

DB4401

广 州 市 地 方 标 准

DB4401/T 10.30—2020

反恐怖防范管理 第 30 部分：金融机构

Anti-terrorism precaution management—

Part 30: Financial institution

2020-12-04 发布

2021-01-19 实施

广州市市场监督管理局
广州市反恐怖工作领导小组办公室

联合发布

目 次

前言.....	III
引言.....	V
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	2
4 反恐怖防范总体要求.....	2
5 防范分类及等级划分.....	2
5.1 防范分类.....	2
5.2 非常态反恐怖防范等级.....	2
6 反恐怖防范重要部位.....	2
7 常态反恐怖防范.....	2
7.1 人防.....	2
7.2 物防.....	4
7.3 技防.....	5
7.4 制度防.....	10
8 非常态反恐怖防范.....	10
8.1 非常态反恐怖防范启动.....	10
8.2 非常态反恐怖防范实施.....	10
8.3 非常态反恐怖防范措施.....	11
8.4 非常态反恐怖防范的人防、物防和技防配置.....	12
9 应急准备要求.....	12
9.1 总体要求.....	12
9.2 应急预案.....	12
9.3 应急队伍.....	12
9.4 预案演练.....	12
10 监督、检查.....	12
附录 A（规范性） 金融机构反恐怖防范工作检查实施.....	13
参考文献.....	15

前 言

本文件按 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。

本文件为 DB4401/T 10 的第 30 部分。DB4401/T 10 已经发布了以下部分：

- 第 1 部分：通则；
- 第 2 部分：党政机关；
- 第 3 部分：广电传媒；
- 第 4 部分：涉外机构；
- 第 5 部分：教育机构；
- 第 6 部分：医疗卫生机构；
- 第 7 部分：商场超市；
- 第 8 部分：酒店宾馆；
- 第 10 部分：园林公园；
- 第 18 部分：宗教活动场所；
- 第 21 部分：公交客运站场；
- 第 24 部分：城市轨道交通；
- 第 25 部分：水务系统；
- 第 26 部分：电力系统；
- 第 27 部分：燃气系统；
- 第 29 部分：粮食和物资储备仓库；
- 第 31 部分：电信互联网；
- 第 32 部分：邮政物流；
- 第 34 部分：民用爆炸物品；
- 第 35 部分：核与放射性物品。

本文件由广州市反恐怖工作领导小组办公室和广州市公安局内保支队提出。

本文件由广州市反恐怖工作领导小组办公室归口。

本文件由广州市公安局内保支队负责具体解释和实施情况收集。

本文件起草单位：广州市公安局内保支队、广州市公安局反恐怖支队、广州市标准化协会、广州计量检测技术研究院、中国人民银行广州分行、中国农业银行广州分行、万联证券股份有限公司、中国平安人寿保险股份有限公司广东分公司。

本文件主要起草人：李文中、廖俊斌、吴志强、唐小军、程胜、马果、陈淑宜、吴朝阳、林嘉欣、王昊昱、李起、戴司雄、王健、高涛、李敏、林洁芙、黄杨清。

引 言

恐怖主义是人类社会的公敌，面对恐怖主义的肆虐，无人可以独善其身。近年来，国际恐怖主义活动持续活跃，严重威胁世界和平与发展。我国将反恐怖斗争作为当前维护国家安全和社会政治稳定的重要工作，明确确立“专门工作与群众路线相结合，防范为主、惩防结合和先发制敌、保持主动”的反恐工作原则，积极构建全民参与的反恐怖防范体系，主动防范暴力恐怖袭击及其危害。在此背景下，如何建立安全、周密、可靠、有效的城市反恐怖防范标准体系，为反恐怖防范工作提供可靠的技术指导和决策支撑，成为当前反恐怖工作的重要课题和必须解决的难题。

广州作为广东省省会城市，是我国重要的中心城市、国际商贸中心和综合交通枢纽，也是华南地区的政治、经济、文化和科教中心，其不仅是我国重要的战略要地，更是我国通往世界的“南大门”，始终面临着恐怖主义的威胁，反恐怖斗争形势严峻复杂。随着全面融入“一带一路”和粤港澳大湾区建设，广州市“枢纽+”效应越加凸显，加速其对外交流与融合，也给广州城市安全反恐怖防范工作带来更多的风险与挑战。

党的十九大以来，广州全面贯彻落实习近平总书记关于新时代反恐怖工作的系列指示批示精神，深刻理解和把握总体国家安全观，坚持底线思维、问题导向、精细管理和法治精神，秉持“借力、嵌入、融合”与“共建共治共享”的社会治理理念，以建设全球最安全稳定、最公正正义、法治环境最好的国际化超大城市为总目标，以“世界一流、国内领先、广州气派”为总要求，以提升反恐重点目标反恐防范能力为主线，以“人防、物防、技防、制度防”的反恐标准为抓手，努力探索构建地方性反恐怖防范标准体系，扎实推进新时代城市安全治理体系和治理能力现代化。为此，广州市委将反恐怖地方标准体系建设作为广州市全面深化改革重点项目之一督办，广州市反恐怖工作领导小组坚持顶层设计，着力从法律法规及通用基础标准、工作标准、技术标准和管理标准等4大门类30多个方面入手，逐一研究、精心谋划、分类制定，在通则的基础上全面完成各项分则的编制工作，初步建立形成广州市反恐怖防范地方标准体系，为我市相关行业及领域落实开展反恐怖防范各项工作举措提供了系统详实先进可行的遵循和依据。

DB4401/T 10《反恐怖防范管理》原计划分为38个部分，现调整为以下33个部分。以后根据反恐怖防范工作需要，再视情况进行调整。

- 第1部分：通则。
- 第2部分：党政机关。
- 第3部分：广电传媒。
- 第4部分：涉外机构。
- 第5部分：教育机构。
- 第6部分：医疗卫生机构。
- 第7部分：商场超市。
- 第8部分：酒店宾馆。
- 第10部分：园林公园。
- 第11部分：旅游景区。
- 第12部分：城市广场和步行街。
- 第14部分：大型专业市场。
- 第15部分：体育场馆。
- 第16部分：影视剧院。
- 第17部分：会展场馆。
- 第18部分：宗教活动场所。
- 第20部分：港口码头。
- 第21部分：公交客运站场。
- 第22部分：隧道桥梁。

