ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0139—2024

信息系统密码应用安全管理体系

Information system cryptography application security management systems

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　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　密码应用安全管理体系概述 …… 2
6　管理保障 …… 3
6.1　组织保障 …… 3
6.2　服务保障 …… 3
7　密码应用安全风险管理 …… 5
7.1　通用要求 …… 5
7.2　密码应用安全风险评估 …… 5
7.3　密码应用安全风险处置 …… 6
8　密码应用安全控制 …… 6
8.1　管理制度 …… 6
8.2　人员管理 …… 8
8.3　环境和资源管理 …… 10
8.4　规划和建设管理 …… 12
8.5　运行和维护管理 …… 13
8.6　应急管理 …… 15
8.7　监督和检查管理 …… 16
8.8　安全审计 …… 16
9　有效性测量和持续改进 …… 17
9.1　监视、测量和分析 …… 17
9.2　持续改进 …… 18
10　密码应用安全管理体系评估 …… 18
10.1　自评估 …… 18
10.2　第三方评估 …… 18
附录 A（规范性）　信息系统密码应用安全管理体系过程文件 …… 20
A.1　通则 …… 20
A.2　信息系统密码应用安全风险管理类文件 …… 20
A.3　信息系统密码应用安全控制类文件 …… 20
A.4　有效性测量和持续改进类文件 …… 21
A.5　密码应用安全管理体系评估类文件 …… 21

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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：工业和信息化部电子第五研究所、广州赛宝认证中心服务有限公司、北京电子科技学院、中国科学院信息工程研究所、中国科学院大学、北京数字认证股份有限公司、暨南大学、北京信安世纪科技股份有限公司、深圳市腾讯计算机系统有限公司。

本文件主要起草人：李丹、卢列文、高锐、尤博、云雷、刘北水、姚莹、古宜平、姚锐冬、肖威、彭辉、邓贵钊、程保琨、金诚斌、陈艳、段沛鑫、阎亚龙、马原、郑昉昱、张永强、谭武征、汪宗斌、谢灿、杜大海。

引　言

为了对组织的信息系统密码应用安全管理提供整体、统一的模型和方法，从管理层面保障信息系统密码应用安全，制定本文件。本文件可作为组织基于GB/T 22080实现信息安全管理体系(ISMS)过程中选择控制时的参考，或作为组织在实现密码应用安全管理控制时的指南。在考虑信息系统安全等级和具体密码应用信息安全风险环境后，本文件也可用于制定特定行业和特定组织满足GB/T 39786—2021密码应用管理要求的指南。

信息系统密码应用安全管理体系

1 范围

本文件规定了组织建立、实施、运行、保持和持续改进密码应用安全管理体系的要求，从管理层面给出了密码应用安全控制措施和实施指南。

本文件适用于信息系统运营者等与密码应用相关的各种类型、规模和特性的组织，适用于网络安全等级保护第一级到第四级的信息系统。

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 22080—2016 信息技术 安全技术 信息安全管理体系要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25069—2022 信息安全技术 术语

GB/T 29246—2023 信息安全技术 信息安全管理体系 概述和词汇

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GB/T 43207 信息安全技术 信息系统密码应用设计指南

GM/Z 4001—2013 密码术语

3 术语和定义

GB/T 29246—2023、GB/T 22080—2016、GB/T 25069—2022、GB/T 39786—2021、GB/T 43207、GB/T 22240 和 GM/Z 4001—2013 界定的以及下列术语和定义适用于本文件。

3.1

组织 organization

具有自身的职责、权威和关系以实现其目标的个人或集体。

注：组织的概念包括但不限于个体经营者、公司、法人、商行、企业、机关、合伙关系、慈善机构或院校，或者其部分或组合，无论注册成立与否、是公共的还是私营的。

3.2

控制 control

改变风险的措施。

注 1：控制包括任何改变风险的过程、策略、装置、实践或其他措施。

注 2：控制可能并不总是发挥出预期或假定的改变效果。

3.3

有效性 effectiveness

实现所计划活动和达成所计划结果的程度。

4 缩略语

下列缩略语适用于本文件。

CPU:中央处理器(Central Processing Unit)

ISMS:信息安全管理体系(Information Security Management Systems)

