管理的企业为例，其他组织（如政府部门、事业单位、公共服务机构及其他未实施全面风险管理的企业等）参考应用思路说明（见 D.7）。

D.2 背景介绍

某公司业务经营范围涵盖非寿险业务的各个领域，包括机动车辆保险、企业财产保险、工程险、货物运输保险、责任险、信用保险、保证保险、家庭财产保险、船舶险、农业保险、电话营销专用车险及环境污染责任险等。

2020 年开始，新型冠状肺炎疫情逐步暴发，对人民生命健康及社会经济发展等造成难以估计的影响。作为保险公司，公司需要采取应对措施，尽可能为用户办理更多的业务。

D.3 疫情初期阶段的应对

D.3.1 明确 IT 应急管理依据并下发通知

疫情初期，主要依据公司 2018 年 12 月发布的“突发公共安全事件综合应急预案”，以及因疫情于 2020 年 2 月补充下发的“关于当前疫情形势下进一步加强疫情防控的通知”进行应对。

D.3.2 应急预案主要内容

D.3.2.1 突发公共安全事件综合应急预案

“突发公共安全事件综合应急预案”的主要内容包括总则、事故风险描述、应急组织机构及职责、预警及信息报告、应急响应、信息公开、后期处理、保障措施、应急预案管理及附件。其中应急组织机构及职责如下。

a) 董事会是突发公共安全事件情况下 IT 应急管理的决策机构，对 IT 应急管理承担最终责任。主要职责包括：
   - 审核和批准应对突发公共安全事件的 IT 应急管理战略、政策和程序；
   - 审批高级管理层应对突发公共安全事件的 IT 应急管理职责，定期听取高级管理层关于相关 IT 应急管理的报告，监督、评价其履职情况；
   - 审批应对突发公共安全事件的 IT 应急管理年度审计报告。

b) 高级管理层负责执行经董事会批准的应对突发公共安全事件 IT 应急管理政策。主要职责包括：
   - 制定 IT 应急管理政策、程序，并定期审查和监督执行情况；
   - 明确各部门应对突发公共安全事件的 IT 应急管理职责，明确报告路线，审批重要业务恢复目标和恢复策略，督促各部门履行管理职责，确保相关 IT 应急管理体系正常运行；
   - 确保配置足够的资源保障相关 IT 应急管理的实施。

c) 设置或明确应对突发公共安全事件的IT应急管理综合协调部门和专项突发公共安全事件应急管理分管部门，负责：
- 组织相关的IT应急体系建设；
- 组织编制公司总体相关的IT应急预案；
- 组织协调分管部门开展相关的IT应急管理日常工作。

d) 业务部门为突发公共安全事件情况下的IT应急管理执行部门，主要负责：
- 风险评估、业务影响分析；
- 确定相关重要业务恢复目标和恢复策略；
- 负责业务条线相关重要业务应急响应与恢复。

e) 信息科技部门为突发公共安全事件情况下的IT应急管理执行部门，主要负责：
- 相关IT应急响应与恢复；
- 制定部门相关应急预案并进行演练。

f) 突发公共安全事件情况下的IT应急保障层由IT应急管理保障部门（如办公室、人力资源部门、财务部门、法律合规部门、公共关系部门、后勤部门等）组成，主要负责：
- 相关IT应急处置所需人力、物力和财力等资源保障；
- 相关IT应急处置对外报告、宣告、通报、沟通与协调；
- 对外媒体公关、秩序维护、安全保障、法律咨询和人员安抚等相关工作。

D.3.2.2 关于当前疫情形势下进一步加强疫情防控的通知

“关于当前疫情形势下进一步加强疫情防控的通知”主要是针对疫情情况下园区办公、居家办公等进行规定，具体包括人员管理、资源管理、技术管理及过程管理等。

D.3.3 实施结果分析

虽然公司已有相关应急预案，但通过对应急预案实施结果进行分析，发现该阶段针对新型冠状肺炎疫情的应急处置存在以下情况：
- 各层级各自为政、应急组织能力各有高低，未能发挥上下级、同级资源的协同效应；
- 有些分支机构在新型冠状肺炎疫情升级后暴露出应急响应迟缓、处置能力不足等问题。

