

T/BAX

团体标准

T/BAX XXXX—XXXX

安全防范风险评估通则

General rules for security prevention risk assessment

（征求意见稿）

（完成时间：）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX—XX—XX 发布

XXXX—XX—XX 实施

北京安全防范行业协会 发布

目 次

前 言 II

引 言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 基本要求 2

5 评估准备 3

6 风险识别 3

 6.1 识别内容 3

 6.2 识别方法 3

 6.3 识别结果 4

7 风险分析 4

 7.1 分析维度 4

 7.2 分析方法 4

8 风险评价 5

 8.1 评价原则 5

 8.2 评价流程 5

 8.3 评价方法 5

9 风险应对建议 5

10 评估报告编制与文档管理 5

参 考 文 献 7

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。

本文件由中国宋庆龄青少年科技文化交流中心提出。

本文件由北京安全防范行业协会归口。

本文件起草单位：。

本文件主要起草人：。

引 言

安全防范工作是维护国家稳定、社会公共安全、保护企事业单位和公民人身财产安全的重要保障，而安全防范风险评估是规范安全防范工作、防范化解安全隐患、提升安全防范效能的核心环节。当前，各类安全威胁呈现多样化、隐蔽化、智能化趋势，安全防范工作面临的形势日趋复杂，部分单位存在防范需求与专业能力不匹配、重建设轻评估、评估流程不规范、措施落实不到位等问题，导致安全隐患排查不彻底、风险管控不精准。

为贯彻落实《中华人民共和国安全生产法》《企业事业单位内部治安保卫条例》等国家法律法规及相关标准要求，规范安全防范风险评估的流程、方法和要求，细化评估内容，提升评估工作的科学性、规范性和可操作性，指导相关单位精准开展安全防范风险评估与管控，防范化解各类安全风险，保障人民群众生命财产安全、公共安全和社会稳定，特制定本文件。

本文件秉持“全链条、系统性、可度量”的理念，覆盖安全防范风险评估的全流程，明确评估组织、人员、流程、方法等具体要求，适用于各类单位的安全防范风险评估工作，为评估主体提供评价依据，推动安全防范工作从“被动应对”向“主动预防”转变，实现标准化、规范化、体系化发展。

安全防范风险评估通则

1 范围

本文件规定了安全防范风险评估的基本要求、评估准备、风险识别、风险分析、风险评价、风险应对建议和评估报告编制与文档管理等要求。

本文件适用于机关、团体、企业、事业单位开展安全防范风险评估工作（包括单位反恐怖风险评估）。

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 50348—2018 安全防范工程技术标准

GB/T 23694—2024 风险管理 术语

GB/T 27921 风险管理 风险评估技术

3 术语和定义

GB 50348、GB/T 23694界定的以及下列术语和定义适用于本文件。

3.1

安全防范 security

综合运用人力防范、实体防范、电子防范等多种手段，预防、延迟、阻止入侵、盗窃、抢劫、破坏、爆炸、暴力袭击等事件的发生。

[来源：GB 50348—2018，2.0.1]

3.2

风险 risk

保护对象自身存在的安全隐患及其所面临的可能遭受入侵、盗窃、抢劫、破坏、爆炸、暴力袭击等行为的威胁。

[来源：GB 50348—2018，2.0.20]

3.3

风险识别 risk identification

发现、确认和描述风险的过程。

[来源：GBT 23694—2024，3.3.9]

3.4

风险分析 risk analysis

理解风险性质、确定风险程度的过程。

[来源：GBT 23694—2024，3.3.15，有修改]

3.5

风险评价 risk evaluation

将风险分析结果与风险准则进行对比，以确定风险是否可以接受或容忍的过程。

[来源：GBT 23694—2024，3.3.25]

3.6

风险评估 risk assessment

风险识别、风险分析和风险评价的全过程。

[来源：GBT 23694—2024，3.3.8]

3.7

风险等级 level of risk

以后果和可能性的组合来描述的单个风险或组合风险的大小。

[来源：GBT 23694—2024，3.3.22]

3.8

防范脆弱性 vulnerability

保护对象在安全防范体系中存在的人员、制度、技术、装备、物理环境及运行管理等方面的薄弱环节或缺陷，在受到安全威胁时，可能导致防范失效、不安全事件发生或损失扩大的状态。

3.9

风险准则 risk criteria

评估评价过程中各环节的判定标尺，形成评估工作的配套基础文件。

3.10

评估工作组 assessment team

承担风险评估实施工作，开展风险识别、分析、评价及评估报告编制等活动的专业人员组成的工作小组。

3.11

风险事件 event

风险的每一种可能情景或可能情景的组合。

4 基本要求

4.1 安全防范风险评估（以下简称风险评估）应坚持客观性、规范性、系统性、动态性和可操作性原则。

4.2 评估工作应符合国家及行业相关法律法规、政策与标准规范，契合被评估单位风险管理实际需求。

4.3 单位出现下列情况时，应启动评估工作：

- a) 新建、改建、扩建的安全防范系统建设项目设计规划前；
- b) 安全态势发生明显变化时；
- c) 上级主管部门或政府相关部门提出开展评估要求时；

4.4 评估工作实施前应组建评估工作组，评估工作组成员应不少于3人，评估工作组及成员应满足以下要求：

- a) 工作组成员应具备安全防范评估相关专业知识与技术能力，熟悉相关法律法规、标准规范及评估流程方法；
- b) 工作组成员应签署保密承诺书，严格做好评估相关信息与资料的保密工作；
- c) 工作组负责人及专家应具备安全防范、保卫、应急管理及相关培训指导等相关履职能力；
- d) 工作组应与被评估单位建立有效沟通渠道；
- e) 工作组应对评估资料统一建档管理，建立资料全流程管控记录制度，并按规定做好资料留存与归档。