PDCA:计划—实施—检查—改进(Plan-Do-Check-Act)

5 密码应用安全管理体系概述

密码应用安全管理遵循信息安全管理科学规律,采用“计划—实施—检查—改进”循环,即 PDCA 管理循环,基于密码应用安全影响分析和密码应用安全风险评估,实施分层面控制,形成如图 1 所示的框架。

a) 在计划阶段,建立健全密码应用安全管理机构,制定密码应用安全管理目标,明确密码应用安全管理过程和程序。

b) 在实施阶段,开展密码应用安全风险管理,实施和运行密码应用安全控制。

c) 在检查阶段,对照密码应用安全管理目标,监视、测量和分析密码应用安全控制,并开展密码应用安全管理体系评估。

d) 在改进阶段,基于密码应用安全管理的内部审核和管理评审的结果,采取纠正和预防措施,适时对密码应用安全管理体系进行变更,以持续改进密码应用安全管理。由此进入新一轮的 PDCA 管理循环。

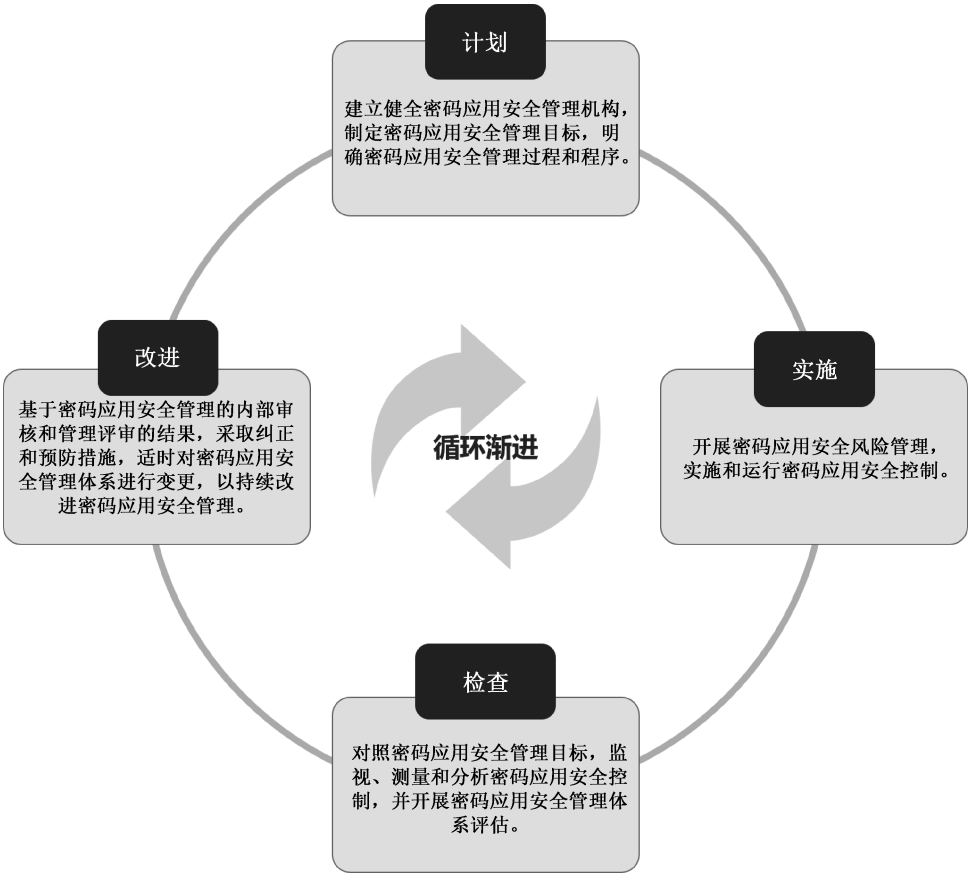

图 1 密码应用安全管理体系框架

6 管理保障

6.1 组织保障

6.1.1 管理机构

应成立指导和管理密码应用安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权，并明确其责任和权力。

a） 密码应用安全工作委员会或领导小组应：

1） 制定密码应用安全管理目标；

2） 全面统筹实施组织内部的密码应用安全工作，对密码应用安全负直接责任；

3） 制定、签发、实施、更新密码应用安全相关规范；

4） 统筹开展密码应用安全性评估；

5） 统筹开展密码应用安全培训；

6） 统筹开展密码应用安全应急演练和应急处置；

7） 统筹开展密码应用安全攻防对抗演习；

8） 统筹密码应用安全管理自评价。

b） 密码应用安全工作委员会或领导小组应确保密码应用安全管理的有效性：

1） 确保密码应用安全管理所需资源可用；

2） 明确密码应用安全管理要求的重要性；

3） 确保密码应用安全管理达到预期结果；

4） 促进密码应用安全管理控制措施持续改进。

6.1.2 参与主体

组织应确定：

a） 密码应用安全管理参与主体，例如组织内信息系统运营者等与密码应用相关的主体；

b） 参与主体与密码应用安全相关的要求。

注：参与主体的要求包括法律、法规要求和合同义务等。

6.1.3 管理范围

管理范围包括以下内容：

a） 组织应确定密码应用安全管理的范围：密码应用范围；

b） 密码应用安全管理涉及的组织范围；

c） 密码算法、技术、产品、服务使用范围；

d） 使用密码技术进行保护的信息系统的物理和环境范围；

e） 使用密码技术进行保护的信息系统的网络和通信范围；

f） 使用密码技术进行保护的信息系统的设备和计算范围；

g） 使用密码技术进行保护的信息系统的应用和数据范围。

该范围应形成文件记录并确保其适用性。

6.2 服务保障

6.2.1 资源保障