鉴于全球新型冠状肺炎病毒不断演变、可能与人类长期共存等影响，为全面掌握突发公共安全事件下IT应急管理存在的风险或问题，加强与外部的联防、联动，避免因违规导致处罚、遭受财务损失及影响公司声誉等情况的发生，提升整体IT应急处置能力，公司决定聘请第三方开展针对突发公共安全事件的IT应急风险管理专项审计。

D.4 IT应急风险管理专项审计的实施

D.4.1 审计目的

通过IT应急风险管理专项审计，了解公司应对突发公共安全事件的IT应急管理总体状况，对公司是否实现IT应急战略目标进行审查和评估，充分识别与评估相关风险，并提出评价意见及改进建议，以加强与外部的联防、联动，促进公司整体IT应急处置能力的提升。

D.4.2 审计范围

审计范围主要从总体范围、组织范围、逻辑范围和物理范围等确定，包括：

a) 总体范围，根据审计目的和投入的审计成本确定；

b) 组织范围，包括IT应急组织机构（如董事会、高级管理层、分管部门、业务部门、IT部门及保障部门等）、制度、流程及IT应急管理活动等；
c) 逻辑范围，包括应急信息系统及环境等；
d) 物理范围，包括生产中心及灾备中心等。

D.4.3 审计内容

审计内容包括但不限于：
a) 与外部的联防、联动机制；
b) IT应急战略；
c) IT应急组织；
d) IT应急架构；
e) IT应急运行体系；
f) 业务影响分析和风险评估；
g) 应急信息系统（含数据安全与个人信息保护等）；
h) IT应急全过程控制（包括预防与应急准备、监测与预警、应急处置与救援、事后恢复与重建等）。

D.4.4 审计发现

通过审计，发现公司针对突发公共卫生安全事件下的IT应急管理存在以下问题和不足，如：
a) 与外部（国家、地方、行业或领域等）联防、联动机制存在缺陷，如沟通不畅、配合不力等；
b) 董事会和高级管理层对IT应急管理重视程度有限，尤其是对新型冠状肺炎疫情的影响程度、影响时间（如短期还是长期等）及可能产生的后果估计不足，缺乏系统的、针对性的应急预案；
c) IT应急管理综合协调部门和专项突发事件应急管理分管部门未能充分发挥其指导、监督及评价的作用，导致各部门应急处置过程中遇到的某些问题时只能自行判断、解决，缺乏必要的沟通和配合；
d) IT应急管理注重短期行为，缺少相关的战略规划；
e) 未将IT应急风险管理纳入公司全面风险管理体系，管理层及员工IT应急风险管理意识薄弱；
f) IT应急管理工作无问责机制，导致相关工作只注重形式，很少关注其合理性和有效性；
g) 员工健康管理缺少相关制度与流程，尤其是针对新冠等突发公共卫生安全事件更是缺少有效的管控措施；
h) 针对居家办公或混合办公（如部分居家办公、部分公司办公等）等缺少细则要求；
i) 针对应急管理信息系统的获取（如购入成品、开发等）缺少有效的控制；
j) 存在网络与信息安全风险、数据安全风险及个人信息保护风险等；
k) 应急数据生存周期管理不规范等。

D.4.5 审计结论

公司需加强应对突发公共卫生安全事件的IT应急管理，对审计报告中反映的问题和不足进行整改。

D.5 疫情发展阶段的应对

D.5.1 整改思路

董事会和高级管理层非常重视IT应急管理专项审计的结果，针对审计报告中反映的IT应急管理不足或存在的问题决定进行整改，包括但不限于：

a) 完善与外部（国家、地方、行业或领域等）的联防、联动机制，加强沟通与协同；
b) 将IT应急管理战略纳入公司总体战略进行统筹考虑；
c) 在“突发公共安全事件综合应急预案”基础上制定“分类应急预案”；
d) 将IT应急风险管理纳入公司全面风险管理体系；
e) 建立IT应急管理问责机制，IT应急工作不仅重视如何应对，还需确保应对措施的合理性和有效性；
f) 加强对员工健康的规范管理；
g) 针对居家办公或混合办公等制定细则；
h) 加强网络与信息安全管理、数据安全管理及个人信息保护等。