- 第 24 部分：城市轨道交通。
- 第 25 部分：水务系统。
- 第 26 部分：电力系统。
- 第 27 部分：燃气系统。
- 第 29 部分：粮食和物资储备仓库。
- 第 30 部分：金融机构。
- 第 31 部分：电信互联网。
- 第 32 部分：邮政物流。
- 第 33 部分：危险化学品。
- 第 34 部分：民用爆炸物品。
- 第 35 部分：核与放射性物品。
- 第 36 部分：传染病病原体。
- 第 37 部分：大型活动。
- 第 38 部分：高层建筑。

其中《反恐怖防范管理 第 1 部分：通则》的目的在于搭建系列标准的标准框架，明确了重点目标普遍适用的反恐防范要求。其余部分在通则的基础上，根据行业的特点，增加行业反恐特殊要求、细化通则的有关内容，使其更有针对性、有效性和可行性。

本文件为《反恐怖防范管理》的第 30 部分，适用于金融机构类反恐怖防范重点目标的防范工作和管理。本文件的金融机构是指依法定程序设立、经营金融业务的机构，包括银行业金融机构、证券业金融机构、保险业金融机构等，其具有现金多、票据多、人员密集、社会影响大等特点，使之易受恐怖袭击，造成重大人员伤亡和财产损失；与此同时，银行等金融机构亦是恐怖活动融资、洗钱等行为的主要渠道之一，国家明确金融机构均负有反洗钱、反恐融资义务。

本文件将金融机构的反恐怖防范重要部位根据性质及防范要求的不同分为金库类、综合办公大楼类和数据中心类；其中，对金库的定义进行了修改，将押运公司的业务库纳入了管理范围。此外本文件根据目前银行营业网点的实际情况及业务发展趋势，针对个人防护装备、公共防护设施、出入口控制系统、安全检查及探测系统等几方面强化了要求。在信息安全方面，对银行、证券、保险等金融机构涉及国计民生的核心系统，将信息安全等级提升到第四级结构化保护级；针对《中华人民共和国反恐怖主义法》中金融机构涉恐融资信息报送要求，对金融机构建立涉恐信息报送、保密制度作出要求，同时细化了报送时效、原则。

反恐怖防范管理 第30部分：金融机构

1 范围

本文件规定了金融机构反恐怖防范管理的术语和定义、反恐怖防范总体要求、防范分类及等级划分、反恐怖防范重要部位、常态反恐怖防范、非常态反恐怖防范、应急准备要求和监督、检查。

本文件适用于金融机构类反恐怖防范重点目标的防范工作和管理，金融机构类反恐怖防范一般目标可参照执行。

注：反恐怖防范重点目标由公安机关会同有关部门确定。

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 10408.1 入侵探测器 第1部分：通用要求
- GB 10408.3 入侵探测器 第3部分：室内用微波多普勒探测器
- GB 10408.4 入侵探测器 第4部分：主动红外入侵探测器
- GB 10408.5 入侵探测器 第5部分：室内用被动红外探测器
- GB 10408.6 微波和被动红外复合入侵探测器
- GB/T 10408.8 振动入侵探测器
- GB 12663 入侵和紧急报警系统 控制指示设备
- GB 12899 手持式金属探测器通用技术规范
- GB 15208.1 微剂量 X 射线安全检查设备 第1部分：通用技术要求
- GB 15209 磁开关入侵探测器
- GB 15210 通过式金属探测门通用技术规范
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 22240 信息安全技术 网络安全等级保护定级指南
- GB/T 25724 公共安全视频监控数字视音频编解码技术要求
- GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求
- GB/T 32581 入侵和紧急报警系统技术要求
- GB/T 37078 出入口控制系统技术要求
- GB 50198 民用闭路监视电视系统工程技术规范
- GB 50348 安全防范工程技术标准
- GB 50394 入侵报警系统工程设计规范
- GB 50395 视频安防监控系统工程设计规范
- GB 50396 出入口控制系统工程设计规范
- GA 38 银行营业场所安全防范要求
- GA/T 72 楼宇对讲电控安全门通用技术条件
- GA/T 367 视频安防监控系统技术要求
- GA/T 394 出入口控制系统技术要求
- GA/T 501 银行保管箱
- GA/T 644 电子巡查系统技术要求
- GA/T 669.1 城市监控报警联网系统技术标准 第1部分：通用技术要求
- GA/T 678 联网型可视对讲系统技术要求
- GA 858 银行业务库安全防范的要求

GA/T 1127—2013 安全防范视频监控摄像机通用技术要求
DB4401/T 10.1—2018 反恐怖防范管理 第1部分：通则
DB4401/T 43 反恐怖防范管理 防冲撞设施

3 术语和定义

DB4401/T 10.1—2018 和 GA 38 界定的以及下列术语和定义适用于本文件。

3.1

金融机构 financial institution

依法定程序设立、经营金融业务的机构，包括银行业金融机构、证券业金融机构、保险业金融机构等。

3.2

金库 vaults

中央银行货币发行库、商业银行的业务库、为金融机构提供金融业务服务的业务库。

4 反恐怖防范总体要求

4.1 金融机构的反恐怖防范应坚持“属地负责，逐级监管”“谁主管，谁负责”“谁经营，谁负责”的工作原则。

4.2 金融机构的反恐怖防范工作应在反恐怖主义工作领导小组统一领导和指挥下开展，公安机关、金融机构主管（监管）部门（简称行业主管部门）履行安全管理、指导、监督和检查责任。

4.3 金融机构是反恐怖防范的责任主体，应按照反恐怖主义法等相关要求履行职责，建立并实施金融机构反恐怖防范系统。

5 防范分类及等级划分

5.1 防范分类

反恐怖防范按防范管理性质分为常态反恐怖防范和非常态反恐怖防范两类。

5.2 非常态反恐怖防范等级

非常态反恐怖防范等级按恐怖威胁预警响应的要求分为4个等级：

- a) 四级非常态反恐怖防范，Ⅳ级（一般），用蓝色表示；
- b) 三级非常态反恐怖防范，Ⅲ级（较大），用黄色表示；
- c) 二级非常态反恐怖防范，Ⅱ级（重大），用橙色表示；
- d) 一级非常态反恐怖防范，Ⅰ级（特别重大），用红色表示。