组织应确定并提供建立、实现、维护和持续改进密码应用安全管理所需的资源：

a) 确定并提供管理组织资源；
b) 确定并提供所需人力资源；
c) 确定并提供所需资金保障；
d) 确定并提供所需组织过程资产。

6.2.2 密码应用安全能力

组织应：
a) 确定密码相关工作人员应具备的能力；
b) 确保密码相关工作人员接受密码应用安全培训和考核；
c) 建立密码应用安全培训和考核体系，并评估其有效性；
d) 保留适当的文件记录作为安全能力证明。

组织应定期(至少每年一次)或在密码应用安全相关要求发生重大变化时，对相关岗位上的人员开展密码应用安全专业化培训和考核，确保相关人员熟练掌握密码应用安全要求。

6.2.3 密码应用安全意识

密码相关工作人员应了解：
a) 密码应用安全相关法律法规；
b) 密码应用安全相关政策；
c) 密码应用安全相关标准规范；
d) 组织内部的密码应用安全相关要求；
e) 密码应用安全相关教育培训的重要性；
f) 密码应用安全性工作的缺失对组织带来的危害和损失。

6.2.4 文件记录

6.2.4.1 通用要求

组织的密码应用安全管理应包括以下内容。
a) 要求的文件记录，包括：
——风险管理类文档；
——安全控制类文档；
——有效性测量和持续改进类文档；
——管理体系评估类文档。
具体要求应符合附录 A 的规定。
b) 为保证密码应用安全管理的有效性，组织所确定的必要的文件记录。

6.2.4.2 文件记录的控制

文件记录的控制应包括以下内容。
a) 文件记录应得到控制，以确保：
1) 文件记录的可用性和适用性；
2) 得到充分的保护(如避免保密性损失、不恰当使用、完整性损失等)。
b) 组织应对文件记录及时归档留存，保证其具有可追溯性，原始文件记录的保存期限不得少于 6 年。
c) 组织应加强对下述场景中文件记录的管理：存储、分发、访问、检索、使用、变更、归档和销毁。

组织确定的为规划和运行密码应用安全管理所必需的外来的文件记录，应得到适当的识别，并予以控制。

7 密码应用安全风险管理

7.1 通用要求

组织进行密码应用安全风险管理时，应满足以下要求。

a) 密码应用安全管理体系规划时，组织应充分识别法律法规的要求，评价安全影响和实施风险评估，并确定需要应对的风险，以：
   1) 准确识别出信息系统存在密码应用安全风险；
   2) 预防或减少密码应用安全风险对信息系统的不良影响；
   3) 确保密码应用安全管理可达到预期结果；
   4) 持续改进。
b) 组织应进行以下事宜：
   1) 编制资产清单；
   2) 对资产的价值和重要性进行分析；
   3) 对系统面临的威胁进行分析；
   4) 对密码应用安全风险和密码应用需求进行分析；
   5) 规划应对威胁、安全风险和密码应用需求的措施；
   6) 将这些措施整合到密码应用安全管理过程中，并予以实现；
   7) 对措施实施有效性进行测量，并在此基础上实施密码应用安全管理的自评价。