D.5.2 建立IT应急风险管理机制

将应对突发公共卫生安全事件的IT应急风险管理纳入公司全面风险管理体系，建立相关IT应急风险管理机制并规范运行，促进公司相关IT应急管理能力的提升，包括：

a) IT应急顶层设计方面：董事会和高级管理层加强应对突发公共卫生安全事件的IT应急战略、组织与IT架构管理，采取措施避免相关风险的发生（参考第6章、第7章、第10章、C.2及A.1、A.2、A.3等）；
b) IT应急管理体系方面：完善应对突发公共卫生安全事件的IT应急运行体系，重视相关的业务影响分析和风险评估、应急信息系统管理工作，采取措施避免相关风险的发生（参考第9章、A.4、A.5、A.6及C.3等）；
c) IT应急全过程控制方面：完善与应对突发公共卫生安全事件相关的预防与应急准备、监测与预警、应急处置与救援、事后恢复与重建等工作，采取措施避免相关风险的发生（参考第11章、A.7等）。

D.5.3 建立IT应急风险管理组织架构

通过建立应对突发公共卫生安全事件的IT应急风险管理组织架构（参考C.2），促进相关IT应急组织管理工作的有效提升。

a) 明确各类机构、部门的职责。
b) 对各类机构、部门进行相关IT应急管理的问责，如：
   - 董事会负最终责任；
   - 高级管理层负总体管理责任；
   - 业务部门及IT部门负直接责任；
   - 保障部门负保障责任；
   - IT应急管理综合协调部门和专项突发事件应急管理分管部门负指导、监督和评估责任；
   - 内部审计部门负审计责任等。
c) 要求各类机构、部门不仅履行相关的IT应急职责要求，并且应对相关工作的合规性、合理性和

成效负责。

d) 促进各类机构、部门在开展相关的 IT 应急管理工作时，有机协调与配合，提升整体工作成效等。

e) 通过对相关 IT 应急管理工作进行计划、实施、检查和改进，不断提升 IT 应急管理水平。

D.5.4 实施 IT 应急风险管理

公司在实施应对突发公共卫生安全事件的 IT 应急风险管理时，需与 IT 应急管理进行整合，实施过程包括：

a) 统筹和规划阶段：将应对突发公共卫生安全事件的 IT 应急风险管理与 IT 应急管理进行紧密结合，在决策层或最高管理者的领导下，充分发挥 IT 应急风险管理的作用(参考 11.1)；

b) 构建和运行阶段：结合应对突发公共卫生安全事件的 IT 应急管理实施，构建相关的 IT 应急风险管理实施机制和路径，确保 IT 应急风险管理实施的有序运行和成效(参考 11.2)；

c) 监控和评价阶段：监控应对突发公共卫生安全事件的 IT 应急风险管理实施过程以及与 IT 应急管理的对接情况，评价相关工作的成效与合规，保障 IT 应急风险管理目标的实现(参考 11.3)；

d) 改进和优化阶段：对突发公共卫生安全事件情况下的 IT 应急风险管理以及与 IT 应急管理的对接工作进行持续改进(参考 11.4)。

D.6 实施效果分析

D.6.1 概述

IT 应急管理旨在为应对突发公共安全事件开展 IT 领域的应急管理，IT 应急风险管理旨在应对基础上进一步强调 IT 应急控制措施的合理性和有效性。

公司通过整改与应对突发公共安全事件(如新型冠状肺炎疫情等)相关的 IT 应急管理工作，引入 IT 应急风险管理机制，不但注重突发公共安全事件下董事会、高级管理层、业务部门、IT 部门及保障部门的作用，同时充分发挥 IT 应急管理综合协调部门和专项突发事件应急管理分管部门及审计部门的作用。