6 反恐怖防范重要部位

金融机构的反恐怖防范重要部位应符合 DB4401/T 10.1—2018 中第6章的要求，可分为以下几类：

- a) 金库重要部位，包括但不限于与外界相连的出入口、守库室、出入库通道、出入库交接场地、票币清分场地、金库库体、供电房、安防监控中心、周界；
- b) 综合办公大楼重要部位，包括但不限于主要出入口、服务大厅、现金服务区、现金交接区域、现金清分场所、保管箱库、档案库、供电房、安防监控中心、贵金属展示区、银行自助设备处；
- c) 数据中心、清算中心重要部位，包括但不限于出入口、机房、供电房、监控室、通风系统。

7 常态反恐怖防范

7.1 人防

7.1.1 基本要求

7.1.1.1 应符合国家、省、市的相关法律法规、规章及有关标准对安保力量的要求。

7.1.1.2 金融机构应根据有关规定，结合单位工作性质及地理位置、单位面积、工作人员数量、重要部位分布等反恐怖防范工作实际需要，合理设置安保岗位和配备足够的安保力量。

注：安保力量指专职保卫干部、保安员、押运员及其他安保工作人员。

7.1.2 人防组织

7.1.2.1 金融机构应设置或确定承担与反恐怖防范任务相适应的反恐怖防范工作机构，明确第一责任人和责任部门，指定联络员，配备专职工作人员，负责反恐怖防范的具体工作。

7.1.2.2 金融机构应明确金融机构反恐怖防范重要岗位，重要岗位主要包括：金融机构主要负责人、金融机构安保部门责任领导、联络员、技防岗位、网管岗位、安保岗位等。

注：上述岗位工作人员即为重要岗位人员。

7.1.3 人防配置

7.1.3.1 金融机构反恐怖防范应按照表1的规定进行人防配置。

表1 人防配置表

序号	项目	配设要求	设置标准	
1	工作机构	健全组织、明确分工、落实责任	应设	
2	责任领导	主要负责人为第一责任人	应设	
3	责任部门	安保部门兼任或独立设置	应设	
4	专职联络员	指定金融机构保卫部门负责人1名	应设	
5	安保力量	技防岗位	重要技防设施	应设
6		固定岗位	与外界相连的出入口、守库室、主要出入口、安防监控中心	应设
7		巡查岗位	出入口、守库室、金库库体外围、供电房、安防监控中心、网络机房、服务大厅、现金清分场所、保管箱库、档案库、贵金属展示区、银行自助设备处、通风系统、周界等	应设
8		网管岗位	机房、网络安全维护	应设
9		机动岗位	备勤	应设

7.1.3.2 金融机构的反恐怖防范常态安保力量应按以下原则进行配备：

- 守库室、主要出入口配备的安保力量不少于1人；
- 安防监控中心配备的安保力量不少于2人，视频监控系统的值班监看人员配备宜与监看显示画面数量相适应；
- 巡查时每班配备的安保力量不少于2人。

7.1.3.3 金融机构配备安保力量除符合表1的要求外，还应符合如下要求：

- 重点目标总人数200人（含本数）以下的，专职保卫干部不少于1人，安保力量不少于单位人员总数5%；
- 200人以上500人（含本数）以下的，专职保卫干部不少于2人，安保力量不少于单位人员总数5%；
- 500人以上2000人（含本数）以下的，专职保卫干部不少于3人，安保力量不少于单位人员总数5%；
- 2000人以上的，专职保卫干部不少于4人，安保力量不少于单位人员总数的4%。

注：专职保卫干部指负责本重点目标反恐安全保卫工作的保卫干部。

7.1.4 人防管理

7.1.4.1 金融机构应建立与反恐怖主义工作领导机构、公安机关的工作联系，定期报告反恐怖防范措施落实情况，互通信息、完善措施。发现可疑人员、事件、违禁和管制物品及违法犯罪行为应及时制止，并报行业主管部门同时报告公安机关，同时采取措施保护现场。

7.1.4.2 金融机构应加强人防管理，按DB4401/T 10.1—2018中7.1.4.2的要求执行：

- a) 金融机构负责领导、责任部门负责人应签订反恐怖防范目标责任书，重要岗位的从业人应签订相应的反恐怖防范承诺书；
- b) 开展重要岗位人员背景审查，建立人员档案，并向公安机关备案，确保用人安全；
- c) 加强反恐怖防范教育宣传，在人员活动密集场所张贴有关维护秩序的法律法规和文件，悬挂加强金融机构安全防范工作宣传标语，提高工作人员安全防范意识；
- d) 金库类金融机构应加强出入口来访人员管理，核对、查验、登记来访人员、车辆信息，必要时对来访人员进行安全检查及身份核验；
- e) 应确保外部人员访问重要部位前得到授权和审批，限制和监控其活动范围，并登记在案。

7.1.4.3 金融机构应指定专职联络员，联络员应确保 24 小时通信畅通；联络员的配置和变更，应及时向管辖的公安机关和反恐怖主义工作领导机构的办事机构备案。

7.1.5 安保力量要求

反恐怖安保力量应符合 DB4401/T 10.1—2018 中 7.1.5 的要求，并应符合以下要求：

- a) 应掌握重要部位的地理环境和主要设施布局，熟悉周边环境和各类疏散途径；
- b) 积极应对金融机构相关涉恐突发事件，协助、配合反恐怖主义工作领导机构、公安机关和行业主管部门开展应急处置工作；
- c) 安保负责人应熟悉反恐怖防范工作情况及相关规章制度、职责及分工、涉及的应急预案等。