4.5 评估流程应包括评估准备、风险识别、风险分析、风险评价、风险应对建议和评估报告编制与文档管理等环节。

4.6 评估实施各阶段选用的方法应根据评估范围、评估时间要求、评估工作成本、应用评估技术资源能力和决策所需要的准确性等，以及 GB/T 27921 表 A2 和表 A3 用的风险评估技术方法适用性，选择评估各阶段应用的技术方法，也可多种方法交叉运用。

4.7 评估类型分为自评估和第三方专业机构评估。

5 评估准备

5.1 被评估单位应根据本单位当前安全防范工作重点，编制安全防范风险评估需求书（简称评估需求书）。明确评估目的、评估范围、评估内容和要求、计划完成时间、评估预算、预期成果和保密要求等内容。

5.2 评估工作组应根据评估需求书编制安全防范风险评估工作方案（以下简称评估方案），并经被评估单位确认。评估方案应包括但不限于：

- a) 任务背景；
 - b) 目的与范围；
 - c) 风险准则；
 - d) 流程、方法与预期成果；
 - e) 工作计划；
 - f) 评估工作组成员与职责分工；
 - g) 评估质量保障与保密措施；
 - h) 评估预计成本；
 - i) 其他。
- 5.3 被评估单位应按照评估工作组制定的评估方案配合支持各阶段评估工作，提供评估所需资料和信息。
- 5.4 评估工作组应收集评估所需的基础信息，包括但不限于：
- a) 被评估单位基本信息；
 - b) 法律法规、规章制度等相关政策文件与标准规范；
 - c) 被评估单位开展安全风险防范工作的相关资料；
 - d) 其他。

6 风险识别

6.1 识别内容

6.1.1 风险识别应包括对被保护资产识别、安全威胁识别，以及防范脆弱性识别。

6.1.2 被保护资产识别范围应包括：自然资源、基础设施、物资装备、货币票据、信息数据、敏感人物等内容。

6.1.3 安全威胁识别应围绕针对被保护资产威胁的威胁动机、威胁手段和途径、威胁能力与可能性、威胁带来的影响等方面内容进行。

6.1.4 防范脆弱性识别应以被保护资产为重点，从安全技术防范系统、安全保卫资源配置和安全管理、内部防范区域与周边社会治安环境等方面，对其安全防范的脆弱性、易损性、易露性、抗压性、措施的有效性等内容进行。

6.2 识别方法

6.2.1 被保护资产识别：在进行资产调查并获取被保护资产信息后，需要对被保护资产信息进行分析，对照资产特征，识别出重要资产，并编制重要资产识别清单。重要资产识别清单应包括资产名称以及损失/影响模式等内容。

6.2.2 安全威胁识别：对安全威胁的特征进行提取，并将收集到的安全威胁信息进行特征分析，编制安全威胁识别清单。安全威胁特征包括：背景威胁与功能威胁；与时间相关的威胁；与空间相关的威胁。