D.6.2 落实综合协调部门和分管部门的职责

落实应对突发公共安全事件的 IT 应急管理综合协调部门和专项突发事件应急管理分管部门的职责，如：

a) 实施相关的 IT 应急风险管理体系建设；

b) 指导、评估、监督业务部门和 IT 部门等相关的 IT 应急风险管理工作；

c) 持续监控相关的 IT 应急风险管理战略、政策和程序的执行情况，对违反风险管理政策和程序的情况及时预警、报告并提出处理建议；

d) 组织开展相关的 IT 应急风险评估，及时发现风险隐患和管理漏洞，持续提高风险管理的有效性；

e) 对本部门相关 IT 应急风险管理工作的合规和成效负责。

D.6.3 落实审计部门应对突发公共安全事件的职责

落实审计部门应对突发公共安全事件的职责，如：

a) 审核相关业务影响分析、风险评估、恢复策略及恢复目标的合理性和完整性；

b） 审核相关 IT 应急计划的完整性和可操作性；
c） 审核相关 IT 应急计划演练过程及报告的真实性和有效性；
d） 审核相关 IT 应急风险总体管理工作的合规性、合理性和有效性；
e） 审核相关 IT 应急管理执行工作的合规性、合理性和有效性；
f） 审核相关 IT 应急保障工作的合规性、合理性和有效性；
g） 对本部门相关 IT 应急审计管理工作的合规和成效负责。

D.6.4 持续提升 IT 应急处理能力

通过开展应对突发公共安全事件的 IT 应急风险管理，公司 IT 应急风险管理意识和社会责任感显著增强，IT 应急处理能力持续提升，并实现以下效果：

a） 在政府的统筹领导下，发生新的突发公共安全事件时，能加强与外部的联防、联动，沉着应对各种 IT 应急风险，公司 IT 应急相关资源的统筹与调配能力全面提升，避免无序和失控情况的发生；
b） 在日常的 IT 管理中，将 IT 应急风险管理意识贯穿于价值、制度、机制和能力等方面，建立和完善应对突发公共安全事件的 IT 应急风险管理体系，提高公司的预期管理能力及增强社会责任意识；
c） 突发公共安全事件情况下的 IT 应急风险管理属于公司风险管理体系一部分，公司通过加强对相关 IT 应急管理合理性、有效性的监督和评价，有力促进 IT 应急管理能力的持续提升，确保业务的持续运营。

D.7 其他组织的应用思路说明

其他组织（如政府部门、事业单位以及公共服务机构等），可参考上述突发卫生安全事件情况下公司的应用场景（参考 D.1、D.2、D.3、D.4、D.5），并考虑行业、领域和自身实际等，建立本组织应对突发公共安全事件的 IT 应急风险管理框架，加强对 IT 应急管理合理性、有效性的监督和评价，促进 IT 应急管理能力的持续提升，确保业务的持续运营。

附 录 E
（资料性）
突发公共安全事件情况下的具体应用场景

E.1 概述

IT 应急风险管理方法论不仅适用于突发公共安全事件情况下组织整体 IT 应急管理能力的提升，同时适用于某一具体的 IT 应急管理领域（如信息系统应急管理），为各类组织（包括企业、政府部门、事业单位以及公共服务机构等）提供借鉴。以下应用场景主要以实施全面风险管理的企业为例，其他组织（如政府部门、事业单位、公共服务机构及未实施全面风险管理的企业等）参考应用思路说明（见 E.5）。

E.2 背景介绍

近年来，有组织、有目的的大规模网络攻击愈加明显，诸如数据泄漏、勒索软件、黑客攻击等网络安全事件频发，国内和国际局势日益严峻，尤其是金融行业，由于个人信息数据更加完备且价值度高，逐渐成为各类攻击的首选目标，信息泄露事件层出不穷，已成为个人信息泄漏的重灾区。