7.2 物防

7.2.1 基本要求

7.2.1.1 应符合国家、省、市的相关法律法规、规章及有关标准对工程建设的要求。

7.2.1.2 应纳入重点目标工程建设规划，新建、改建和扩建项目应与主体工程同步设计、同步建设、同步运行。

7.2.1.3 使用的设备和设施应符合相关标准要求，并经检验或认证合格。

7.2.2 物防组成

重点目标物防包括实体防护设施、个人应急防护装备、公共应急防护装备等。

7.2.3 物防配置

金融机构反恐怖防范重要部位应按照表 2 的规定进行物防配置。

表 2 物防配置表

序号	项目	安放区域或位置			设置标准
		金库	综合性办公大楼	数据中心、清算中心	
1	机动车阻挡装置	出入口	出入口	出入口	应设
2	防机动车冲撞或隔离设施	出入口	出入口	出入口	应设
3	金库门	金库	金库、保管箱库	—	应设
4	防盗安全门、金属防护门或防尾随联动互锁安全门	出入库交接场地、票币清分场地、安防监控中心、供电房、档案库	安防监控中心、现金清分场所、供电房、整体式保管箱库、档案库	网络机房、供电房	应设
5	防盗保险柜（箱）	档案库	保管箱库、档案库	—	应设
6	透明防护屏障	—	现金服务区	—	应设
7	人车分离通道	—	出入口	—	应设

表2 物防配置表（续）

序号	项目	安放区域或位置			设置标准	
		金库	综合性办公大楼	数据中心、清算中心		
8	个人 应急防 护装备	对讲机、强光手电、防暴棍棒	守库室、安防监控中心、消控中心	门卫室、值班室、安防监控中心、消控中心	门卫室、值班室、安防监控中心、消控中心	应设
9		毛巾、口罩	各工作区域	各工作区域	各工作区域	应设
10		防毒面罩或防烟面罩	各工作区域	各工作区域	各工作区域	应设
11		防暴盾牌、钢叉	守库室、安防监控中心、消控中心	门卫室、值班室、安防监控中心、消控中心	门卫室、值班室、安防监控中心、消控中心	应设
12		防暴头盔、防割（防刺）手套、防刺服	守库室、安防监控中心、消控中心	门卫室、值班室、安防监控中心、消控中心	门卫室、值班室、安防监控中心、消控中心	应设
13		防弹背心	守库室	—	—	应设
14	公共应 急防护 装备及 设施	防爆桶、防爆毯（含防爆围栏）	门卫室	门卫室	—	应设
15		应急警报器	守库室、安防监控中心	现金业务区、安防监控中心	安防监控中心	应设
16		灭火器材	各工作区域	各工作区域	各工作区域	应设

7.2.4 物防要求

7.2.4.1 防护设备设施要求

7.2.4.1.1 物防应符合 DB4401/T 10.1—2018 中 7.2.4.1 的要求。

7.2.4.1.2 金融机构设有业务库、保管箱库的应符合 GA 858、GA/T 501 的规定。

7.2.4.1.3 金融机构的安防监控中心、安防设备间应设置存放图像（备份）信息硬盘的安防数据防护柜。安防数据防护柜应具有防火、防盗、防磁性能，其技术要求应符合相关规定。

7.2.4.2 防冲撞设施

防冲撞设施的技术要求应符合 DB4401/T 43 的规定。

7.2.4.3 防护设备设施采购与维护

防护设备设施采购与维护应符合 DB4401/T 10.1—2018 中 7.2.4.2 的要求。

7.3 技防

7.3.1 基本要求

7.3.1.1 应符合国家、省、市的法律法规、规章及有关技术标准对工程建设的要求。

7.3.1.2 应纳入重点目标工程建设规划，新建、改建和扩建项目应与主体工程同步设计、同步建设、同步运行。

7.3.1.3 使用的设备设施应符合相关技术标准的要求，并经检验或认证合格。

7.3.2 技防组成

金融机构技防包括安防监控中心、电子防护系统、公共广播系统、无线通信对讲指挥调度系统、通讯显示记录系统、信息隔离控制系统（防火墙）等，其中电子防护系统包括视频监控系统、入侵和紧急报警系统、出入口控制系统、停车库（场）管理系统、电子巡查系统（巡更系统）、安全检查及探测系统等。

7.3.3 技防配置

金融机构反恐怖防范重点部位应按照表 3 的规定配置技防系统。

表3 技防配置表

序号	项目	安装区域或覆盖范围			设置标准	
		金库	综合性办公大楼	数据中心、清算中心		
1	安防监控中心	重点目标内部	重点目标内部	重点目标内部	应设	
2	视频监控系统	摄像机	主要出入口、周界	主要出入口、服务大厅	主要出入口	应设
3			主要通道、电梯轿厢	主要通道、电梯轿厢	主要通道、电梯轿厢	应设
4			供电房、网络机房、库房内、出入库通道、守库室、票币清分场地、出入库交接场地、地下回廊	供电房、网络机房、楼顶	供电房、网络机房、通风系统	应设
5			停车库（场）及其主要通道和主要出入口	停车库（场）及其主要通道和主要出入口	停车库（场）及其主要通道和主要出入口	应设
6			安防监控中心	安防监控中心	安防监控中心	应设
7			—	现金服务区、业务办理区	—	应设
8			声音复核装置	库房内、守库室、安防监控中心、票币清分场地、出入库交接场地	现金服务区、业务办理区、银行自助设备	—
9		主要出入口		主要出入口	主要出入口	宜设
10		视频智能分析系统	安防监控中心	安防监控中心	安防监控中心	宜设
11		人脸图像识别系统	主要出入口、安防监控中心	主要出入口、安防监控中心、银行自助设备	出入口、安防监控中心	应设
12		机动车号牌自动识别系统	停车库（场）、主要出入口	停车库（场）、主要出入口	停车库（场）、主要出入口	应设
13		控制、记录、显示装置	安防监控中心	安防监控中心	安防监控中心	应设
14		入侵和紧急报警系统	入侵探测（报警）器	金库库体、周界	保险柜库、档案库（室）	网络机房
15	紧急报警装置		守库室	现金服务区	—	应设
16	（一键报警）		安防监控中心	安防监控中心	安防监控中心	应设
17	报警控制器		安防监控中心、守库室	安防监控中心	安防监控中心	应设
18	终端图形显示装置	安防监控中心	安防监控中心	安防监控中心	应设	
19	出入口控制系统	门禁系统	各工作区域	—	—	应设
20			—	网络机房	网络机房	应设
21			—	档案库、库房、保险柜库	—	应设
22		生物识别系统	安防监控中心、主要出入口	安防监控中心、现金服务区	安防监控中心	宜设
23		来访人员登记系统（与公安机关联网）	—	出入口	—	应设
24	停车库（场）管理系统	停车库（场）	停车库（场）	—	应设	
25	电子巡查系统（巡更系统）	周界	—	周界	应设	
26		办公楼内各楼层	—	办公楼内各楼层	应设	
27		出入口、守库室、金库库体外围、供电房、安防监控中心、网络机房、通风系统等	重要部位	重要部位	应设	
		公共广播系统	区域全覆盖	区域全覆盖	区域全覆盖	应设
28	无线通信对讲指挥调度系统	区域全覆盖、安防监控中心	区域全覆盖、安防监控中心	区域全覆盖、安防监控中心	应设	
29						

