



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	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 总则	2
5.1 IT 应急风险管理与 IT 应急管理的关系	2
5.2 风险管理原则	2
5.3 风险管理文化	3
5.4 风险管理策略	3
5.5 风险管理技术	3
5.6 风险管理对象	4
6 风险管理框架	4
7 顶层设计	5
7.1 战略规划	5
7.2 组织构建	6
7.3 架构设计	6
8 风险管理环境	6
8.1 内外部环境	6
8.2 促成因素	7
9 风险管理体系	7
10 风险管理要素	7
10.1 专业团队与人员	7
10.2 风险类型	8
10.3 风险管理流程	8
10.4 信息系统	8
10.5 数据	9
10.6 其他	9
11 风险管理实施	9
11.1 统筹和规划	9
11.2 构建和运行	9
11.3 监控和评价	10

11.4 改进和优化	10
附录 A (资料性) IT 应急管理总体风险	11
附录 B (资料性) IT 应急管理专项风险	14
附录 C (资料性) IT 应急风险管理组织架构与管理体系	22
附录 D (资料性) 突发公共安全事件情况下的整体应用场景	25
附录 E (资料性) 突发公共安全事件情况下的具体应用场景	31
参考文献	34

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、上海震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、杨焱、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。