7.2 密码应用安全风险评估

组织应从以下几方面开展密码应用安全风险评估。

a) 识别资产并进行分析：
   1) 梳理信息系统资产；
   2) 分类统计并编制资产清单；
   3) 对资产进行重要程度标识。
b) 识别威胁并进行分析：
   1) 根据以往发生的密码应用安全事件、外部提供的资料和积累的经验等，对威胁进行粗略的分析；
   2) 结合业务应用、系统结构特点以及数据流转路径等因素，建立并维护威胁列表。
c) 识别密码应用安全风险并形成风险列表：
   1) 密码应用全生命周期内，不符合安全管理要求，带来不可接受影响的相关风险；
   2) 来自内部变化（如密码应用需求增长）和外部变化（如政策变化、技术进步）的密码应用潜在风险；
   3) 密码应用安全风险的类别；
   4) 风险责任人。
d) 分析密码应用安全风险：
   1) 用户和专家对资产、威胁和风险等方面进行综合评估；
   2) 评估风险发生后可能导致的不良影响及潜在后果；
   3) 评估风险实际发生的可能性；
   4) 分析产生风险的潜在因素。

e） 评价密码应用安全风险：

1） 将风险分析结果与风险评价准则进行比较，确定风险等级；

2） 为风险处置排序以评价风险处置的优先级。

组织应保留有关密码应用安全风险评估过程的文件记录。

7.3 密码应用安全风险处置

组织应进行密码应用安全风险处置：

a） 在考虑密码应用安全风险评估结果的基础上，结合组织对于信息系统密码应用的需求，选择适合的风险处置措施；

b） 制定正式的密码应用安全风险处置方案；

c） 针对信息系统的资产清单、威胁列表、风险列表，结合已采用的安全控制措施，分析存在的残余风险；

d） 获得风险责任人对密码应用安全风险处置方案的批准；

e） 获得风险责任人对密码应用安全残余风险处置措施（残余风险接受、残余风险监视、安全风险再评估）的批准；

f） 按照选定的风险处置方案和残余风险处置措施进行风险处置。

注：风险处置措施一般包括：风险接受、风险减缓、风险转移和风险规避，组织也能使用其他分类和描述方式的风险处置措施。

组织应保留有关密码应用安全风险处置过程的文件记录。

8 密码应用安全控制

8.1 管理制度

8.1.1 安全管理制度的制定和落实

8.1.1.1 控制措施

根据组织的业务实际和密码应用需求，制定信息系统密码应用安全管理规章制度，并按要求落地实施。

8.1.1.2 实施指南

具体实施指南如下。

a） 依据下列原则制定并落实信息系统密码应用安全管理规章制度：

1） 安全需求原则；

2） 主要领导负责原则；

3） 全员参与原则；

4） 系统方法原则；

5） 持续改进原则；

6） 依法管理原则；

7） 分权和授权原则；

8） 管理与技术并重原则；

9） 自保护和国家监管结合原则。

b） 对信息系统密码应用的生存周期全过程实施管理，包括：

1） 成立密码应用安全管理机构；

2） 设置密码应用安全管理相关岗位，并明确岗位职责；
3） 配置与岗位职责要求相匹配的安全管理人员；
4） 结合信息系统密码应用需求制定管理制度；
5） 依据密码资源建设形态（物理资源、云资源）、管理机构设置情况和业务应用实际，制定密钥管理制度；
6） 根据信息系统规划、建设、运行、运维等全生命周期密码应用安全管理需求，制定密码应用建设运行规章制度；
7） 结合信息系统实际，制定密码应用应急处置策略；
8） 依据资产清单，制定密码软硬件及介质管理制度；
9） 选择与实施密码应用安全措施；
10） 定期进行监控和检查，妥善处置密码应用安全事件；
11） 定期开展密码应用安全意识教育培训。