表3 技防配置表（续）

序号	项目		安装区域或覆盖范围			设置标准
			银行金库	综合性办公大楼	数据中心、清算中心	
30	安全检查及探测系统	微剂量X射线安全检查装置	主要出入口	—	—	宜设
31		通过式金属探测门	主要出入口	—	—	宜设
32		手持式金属探测器	主要出入口	主要出入口	主要出入口	应设
33		爆炸物探测仪	—	主要出入口	—	宜设
34			主要出入口	—	—	应设
35	通讯显示记录系统	—	服务、咨询电话、总机	—	应设	
36	信息隔离控制系统（防火墙）	网络通讯控制区域	网络通讯控制区域	网络机房	应设	

7.3.4 技防要求

7.3.4.1 技防系统总体要求

金融机构的反恐怖防范技防系统总体要求，应满足以下要求：

- 系统应符合 DB4401/T 10.1—2018 中 7.3.4 对技防要求；
- 系统应满足 GB 50348 中技防设备设施的相关规定；
- 金库的安全防范应符合 GA 858 的相关要求；
- 金融机构应符合 GB/T 22239—2019 和 GB/T 22240 中相应规定，银行、证券、保险业金融机构的核心业务系统其技术要求应至少符合 GB/T 22239—2019 中第四级安全防护的相关规定，网上银行、重要支撑系统、在线服务系统应至少符合第三级安全防护的相关规定。

7.3.4.2 安防监控中心

安防监控中心应符合以下要求：

- 视频安防监控、入侵报警、电子巡查的终端设备，以及出入口控制系统的报警信号输出终端均应设置在安防监控中心，应能实现对各子系统的操作、记录和显示；
- 安防监控中心配置的与报警同步的终端图形显示装置，应能准确地指示报警区域，实时声、光提示发生警情的区域、日期、时间等信息，并应配备有线、无线专用通讯工具，以及专用防护器械和消防设备；
- 安防监控中心的视频安防监控系统、入侵报警系统、出入口控制系统的终端接口及通信协议应符合国家现行有关标准规定，可与上一级管理系统联网。

7.3.4.3 视频监控系统

7.3.4.3.1 系统要求

视频监控系统应符合以下要求。

- 视频监控系统应具有对图像信号的采集、传输、切换控制、显示、分配、记录和重放等基本功能，视频监控系统的要求应同时满足 GB 50198、GB 50395、GA/T 367、GA/T 669.1 的要求。
- 视频监控系统应采用数字系统。
- 图像信号的采集使用的摄像机应符合 GA/T 1127—2013 的要求，与外界相通的出入口配置的摄像机应满足 C 类以上高清晰度，其他重要部位配置的摄像机应满足 B 类以上高清晰度。
- 宜支持 H.264、H.265 或 MPEG-4 视频编码格式和文件格式进行图像存储，宜支持 G.711、G.723.1、G.729 等音频编解码标准实现音频同步存储。新建、改建、扩建的视频监控系统音视频编解码宜优先采用 GB/T 25724 规定的 SVAC 编码方式。
- 图像信号的传输、交换和控制应符合 GB/T 28181 的要求。

- f) 图像信号的切换应具有手动和编程两种模式。
- g) 图像信号的显示设备应采用 FHD (1920×1080) 以上分辨率的大屏设备, 当系统配备的超高清摄像机 (GA/T 1127—2013 的 D 类) 时, 宜采用 4K (4096×2160) 以上分辨率的大屏设备。
- h) 图像信号的存储:
 - 1) 外界相通的出入口的单路图像应具有 16CIF (1920×1080) 或以上图像分辨率;
 - 2) 非直接与外界相通的重要部位单路图像应具有 9CIF (1280×720) 或以上图像分辨率;
 - 3) 单路显示基本帧率不小于 25 fps;
 - 4) 存储时间不小于 90 天。
- i) 视频安防监控系统应安装视频安防监控数据导出防泄密系统。

7.3.4.3.2 摄像机

摄像机应符合以下要求。

- a) 摄像机安装应减少或避免图像出现逆光, 且摄像机工作时监视范围内的平均照度宜不小于 200 lx。
- b) 出入口、与出入口相连的通道摄像机安装应符合以下要求:
 - 1) 出入方向上, 具有正反向两组摄像机;
 - 2) 监视区域内不应有盲区;
 - 3) 通过监视屏应 24 小时均能清楚地辨别出入人员面部特征、机动车牌号;
 - 4) 显示的人员正面面部有效画面宜不小于监视屏显示画面的 1/60;
 - 5) 摄像机安装支架应稳定、牢固, 安装位置应不易受外界干扰、破坏;
 - 6) 固定摄像机的安装指向与监控目标形成的垂直夹角宜 $<30^{\circ}$, 与监控目标形成的水平夹角宜 $<45^{\circ}$ 。
- c) 金融机构公共区域宜安装带有云台、变焦镜头的摄像机, 通过监视屏应能清楚地显示人员的活动情况。
- d) 带有云台、变焦镜头的摄像机在云台、变焦停止操作后, 摄像机应在 (2±0.5) 分钟内自动复位至初始设定状态。

