

公共安全重点区域安全防范
风险管理规范

Specification for risk management of security prevention in key public safety areas

2026 - 01 - 05 发布

2026 - 02 - 05 实施

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。

本文件由合肥保安智能科技有限公司提出。

本文件由安徽省公安厅归口。

本文件起草单位：合肥保安智能科技有限公司、安徽省公安厅科技信息化总队、安徽省公安厅反恐总队、合肥市公安局治安警察支队、滁州市公安局科技信息通信科、安徽光电技术研究所、安徽建筑大学、安徽省安全技术防范行业协会、青岛利盾安保服务集团有限公司、国家石油天然气管网集团有限公司西气东输分公司合肥输气分公司。

本文件主要起草人：张敬锋、舒萍、张守宁、秦荣水、朱寅生、李继伟、黄德超、张巨、李莲英、刘丹丹、张利、何俊、于顺顺、张建、金星、吴超、余陶、高用瑞、张秀、水美蓉、丁更荣、季炎、胡旭、李少然、刘艳、胡昕韵、胡锦霞、谈建农。

公共安全重点区域安全防范风险管理规范

1 范围

本文件确立了公共安全重点区域安全防范风险管理的基本要求，并规定了公共安全重点区域安全防范风险管理的重点区域、风险类型、风险评估、风险应对和监督检查。

本文件适用于公共安全重点区域安全防范的风险管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 16571 博物馆和文物保护单位安全防范系统要求
- GB/T 23694 风险管理 术语
- GB/T 24353 风险管理 指南
- GB/T 27921 风险管理 风险评估技术
- GB 50348 安全防范工程技术标准
- GB 55029 安全防范工程通用规范
- GA 38 银行安全防范要求

3 术语和定义

GB/T 23694、GB 50348界定的术语和定义适用于本文件。

4 基本要求

- 4.1 应设立或明确安全防范风险管理部门。
- 4.2 应配备具有安全防范风险管理专业技能并经培训合格的人员。
- 4.3 应建立安全防范风险管理制度。
- 4.4 应建设满足风险管理和应急处置需要的安全防范系统。
- 4.5 应定期组织培训和演练。
- 4.6 应形成安全防范风险管理资料并存档。

5 重点区域

重点区域应包括但不限于：

- 党政机关；
- 机场、火车站、汽车站、码头、城市公交场站等重要交通枢纽；
- 大型桥梁、隧道等重要交通设施；
- 广播电台、电视台、报社、网络传媒等重要新闻单位；

- 金融、电信、邮政、寄递单位；
- 大型能源动力设施、水利设施和城市水、电、燃气、热力供应设施；
- 教育、科研、医疗单位和大型文化、体育场所；
- 博物馆、档案馆和重点文物保护单位；
- 研制、生产、销售、储存危险物品或者实验、保藏传染性菌、毒种的单位；
- 广场、公园、大型综合体等人员密集场所；
- 国家重点建设工程单位。

6 风险类型

- 6.1 公共安全重点区域安全防范风险类型分为治安风险和恐怖风险。
- 6.2 治安风险包括但不限于盗窃抢劫，刀斧砍杀，非法闯入，驾车冲撞，拥挤踩踏等。
- 6.3 恐怖风险包括但不限于爆炸，劫持，投毒，纵火，破坏等。

7 风险评估

7.1 一般规定

- 7.1.1 风险评估包括风险识别、风险分析、风险评价、风险确认、风险应对、风险更新、风险防范。评估内容应符合 GB/T 24353 的规定。
- 7.1.2 可委托有资质的第三方机构开展风险评估。

7.2 风险识别

- 7.2.1 风险识别的内容应符合 GB 50348、GB 55029 规定。
- 7.2.2 应识别风险来源，包括自然风险、人为风险、技术风险、管理风险等。
- 7.2.3 应识别风险的类型、地点、区域、时间段、可能的原因等。
- 7.2.4 应根据风险识别的结果形成风险列表。

7.3 风险分析

- 7.3.1 应对识别出的风险发生可能性和造成后果严重性进行分析。
- 7.3.2 应灵活运用定性、半定量、定量或者几种分析方法相结合的方式进行分析。分析方法应符合 GB/T 27921 规定。
- 7.3.3 采用定性分析法时，应对收集的材料进行专业分析，形成定性结果意见。
- 7.3.4 采用半定量、定量分析法时，应对收集的数据进行专业分析，形成定量结果意见。

7.4 风险评价

- 7.4.1 应根据法律、政策、标准和专家经验等预先设定风险准则。
- 7.4.2 风险准则应包括风险可能性指标和风险严重性指标。
- 7.4.3 风险发生可能性可分为几乎不可能、很小、偶尔、很可能、经常五个等级。
- 7.4.4 风险后果严重性可分为很小、小、一般、严重、非常严重五个等级。
- 7.4.5 应将风险分析结果与风险准则进行比对，确定风险等级。
- 7.4.6 风险等级按严重程度分为很高、高、中、低、很低五个等级。
- 7.4.7 法律、法规、行业或地区的风险管理已明确风险等级的，风险等级按其规定执行。

7.5 风险确认

应根据安全防范需求和标准规范要求，结合风险评价结果，将风险确认为“不可接受风险”和“可接受风险”。

7.6 评估报告

风险评估报告内容应包括但不限于编制依据、目的与适用范围、风险评估过程、风险等级分析、评估结论及风险应对措施和改进建议等，并附必要资料。

8 风险应对

8.1 风险沟通

8.1.1 应通过召开会议、编制简报、电话、通知等方式与相关方进行风险沟通。

8.1.2 宜搭建跨部门、跨区域的风险信息共享平台。

8.2 风险更新

8.2.1 应建立风险更新机制，对风险进行动态评估。

8.2.2 出现以下情况之一时，应进行风险更新：

- 相关法律法规、应急预案、标准规范发生变更，可能影响风险管理要求；
- 组织机构发生重大调整，影响风险管理范围；
- 安全防范发生具备新的风险特征的突发事件；
- 其他地区发生重大突发事件，该事件与本安全防范的风险源具备相似风险因素；
- 其它可能导致风险发生变化的情况。

8.3 风险防范

8.3.1 应根据风险确认结果，制定风险防范方案。风险防范方案应符合 GB 50348、GB 55029、GB/T 16571、GA 38 等规定。

8.3.2 应组织专家组对风险防范方案进行论证，并对风险防范方案实施情况进行评价。

8.3.3 专家组应由安全管理人员、专业技术人员组成，人数不少于 5 人，且为单数，其中专业技术人员比例应不低于 2/3。

8.3.4 风险防范方案论证和评价应符合 GB 50348、GB 55029 规定。

9 监督检查

9.1 每半年应至少开展 1 次安全防范风险管理监督检查。

9.2 重大活动举办前、突发事件处置后等特殊情况下，应开展监督检查。

9.3 监督检查人员应由安全管理人员、专业技术人员组成，其中专业技术人员比例应不低于 1/2。

9.4 应形成监督检查工作报告。