c） 将密码应用安全管理纳入到组织的日常安全管理中，定期检查密码应用安全管理制度的落实情况，例行评估和报告密码应用安全事件，定期测试关键环节的密码控制措施。

8.1.2 密钥管理规则的制定和落实

8.1.2.1 控制措施

根据组织的密钥管理制度和信息系统的密码应用方案，制定并落实符合系统实际的密钥管理规则。

8.1.2.2 实施指南

具体实施指南如下：

a） 依据密钥管理制度，制定信息系统的密钥管理规则；
b） 围绕信息系统密码应用方案中明确的密钥体系，制定密钥管理规则；
c） 综合考虑信息系统业务应用实际、密码产品特征、密码介质使用规定等因素，制定涵盖密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等全生命周期的密钥管理规则；
d） 在密码应用实施中严格落实密钥管理规则；
e） 定期检查密钥管理规则的落实情况。

8.1.3 操作规程的建立和落实

8.1.3.1 控制措施

对管理及操作人员执行的日常管理操作建立操作规程，并在日常管理过程中严格落实。

8.1.3.2 实施指南

具体实施指南如下：

a） 依据现行的政策法规、标准规范，并结合组织实际，围绕组织内的管理环节，制定操作规程；
b） 明确操作规程的适用范围，在日常管理中严格落实各项操作规程；
c） 指定管理和操作人员，依据信息系统密码应用操作规程，负责信息系统的密码服务及密码设备的管理和操作；
d） 指定专人保管信息系统密码应用操作规程文档，借阅操作规程文档，应由相应级别负责人审批和登记；
e） 对信息系统各个岗位应进行定期检查操作规程和管理程序的执行情况，确保遵从组织机构的安全策略；

f） 培养管理及操作人员密码安全意识，并提供对安全政策和操作规程的认知教育和训练等。

8.1.4 安全管理制度的修订

8.1.4.1 控制措施

定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订。

8.1.4.2 实施指南

具体实施指南如下：

a） 定期对密码应用安全管理制度体系的合理性和适用性进行审定，留存审定或论证记录，如果对制度做过修订，留存各个版本安全管理制度；

b） 定期对操作规程的适用性和有效性进行审定，留存审定或论证记录，当密码技术、密码设备发生重大变更时，要及时审核修订操作规程。

8.1.5 安全管理制度的发布

8.1.5.1 控制措施

明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制。

8.1.5.2 实施指南

具体实施指南如下：

a） 制定安全管理制度和操作规程的发布流程；

b） 留存各个版本的制度和操作规程发布文件或记录。

8.1.6 制度执行过程的记录留存

8.1.6.1 控制措施

按照制度和操作规程开展日常管理工作，做好执行记录并妥善保存。

8.1.6.2 实施指南

具体实施指南如下：

a） 制作制度及操作规程执行记录表单；

b） 执行相关制度及操作时做好记录；

c） 留存相关制度及操作执行中产生的各类文件和表单。

8.2 人员管理

8.2.1 岗位责任制度

8.2.1.1 控制措施

建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限。

8.2.1.2 实施指南

具体实施指南如下。

a) 根据密码应用实际情况，设置密码应用关键安全岗位：
   1) 设立密码应用相关岗位；
   2) 定义岗位职责，并建立岗位职责文档；
   3) 设置密钥管理员、密码安全审计员、密码操作员等密码应用关键岗位；
   4) 为密码应用相关岗位配备与岗位能力要求相匹配的管理人员；
   5) 关键岗位人员应定期接受安全培训，加强安全意识和风险防范意识；
   6) 必要时关键岗位人员应采取定期轮岗制度。
b) 对关键岗位建立多人共管机制。
c) 关键岗位人员职责互相制约互相监督：
   1) 坚持关键岗位人员“权限分散、不得交叉覆盖”的原则；
   2) 允许一人多岗；
   3) 密钥管理、密码安全审计、密码操作人员等关键岗位职责互相制约互相监督；
   4) 密码安全审计员岗位不可与密钥管理员、密码操作员兼任。
d) 相关设备与系统的管理和使用账号不得多人共用。
e) 密钥管理员、密码安全审计员、密码操作员应由本组织的内部员工担任，并在任前对其进行背景调查。