7.3.4.4 入侵和紧急报警系统

7.3.4.4.1 入侵和紧急报警系统应符合以下要求:

- a) 入侵和紧急报警系统应符合 GB 12663、GB/T 32581、GB 50394 等入侵和紧急报警系统相关标准的要求;
- b) 应按需要选择、安装入侵探测器, 防区内不应有盲区;
- c) 防区划分应有利于报警时准确定位, 周界封闭屏障防区间距应不大于 50 m;
- d) 周界报警系统应 24 小时设防;
- e) 紧急报警装置应安装在隐蔽、便于操作的部位, 并应设置为不可撤防模式, 且应有防误触发措施; 当被触发报警后应能立即发出紧急报警信号并自锁, 复位应采用人工操作方式;
- f) 除周界封闭屏障处以外, 无人看守的场所安装入侵探测器的部位均应安装声光告警器, 其报警声压不小于 80 dB (A), 报警持续时间不少于 5 分钟;
- g) 独立设防区域的入侵和紧急报警系统应与配置专职值守人员的安防中心控制室联网; 安防中心控制室应安装与区域报警中心联网的紧急报警装置; 系统使用专用电缆传输报警信号时报警响应时间应不大于 3 秒; 使用公共电话网络传输时报警响应时间应不大于 20 秒;
- h) 以公共电话网络作为报警传输专线时, 不应在线路上挂接其他通信设施;
- i) 系统应具有时间、日期的显示、记录和调整功能, 时间误差应在±30 秒以内;
- j) 系统布防、撤防、报警、故障等信息的存储时间应不少于 180 天, 并能输出打印;
- k) 系统的备用电源应满足 24 小时正常工作;
- l) 宜配备图片复核及视频复核功能;
- m) 入侵和紧急报警系统应能与视频安防监控系统、人脸图像识别系统、声音复核装置、出入口控制系统等联动使用。

7.3.4.4.2 入侵探测器应符合 GB 10408.1、GB 10408.3、GB 10408.4、GB 10408.5、GB 10408.6、GB/T 10408.8、GB 15209 的要求。

7.3.4.5 出入口控制系统

7.3.4.5.1 识读式出入口控制系统应符合以下要求：

- a) 识读装置安装应安全、牢固，安装高度宜离地 1400 mm±100 mm；
- b) 出入口控制器应设置在受控门以内；
- c) 系统应有备用电源，并能在市电断电后保证该子系统正常运行时间不少于 48 小时；当供电不正常、断电时，系统的密钥（钥匙）信息及各记录信息不得丢失；
- d) 系统应满足紧急逃生时人员疏散的相关要求；当通向疏散通道方向为防护面时，系统应与火灾报警及其他紧急疏散系统联动，当发生火警或需紧急疏散时，人员不使用钥匙应能迅速安全通过；
- e) 重要部位的出入口控制装置应能与视频安防监控系统联动。

7.3.4.5.2 银行自助设备的加钞间应设置出入口控制设备。

7.3.4.5.3 银行自助设备与外界相通的出入口应安装具备远程控制功能的电子锁具，其出入口门体安装的闭门器（包括地弹簧）应确保门体在开启任意角度时都能复位至关闭状态。

7.3.4.5.4 各类识别装置、执行机构应保证操作性和可靠性。系统应根据安全防范管理的需要，按不同的通行对象及其准入级别进行控制与管理。对非法进入的行为或连续 3 次不正确的识读，系统应发出报警信号。安防中心控制室的声光报警应保持至人工操作复位。

7.3.4.5.5 系统应具有人员的出入时间、地点、顺序等数据的设置，以及显示、记录、查询和打印等功能，并有防篡改、防销毁等措施。

7.3.4.5.6 系统时间与标准时间的误差应在±10 秒内，系统数据资料保存时间应不少于 180 天。

7.3.4.5.7 金融机构营业场所、集中式数据中心、远程安防监控中心、离行式银行自助设备及自助保管箱库等安装组合认证出入口控制系统的，其技术要求应符合相关规定。

7.3.4.5.8 出入口控制系统的其他要求应符合 GB/T 37078、GB 50396、GA/T 72、GA/T 394、GA/T 678 的有关规定。

7.3.4.6 电子巡查系统

7.3.4.6.1 电子巡查系统设置应符合以下要求：

- a) 在重要部位及巡查路线上设置巡查点，巡查钮或读卡器安装应牢固、隐蔽，高度宜离地 1400 mm±100 mm；
- b) 巡查路线、时间应根据需要进行设定和修改；
- c) 应能通过电脑查阅各巡查人员的到位时间，应具有对巡查时间、地点、人员和顺序等数据的显示、归档、查询和打印等功能；
- d) 应具有巡查违规记录提示。

7.3.4.6.2 宜采用在线式电子巡查系统。采用非在线式电子巡查系统的，采集器数量配置数应大于 2 个，且应为巡查人员配备无线即时通讯工具，确保其在每个巡查点位能够与安防中心控制室保持实时通讯联络。