某公司遵循监管要求，公司早期根据 RTO 和 RPO，结合风险控制策略，从基础设施、网络、信息系统等不同方面，制定了信息系统应急管理预案。

为了保障网络安全，公司将 IT 应急风险管理方法融入信息系统应急风险管理工作中的重要性，进一步加强网络与信息安全管理工作，以实现对现有信息系统应急管理方法和应急信息系统的优化和改进。

E.3 将 IT 应急风险管理方法融入信息系统应急管理工作

E.3.1 概述

为了防范日益严重的网络安全威胁，有效应对突发网络公共安全事件，公司将 IT 应急风险管理方法融入信息系统应急管理工作。通过加强与外部（国家、地方、行业或领域等）的联防、联动，以及事前预防、事中控制和事后总结，不断提升应对突发网络公共安全事件的信息系统应急处理能力。

E.3.2 事前预防-不断完善信息系统应急预案

E.3.2.1 组织架构

建设并完善应对突发网络公共安全事件的 IT 应急组织体系，包括：

a) 明确与外部（国家、地方、行业或领域等）的联防、联动责任部门；
b) 明确董事会和高级管理层对公司相关 IT 应急管理政策及其实施效果负有最终责任；
c) 明确风险管理部门牵头相关 IT 应急总体管理工作，并对工作成效和合规负责；
d) 明确信息科技管理部门和业务部门负责相关 IT 应急管理工作，并对工作成效和合规负直接责任；
e) 明确应急保障管理部门（如人力资源部门、计划财务部门、公共关系部门、安全保卫部门、后勤保障部门等）承担相关信息系统应急保障管理责任，并对工作成效和合规负责；
f) 组建各类应急小组，包括：

- 应急领导小组，由高管人员任相关应急领导小组组长，各相关职能部门等为相关应急领导小组成员；
- 应急执行小组，由业务部门、信息科技管理部门、运营部门等相关人员组成；
- 支持保障小组，由其他如人力资源部门、计划财务部门、公共关系部门、安全保卫部门、后勤保障部门等相关人员组成。

E.3.2.2 确定 RTO 和 RPO

公司根据业务等级确定 RTO 和 RPO。

E.3.2.3 建立完善的预警系统

建立完善的预警系统，加强与外部的联防、联动，对涉及的突发网络公共安全事件进行风险分析，科学实行风险分级机制，将信息系统突发事件等级划分为特别重大、重大、较大三个等级。

建立监测预警和信息通报机制，通过与外部的联防、联动，对 IT 风险进行预警。明确各类故障的诊断方法和流程。提前制定 IT 应急响应流程和应急处置操作手册，做到“及时发现、科学认定、有效处置”。

E.3.2.4 建立新型更完善的应急处理系统

为有效开展应对突发网络公共安全事件的信息系统应急管理，公司计划建立新型更完善的应急处理系统，即应急、容灾和备份相关系统的建设，确保在突发网络公共安全事件后，能快速恢复数据、信息系统和业务。具体包括：

a) 为保证网络安全，部署多层次网络安全纵深防御措施，重视与外部的联防、联动，切实保障信息安全；
b) 为保证业务安全，在原有两地三中心的架构上，继续演进为三地五中心，确保业务连续性；
c) 为保障数据安全，采用数据备份、副本数据管理等技术手段，切实保证数据安全。

E.3.2.5 加强新型的应急演练

在新风险形势下加强新型的应急演练，如积极开展“护网行动”。在演练过程中找问题、补短板，检验关键信息基础设施及重要信息系统网络安全，切实提升 IT 基础设施的保护水平，提高突发网络公共安全事件的应对能力，打造“防得住”的应对体系。

E.3.3 事中控制-优化应急处置流程

根据预先制定的相关应急预案，进行快速风险定位和风险应对，根据故障等级，采取相应的应急处置流程，并及时报告应急领导小组。应对突发公共安全事件的应急处置，注重保障业务活动能够持续运营或在业务活动中断后将其恢复到正常状态。