8.2.2 人员培训制度

8.2.2.1 控制措施

建立并落实人员培训制度。

8.2.2.2 实施指南

具体实施指南如下：

a) 建立上岗人员培训制度，对于涉及密码操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；
b) 建立日常培训制度，定期或不定期对密码相关岗位人员进行密码相关法律法规、标准规范培训，增强岗位人员的密码相关法律法规意识和对组织内密码应用安全管理制度的理解程度；
c) 针对不同密码应用岗位，制定培训和教育计划，包括但不限于政策法规要求、密码安全知识、密码安全技术、密码安全标准、密码安全要求和日常操作规程等；
d) 留存培训记录，包含但不限于培训人员、培训内容、培训结果等内容；
e) 对所有岗位人员的安全资质进行定期检查和评估，使相应的安全培训成为组织工作的一部分。

8.2.3 人员定期考核

8.2.3.1 控制措施

定期对密码应用安全岗位人员进行考核。

8.2.3.2 实施指南

具体实施指南如下：

a) 建立人员考核制度，定期开展密码应用安全管理相关考核；
b) 定期对各个岗位的人员进行不同侧重的密码安全认知和密码安全技能的考核，作为人员是否适合当前岗位的参考；
c) 定期审查密码应用关键安全岗位人员，及时调整违反安全规定的关键安全岗位人员；

d) 制定考核结果惩戒措施，对考核不合格人员实施惩戒并要求限期整改；
e) 对考核记录进行留存和归档。

8.2.4 人员录用管理

8.2.4.1 控制措施

建立人员录用管理制度，对拟录用人员进行审查与考核，确保人员满足业务需求和安全管理要求。

8.2.4.2 实施指南

具体实施指南如下：
a) 对应聘者进行审查，确认其具有基本的专业技术水平，接受过安全意识教育和培训，能够掌握密码应用安全管理基本知识，对密码应用关键安全岗位人员还应注重思想品质方面的考察；
b) 由单位人事部门对应聘者进行人员背景和资质审查、技能考核等，合格者签署保密协议方可上岗。

8.2.5 人员保密和调离管理

8.2.5.1 控制措施

建立关键人员保密制度和调离制度，签订保密协议，承担保密义务。

8.2.5.2 实施指南

具体实施指南如下：
a) 建立密码关键岗位人员的保密制度和调离制度，明确人员调岗、离岗时的相关规定；
b) 建立保密制度时，应包含保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容；
c) 定期对密码关键岗位人员进行保密教育培训，增强相关岗位人员的安全保密意识；
d) 关键岗位人员调岗、离岗时，按照调离制度办理调离手续并留存相关调离记录；
e) 立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限，收回所有相关证件、徽章、密钥、访问控制标记，收回机构提供的设备等；
f) 密码关键岗位人员调离岗位，必须经单位人事部门办理调离手续，并履行调离后的保密义务。

8.3 环境和资源管理

8.3.1 机房安全管理

8.3.1.1 控制措施

配置机房安全的责任部门和管理人员，建立有关机房安全方面的规章制度。

8.3.1.2 实施指南

具体实施指南如下：
a) 明确机房安全管理的责任人，指定专人负责机房出入管理，禁止未经允许的人员进入机房；
b) 获准进入机房的来访人员，其活动范围应受到限制，并有接待人员陪同；
c) 指定专人管理机房门禁系统和视频监控系统；
d) 未经许可不得将与工作无关的物品带入机房，不得将任何记录介质、文件材料及各种设备部件带出机房；

e) 门禁系统的电子记录应妥善保存以备检查；
f) 视频监控系统的音像记录应妥善保存以备检查。

8.3.2 办公环境安全管理

8.3.2.1 控制措施

加强对设置有服务器、存储、网络、安全、密码设备运维终端及应用系统管理终端的办公环境的安全管理，确保办公环境的安全性。

8.3.2.2 实施指南

具体实施指南如下：
a) 为设备运维和应用系统管理设置专门的办公区域；
b) 制定办公环境安全管理制度；
c) 工作人员下班后应关闭计算机终端；
d) 存放敏感文件或信息载体的文件柜应上锁或设置密码；
e) 工作人员调离部门或更换办公室时，应立即交还办公室钥匙；
f) 工作人员离开座位时，计算机终端应退出登录状态、采用屏幕保护口令保护或关机。