7.3.4.6.3 系统数据资料保存时间应大于 30 天。

7.3.4.6.4 电子巡查系统的其他要求应符合 GA/T 644 的有关规定。

7.3.4.7 声音复核装置/远程对讲装置

7.3.4.7.1 声音复核装置，在营业时间内应与视频图像信号同步记录。声音记录应能清晰辨别监听区域以及营业员与客户的对话内容。

7.3.4.7.2 声音复核装置应能清晰连续记录交易过程的对话内容，清晰探测撬、挖、凿、锯等动作发出的声音。

7.3.4.7.3 声音复核资料保存时间应与相关区域视频图像资料的保存时间保持一致。

7.3.4.7.4 远程对讲装置应采用全双工模式，音质应清晰可辨。

7.3.4.8 通讯显示记录系统

7.3.4.8.1 来电号码显示应清晰。

7.3.4.8.2 电话记录回放时应清晰可辨，通话记录保存时间应大于或等于 30 天。

7.3.4.9 安全检查系统

7.3.4.9.1 手持式金属探测器的技术要求应符合 GB 12899 的规定。

7.3.4.9.2 通过式金属探测系统的技术要求应符合 GB 15210 的规定。

7.3.4.9.3 X 射线安全检查设备的技术要求应符合 GB 15208.1 的规定。

7.3.5 系统检验与验收

系统验收前应进行检验，系统检验和验收应符合法律、法规、行业有关技术标准及公安机关的相关要求。

7.3.6 运行维护及保养

运行维护及保养按 DB4401/T 10.1—2018 中 7.3.6 要求进行。

7.4 制度防

7.4.1 一般要求

制度防建设应符合 DB4401/T 10.1—2018 中 7.4 的要求，制度防组成包括管理标准、工作标准和技术标准。

7.4.2 制度防配置

金融机构制度防配置除应符合 DB4401/T 10.1—2018 中 7.4.3 要求外，还应符合表 4 的要求。

表 4 制度防配置表

序号	项目	配设要求	设置标准
1	信息报送制度	发现的疑似涉恐信息应立即主动报送公安机关	应设
2	涉恐信息保密制度	保障相关涉恐信息不外泄	应设
3	管理标准 线索快速反应制度	按“涉恐线索立即处理，重案要案线索当天处理，专项行动线索优先处理”的原则由本地区人民银行牵头，各金融机构主动监控并定期上报可疑资金、可疑人群信息，并根据公安机关的特殊要求，调整相关监控要求	应设
4	现金等高价值物资押送管理制度	应制定包括人员职责、工作流程等内容的管理要求	应设
5	押运车管理制度	应制定包括车辆检查、押运路线、应急处理等内容的管理要求	应设

8 非常态反恐怖防范

8.1 非常态反恐怖防范启动

8.1.1 根据反恐怖主义工作领导小组、公安机关发布的恐怖威胁预警，进入非常态反恐怖防范。

8.1.2 金融机构可根据实际工作需要进入非常态反恐怖防范，并向反恐怖主义工作领导小组和行业主管部门报告。

8.2 非常态反恐怖防范实施

金融机构应积极响应恐怖威胁预警要求，采取的非常态反恐怖防范等级应不低于有关部门或机构发布的恐怖威胁预警等级。

非常态反恐怖防范等级和恐怖威胁预警等级对应关系见表 5。

表5 非常态反恐怖防范等级和恐怖威胁预警等级对应关系表

非常态反恐怖防范等级	恐怖威胁预警等级	恐怖威胁预警颜色
四级（IV）	四级（IV）	蓝色
三级（III）	三级（III）	黄色
二级（II）	二级（II）	橙色
一级（I）	一级（I）	红色

8.3 非常态反恐怖防范措施

8.3.1 四级非常态反恐怖防范

应在符合常态反恐怖防范的基础上，同时采取以下工作措施：

- a) 启动反恐怖应急指挥部，各类防范、处置装备设施处于待命状态；
- b) 金融机构保卫部门负责人带班组织防范工作；
- c) 在常态安保力量的基础上增派 50%以上；
- d) 严格执行各项管理制度，检查物防、技防设施；
- e) 禁止非本单位工作人员进出；
- f) 主要出入口设置障碍，严禁外部车辆进入；
- g) 联系属地公安机关和行业主管部门指导防范工作；
- h) 每日主动向属地公安机关和行业主管部门报告防范工作落实情况，重要情况应随时报告；
- i) 配合反恐怖主义工作领导机构及其办事机构、公安机关开展工作；
- j) 根据反恐怖主义工作领导机构及其办事机构、公安机关要求采取的其他防范措施。

8.3.2 三级非常态反恐怖防范

应在符合四级非常态反恐怖防范的基础上，同时采取以下工作措施：

- a) 金融机构分管领导带班组织防范工作；
- b) 在常态安保力量的基础上增派 70%以上；
- c) 对区域内人员、车辆、物品进行安全检查；
- d) 外来物品禁止进入重点目标；
- e) 每半日主动向属地公安机关报告防范工作落实情况，重要情况应时报告；
- f) 联系属地公安机关和行业主管部门派员指导防范工作。

8.3.3 二级非常态反恐怖防范

应在符合三级非常态反恐怖防范的基础上，同时采取以下工作措施：

- a) 金融机构主要领导及分管领导共同带班组织防范工作；
- b) 在常态安保力量的基础上增派 100%以上；
- c) 重要部位巡视频率较常态提高 1 倍；出入口派员加强值守；
- d) 联系属地公安机关和行业主管部门派员参与反恐怖防范工作。

8.3.4 一级非常态反恐怖防范

应在符合二级非常态反恐怖防范的基础上，同时采取以下工作措施：

- a) 金融机构主要领导、分管领导及领导班子其他成员共同带班组织防范工作；
- b) 装备、力量、保障进入临战状态；
- c) 重要部位应有 2 名以上安保人员守护，实行 24 小时不间断巡查；
- d) 对无关工作人员进行疏散，必要时转移重要信息、物资；
- e) 封闭出入口，严密监视内外动态；
- f) 对目标区域进行全面、细致检查；
- g) 对相关要害部位、设施、场所实施现场管控，必要时暂停相关业务。

8.4 非常态反恐怖防范的人防、物防和技防配置

金融机构应有机制确保符合启动非常态反恐怖防范时人防、物防和技防配置的要求，确保增派的安保力量、物防设备设施和技防系统能及时到位。

9 应急准备要求

9.1 总体要求

9.1.1 应符合 DB4401/T 10.1—2018 中第 9 章相关规定。

9.1.2 金融机构应针对恐怖事件的规律、特点和可能造成的社会危害，分级分类制定并实施应急预案，应对可能遭受的恐怖袭击或危害的紧急情况，并对本单位的应急准备和应急能力进行评估。

9.1.3 金融机构应明确应急准备工作的责任部门，明确相关人员职责。

9.2 应急预案

应符合 DB4401/T 10.1—2018 中 9.2 的要求。

9.3 应急队伍

应组建具有组织人员疏散、保护重要部位、控制损失和准确反馈现场情况等能力的应急作战队伍。应急作战队伍由安保力量组成，应包括以下几部分：指挥组、警戒组、疏散组、处置组、救护组、通讯组等。