对于突发网络公共安全事件，如业务中断，可依据应对流程采取业务容灾切换等措施；如引起数据丢失或发生勒索病毒，可按照应急处置流程进行数据即时恢复等操作。

E.3.4 事后总结-进行总结评估和持续改进

持续改进应对突发公共安全事件的 IT 应急管理，有利于提升 IT 应急风险管理意识及社会责任感。只有不断总结，才能吸取教训，真正做到保证安全。

在护网等应急演练结束后，公司撰写相应的网络应急演练总结报告，分析存在的问题并提出后续改进措施。根据每年护网行动总结报告提出的改进建议进行整改，及时修订相应的应急预案并归档。

同时每年对突发网络公共事件风险防范措施和应急响应工作重新评估，及时发现新的网络风险，验证IT应急预案的有效性和完备性，检验防范措施的合理性和有效性，并不断持续改进。

E.4 应用效果分析

通过将应对突发网络公共安全事件的IT应急风险管理理念融入信息系统应急管理工作，公司信息系统应急风险管理意识显著增强，相应的应急处理能力持续提升，并实现以下效果：

a) 面临新的突发网络公共卫生安全事件时，充分加强与外部的联防、联动，能沉着应对各种信息系统应急管理风险，相关资源的统筹与调配能力有效提升，避免无序和失控情况的发生；

b) 与时俱进，通过不断优化的信息系统应急处理流程、更新的IT技术保障、更全面的网络应急演练，从多维度保障信息系统应急管理的合理性和有效性，持续提升信息系统应急管理能力，从容应对突发网络公共安全事件，确保业务的稳定运营，并增强社会责任意识。

E.5 其他组织的应用思路说明

其他组织（如政府部门、事业单位以及公共服务机构等），可参考上述突发网络公共安全事件情况下公司的应用场景，并考虑行业、领域和自身实际情况等，建立本组织应对突发网络公共安全事件的信息系统应急管理工作，加强对信息系统应急管理合理性、有效性的监督和评价，促进信息系统应急管理能力的持续提升，确保业务的持续运营。

参 考 文 献

[1] GB/T 19000—2016 质量管理体系 基础和术语
[2] GB/T 20984 信息安全技术 信息安全风险评估规范
[3] GB/T 24353 风险管理 指南
[4] GB/T 26317 公司治理风险管理指南
[5] GB/T 30146 公共安全 业务连续性管理体系 要求
[6] GB/T 31595 公共安全 业务连续性管理体系 指南
[7] GB/T 34960.1 信息技术服务 治理 第1部分:通用要求
[8] GB/T 34960.2 信息技术服务 治理 第2部分:实施指南
[9] GB/T 34960.3 信息技术服务 治理 第3部分:绩效评价
[10] GB/T 34960.4 信息技术服务 治理 第4部分:审计导则
[11] GB/T 35561 突发事件分类与编码
[12] GB/T 35625 公共安全 业务连续性管理体系 业务影响分析指南(BIA)
[13] GB/T 37228 公共安全 应急管理 突发事件响应要求
[14] GB/T 40755 公共安全 业务连续性管理体系 业务连续性管理能力评估指南
[15] 突发事件应急预案管理办法(国务院办公厅国办发〔2013〕101号)2013-10-25.
[16] 突发公共卫生事件应急条例(中华人民共和国国务院令第〔376〕号)2003-5-9.
[17] 中华人民共和国突发事件应对法(中华人民共和国主席令第〔69〕号)2007-8-30.
[18] 企业内部控制基本规范(中华人民共和国财政部财会〔2008〕7号)2008-5-22.
[19] 企业内部控制审计指引(中华人民共和国财政部财会(2010)11号)2010-4-15.
[20] 内部审计基本准则(中国内部审计协会公告2013年第1号)2013-8-20.
[21] 中央企业全面风险管理指引(国务院国有资产监督管理委员会国资发改革〔2006〕108号)2006-6-6.