8.3.3 密码设备管理

8.3.3.1 控制措施

建立密码设备管理制度，确保密码设备使用安全。

8.3.3.2 实施指南

具体实施指南如下：
a) 编制并维护与信息系统相关的密码设备清单；
b) 制定密码设备管理制度，做好日常管理工作；
c) 制定各类密码设备操作手册，指导使用人员开展工作；
d) 明确各密码设备的责任人、运行状态以及资产所在的位置等；
e) 根据密码设备的重要程度对其进行标识，基于设备资产的价值选择保护措施；
f) 对密码设备进行分类管理；
g) 明确密码设备的选型、采购、使用和保管的责任人，落实设备管理岗位责任制；
h) 对密码设备的使用、转移、废弃及其授权过程做好记录，保证设备的安全性。

8.3.4 介质管理

8.3.4.1 控制措施

建立介质管理规章制度，严格各类介质管理。

8.3.4.2 实施指南

具体实施指南如下：
a) 制定介质管理制度，规范介质管理；
b) 对各类介质(特别是密码介质)进行控制和保护，防止被盗、被毁、被修改以及信息泄露；
c) 对介质进行定期盘点，并建立介质归档和查询记录；

d) 建立介质借阅、拷贝、传输批准制度，并登记在册；
e) 介质的销毁必须经批准并按指定方式进行，不得自行销毁；
f) 对于需要送出维修或销毁的介质，应首先删除信息，再重复写操作进行覆盖，防止数据恢复和信息泄露；
g) 需要带出工作环境的介质，其信息应受到保护；
h) 对存放在介质库中的介质应定期进行完整性和可用性检查，确认其数据或软件没有受到损坏或丢失；
i) 介质的保存和分发传递应有严格的规定并进行登记。

8.4 规划和建设管理

8.4.1 密码应用规划管理

8.4.1.1 控制措施

依据密码相关标准和密码应用需求，制定密码应用方案，配备必要的资金和专业人员。

8.4.1.2 实施指南

具体实施指南如下。

a) 组织依据 GB/T 43207 等密码相关标准，结合系统实际情况分析密码应用需求，制定密码应用方案。
b) 密码应用方案包含但不限于如下内容。
   1) 背景。明确系统的建设规划、国家有关法律法规要求、与规划有关的前期情况概述和项目实施的必要性，以及信息系统相关的其他情况说明。
   2) 系统概述。包含但不限于系统基本情况、计算平台现状、业务应用现状、密码应用现状、密码应用管理现状等。
   3) 密码应用需求分析。结合信息系统现状和 GB/T 39786—2021 中对不同等级的信息系统提出的密码应用基本要求，对计算平台、业务应用、管理制度、人员管理、建设运行和应急处置进行安全风险分析，确定风险控制措施、密码应用基本需求和密码应用特殊需求。通过风险控制措施缓解信息系统存在的高风险。
   4) 安全目标及设计原则。提出密码应用方案所涉及对象的密码应用安全目标。提出密码应用方案的设计原则、遵循的政策法规和相关标准。
   5) 密码应用设计。包含但不限于密码应用技术框架、计算平台密码应用方案、密码支撑平台方案、业务应用的密码应用方案、密码应用部署等内容。
   6) 安全管理方案。参照 GB/T 22240 中等级保护定级，按照 GB/T 39786—2021 对该等级的管理要求，根据部署的密码产品管理机制，设计安全管理方案，包括管理制度、人员管理、建设运行和应急处置方面的制度。
   7) 安全与合规性分析。逐条对照 GB/T 39786—2021 对应等级下的各项密码应用基本要求，对方案的适用情况、采取的密码保障措施、采取的缓解及替代性措施及自评结果进行说明。
c) 委托商用密码应用安全性评估机构对密码应用方案进行评估，评估报告形成后，将评估报告和相关工作情况按照国家有关规定报送密码管理部门备案。
d) 通过评估后的密码应用方案作为项目规划立项的重要材料，也是建设、验收和测评的重要依据。
e) 组织根据信息系统实际情况，配备必要的资金和专业人员，包含密码应用规划、建设、运行、运