9.4 预案演练

9.4.1 金融机构应根据实际情况，因地制宜，按应急预案要求开展应急演练。

9.4.2 金融机构应每半年组织 1 次反恐应急综合演练。重点加强重要岗位人员的培训和实操演练，确保重要岗位人员熟练掌握各类应急业务技能，保证安全、有序、可控。

10 监督、检查

10.1 应符合 DB4401/T 10.1—2018 第 10 章的要求。

10.2 公安机关、行业主管部门适时开展的部门检查、反恐怖主义工作领导机构的办事机构开展的督导检查，开展安全检查或开展重点项目抽查（重点项目抽查见附录 A）。

附录 A
(规范性)
金融机构反恐怖防范工作检查实施

A.1 概述

金融机构反恐怖防范工作的检查实施按 DB4401/T 10.1—2018 的附录 C 规定进行。

A.2 检查表格

检查表格应包括依据的标准条款，检查内容概要，检查过程记录和项目结论。格式见表 A.1。

表 A.1 重点项目检查表格

序号	标准条款	内容概要	检查记录	项目结论	
1	7.1.3	是否按实际需要配备了技防岗位、固定岗位、巡查岗位、网管岗位和机动岗位等安保力量			
2	7.1.4.1	与反恐怖主义工作领导机构、公安机关及金融机构主管部门的工作联系途径是否有效			
3	7.1 人 防	是否对重要岗位人员开展背景审查，查看审查记录			
4		是否建立重要岗位人员档案并备案，查看档案资料			
5		是否对出入口人员、车辆进行登记检查，检查记录			
6		是否按有效的路径和方式开展巡查，检查记录			
7		是否在正确的位置正确使用安检设备开展安检工作			
8		7.1.4.2	视频监控系统的值班监看是否到位		
9		检查教育培训计划和教育培训记录			
10		检查训练计划和训练记录			
11		检查演练计划和演练记录			
12		是否指定了专职联络员，联络员的配置和变更，是否及时按要求报备，年内是否存在工作联系不到的情况			
13		7.1.5	反恐怖防范工作机构设置、责任领导、责任部门等是否按要求报备，		
14	保安员承担保安职责，是否满足《保安服务管理条例》和 GA/T 594 的相关要求并持证上岗				
15	反恐怖防范专职工作人员是否掌握重点目标内部和周边环境、消防通道和各类疏散途径				
16	反恐怖防范专职工作人员是否掌握本重点目标反恐怖防范工作情况及相关规章制度、应急预案等				
17	7.2 物 防	7.2.3	机动车阻挡装置设置是否已覆盖无实体防护屏障的出入口		
18			防机动车冲撞或隔离设施是否已覆盖出入口		
19			安防监控中心等重要部位出入口有否设立防盗安全门等实体防护设施		
20			出入口是否设置人车分离通道		
21			是否按实际需要配备了对讲机、强光手电、防暴棍棒、防暴盾牌、钢叉、防暴头盔、防割（防刺）手套、防刺服、防弹背心等个人应急防护装备		

表 A.1 重点项目检查表格（续）

序号	标准条款	内容概要	检查记录	项目结论	
22	7.2 物防	7.2.3 是否按实际需要配备了防爆毯（含防爆围栏）等公共应急防护装备			
23			安防监控中心、现金业务区等是否已按要求设置了应急警报器		
24			各工作区域是否按要求设置了灭火器材		
25	7.3 技防	7.3.3 是否已按要求设置了安防监控中心，安防监控中心是否设有控制、记录、显示等装置			
26			摄像机是否已覆盖出入口、周界、电梯轿厢、供电房、网络机房、库房内、出入库通道、守库室、票币清分场地、出入库交接场地、地下回廊、停车库（场）及其主要通道和出入口、安防监控中心、主要通道等部位		
27			库房内、守库室、安防监控中心、票币清分场地、出入库交接场地、现金服务区、业务办理区、银行自助设备、出入口是否已安装声音复核装置		
28			入侵探测（报警）器是否已覆盖金库库体、库房、网络机房、档案库等重要场所		
29			紧急报警装置（一键报警）是否已设置在守库室、现金服务区、安防监控中心		
30			报警控制器是否已设置在安防监控中心及相关的独立设防区域		
31			出入口控制系统是否已设置在网络机房、现金服务区、档案库、库房、保险柜库		
32			停车库（场）是否设置停车库（场）管理系统		
33			出入口、办公楼内各楼层、守库室、金库库体外围、供电房、安防监控中心、网络机房、通风系统等重要部位是否设置了电子巡查系统		
34			公共广播系统是否已区域全覆盖		
35			无线通信对讲指挥调度系统是否已安装在安防监控中心并做到区域全覆盖		
36			视频录像保存时间是否不少于 90 天		
37			视频监控系统的备用电源是否满足至少 4 小时正常工作的需要；入侵报警系统备用电源是否满足至少 24 小时正常工作的需要		
38	7.4 制度防	7.4.1 7.4.2 是否按要求配置了相关管理制度，包括教育培训制度、人员背景审查制度、人员档案及备案制度、巡查与安检制度、值班查看和运维制度、训练演练制度、检查督导制度、人防增援配置制度、采购管理制度、设备设施档案制度、技防系统管理制度、工作报告制度、网络安全管理制度、专项经费保障制度、情报信息管理制度、恐怖威胁预警响应制度、恐怖威胁风险评估制度、联动配合机制、应急管理制度、押送管理制度、涉恐信息保密制度、线索快速反应制度、押运车管理制度等			
39	9 应急准备	9 是否制定了应急预案			
40			应急预案的内容是否全面		
41			是否有组建应急作战队伍并建立有效增援保障措施		
42			是否按规定开展应急预案的演练		

检查部门：

检查人员（签名）：

检查日期：

参 考 文 献

- [1] 中华人民共和国主席令 第6号 中华人民共和国反恐怖主义法（2018修正）
- [2] 中华人民共和国主席令 第六十九号 中华人民共和国突发事件应对法
- [3] 中华人民共和国国务院令 第421号 企业事业单位内部治安保卫条例