6.2.3 防范脆弱性识别：分别对与时间、空间、资产及对策相关的弱点进行识别并形成对应的识别图

表，编制防范脆弱性识别清单。

6.3 识别结果

6.3.1 根据风险准则确定识别结果。

6.3.2 确定被保护资产重要程度，出具重要资产排序表；

6.3.3 确定安全威胁事件发生程度及可能性，出具安全威胁排序表；

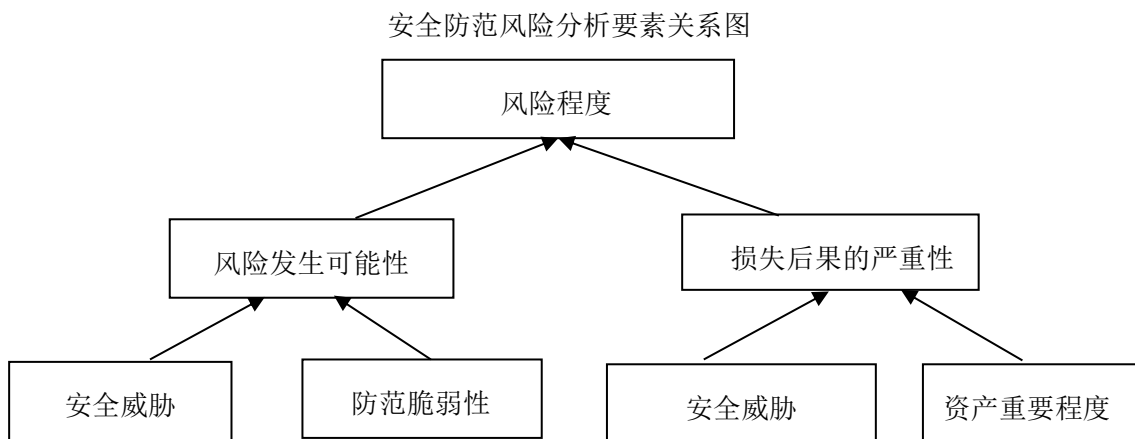
6.3.4 确定防范脆弱性程度，出具防范脆弱性排序表。

7 风险分析

7.1 分析维度

7.1.1 风险分析应对安全威胁与防范脆弱性的关系、安全威胁与资产的关系进行分析，确定风险发生的可能性和损失后果的严重性。根据风险发生的可能性和损失后果的严重性分析得出风险程度。

7.1.2 按照安全防范风险分析要素关系进行分析。示例如下：



7.2 分析方法

风险分析可采用定性、半定量、定量以及几种分析相结合的方法，常用方法如：矩阵法（更多方法参见GB/T 27921 表A2和表A3用的风险评估技术方法）。矩阵法示例如下：

风险发生可能性

风险发生可能性		防范脆弱性		
		高	中	低
安全威胁	高	高	高	中
	中	高	中	中
	低	中	中	低

损失后果的严重性

损失后果的严重性		资产重要程度		
		高	中	低
安全威胁	高	严重	较严重	一般严重
	中	较严重	一般严重	一般严重
	低	一般严重	一般严重	不严重

8 风险评价

8.1 评价原则

- 8.1.1 风险评价应在风险分析结果与风险准则相比较的基础上开展，并确定风险等级。
- 8.1.2 风险等级宜分为极高风险、较高风险、一般风险、低风险四个等级。适用单一风险和总体综合风险的风险等级确定。

8.2 评价流程

- 8.2.1 依据风险准则对每一项风险逐一进行等级评价，根据风险发生可能性和损失后果严重性确定风险程度，对照风险准则确定风险等级。
- 8.2.2 组织专家审核风险等级划分，以及确定风险是否可以接受或容忍的合理性。
- 8.2.3 将风险评价结果提交被评估单位确认。
- 8.2.4 评估过程应全程有记录，可追溯。

8.3 评价方法

应根据被评估单位的特点，参照GB/T 27921 表A2和表A3用的风险评估技术方法，灵活运用定性、半定量、定量或几种方法相结合的方式进行评估。

其中常用的矩阵法示例：

风险评价矩阵法

风险等级		损失后果严重性		
		高	中	低
风险发生可能性	高	高风险	较高风险	中风险
	中	较高风险	一般风险	一般风险
	低	一般风险	一般风险	低风险

9 风险应对建议

- 9.1 风险应对建议应遵循分级应对、预防措施为主、最小成本投入和可操作性的原则。
- 9.2 评估工作组应根据风险等级，结合被评估单位的实际能力、资源条件，逐一提出将风险水平降低至可接受风险范围的应对建议和措施。
- 9.3 提出的风险应对措施应能达到消除、降低、转移或被评估单位可接受风险的程度。
- 9.4 风险应对建议应与风险评价结果相适应，应对措施所需要投入的成本应与被保护资产重要程度相匹配。

10 评估报告编制与文档管理

10.1 安全防范风险评估报告（以下简称评估报告）内容应覆盖评估工作全过程，包括评估准备、风险识别、风险分析、风险评价、风险应对等环节。

10.2 评估报告的主要内容应包括但不限于：

- a) 前言；
- b) 被评估单位概况；
- c) 评估任务的背景、范围、目标和预期成果；
- d) 评估主要依据；
- e) 风险准则；
- f) 评估工作执行计划及实施情况；
- g) 评估结果；
- h) 风险应对建议及措施；
- i) 附件。

注：附件是评估报告的相关支撑资料，包括评估任务书、评估工作方案、安全防范风险源识别清单、安全防范风险分析表、安全防范风险评价表、问卷调查和人员访谈记录等。

10.3 评估工作组宜通过评审会形式，审查评估工作流程；评估方法；评估结果的规范性、适用性和合理性，听取被评估单位及其邀请专家的意见或建议，确定评估报告。

10.4 评估报告的信息/数据应真实、准确。

10.5 风险评估文件记录应作为风险评估报告连带的重要文件，并按照被评估单位要求进行造册保管。

10.6 风险评估过程文件资料和评估结果文件资料应独立建档，并按照评估被评估单位要求进行保管。

参 考 文 献

- [1] GB/T 31708—2015 安全防范 术语
 - [2] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
 - [3] GB/T 33170.2—2016 大型活动安全要求 第2部分：安全评估
 - [4] GB/T 24353—2022 风险管理 指南
 - [5] DB11T 1478—2017 生产经营单位安全生产风险评估规范
 - [6] DB11/T 2552—2026 单位内部安全防范通用要求
-