维、评估等环节。

8.4.2 密码应用建设管理

8.4.2.1 控制措施

按照密码应用方案实施建设，做好密码应用安全性评估工作。

8.4.2.2 实施指南

具体实施指南如下。

a) 做好密码应用建设前的准备工作，包括但不限于确定项目负责人、制定项目实施计划、制定监理管理制度等：
   1) 确定项目负责人，对密码应用建设进行全过程的管理和监督；
   2) 制定详细的项目实施计划，作为项目管理的依据；
   3) 必要时建立密码应用建设监理管理制度，规范项目过程管理。
b) 按照密码应用方案实施建设，建设过程中涉及密码应用方案调整优化的，应委托专家或商用密码应用安全性评估机构对调整后的密码应用方案进行确认。
c) 系统建设完成后、投入运行前，按照 GB/T 39786—2021 的管理要求，进行密码应用安全性评估，评估通过后系统方可正式运行。未通过评估的系统，组织应针对评估中发现的安全问题及时整改，整改完成后进行复评估。评估报告形成后，将评估报告和相关工作情况按照国家有关规定报送密码管理部门备案。

8.5 运行和维护管理

8.5.1 密码应用安全性评估

8.5.1.1 控制措施

系统投入运行后，严格执行既定的密码应用安全管理制度，并定期开展密码应用安全性评估。

8.5.1.2 实施指南

具体实施指南如下：

a) 系统运行过程中，按照既定的密码应用安全管理制度和操作规程，开展日常运行管理工作，及时检查、总结、调整现有的密码应用措施，确保系统各项密码技术和管理措施落实到位；
b) 系统运行过程中，定期对信息系统开展密码应用安全性评估，并进行持续改进，确保系统密码应用的安全性。

8.5.2 密码应用攻防对抗演习

8.5.2.1 控制措施

系统投入运行后，应定期开展密码应用攻防对抗演习，检验系统密码应用的安全性。

8.5.2.2 实施指南

具体实施指南如下：

a) 围绕密码应用薄弱环节和典型应用场景，制定密码应用攻防对抗演习方案；
b) 系统投入运行后，定期开展密码应用攻防对抗演习；
c) 必要时配置与信息系统一致的模拟/仿真环境，在模拟/仿真环境中开展攻防对抗演习；

d) 对密码应用攻防对抗演习进行总结，提炼经验做法，查找问题不足，促进安全整改，不断提升系统密码应用的安全性。

8.5.3 密码设备操作管理

8.5.3.1 控制措施

在运行过程中，加强对密码设备的管理和监控。

8.5.3.2 实施指南

具体实施指南如下。

a) 由授权的人员对密码设备进行操作。
b) 按照操作规程实现密码设备的启动/停止、加电/断电等操作。
c) 维护密码设备的运行环境及配置。
d) 采用密码技术实现操作的身份鉴别管理。
e) 加强密码设备的日志文件管理和监控管理：
   1) 日志管理包括但不限于对密码设备调用、设置等日志的管理和维护；
   2) 监控管理包括但不限于监控密码设备的性能，如监测 CPU 和内存的利用率、检测进程运行及磁盘使用情况等。
f) 加强配置文件管理，包括密码设备的系统配置和服务设定的配置文件的管理，定期对密码设备运行的安全性进行检查和评估，及时发现密码设备在使用过程中的缺陷或漏洞。

8.5.4 密码软硬件及介质维护管理

8.5.4.1 控制措施

在运行过程中，加强对密码软硬件及介质的维护和管理。

8.5.4.2 实施指南

具体实施指南如下：

a) 明确信息系统密码软硬件及介质维护的人员和责任，规定维护的时限，以及设备更新和替换的管理办法；
b) 制定密码软硬件及介质维修管理制度；
c) 依据设备特征，针对需要维修的设备制定维修方案；
d) 根据维修方案和风险评估的结果确定维修方式；
e) 外部维修人员进入机房维修，应经过审批，并有专人负责陪同；
f) 对需要外出维修的设备，应经过审批，并有专人负责陪同；
g) 对密码设备的重要数据和软件系统进行必要的保护，防止因维修造成破坏和泄露；
h) 对维修过程及有关现象记录备案。

8.5.5 日常运行安全管理

8.5.5.1 控制措施

在运行过程中，动态监控密码设备的运行状况，对密码设备的日常运行进行安全管理。

8.5.5.2 实施指南

具体实施指南如下：

a) 通过正式授权程序委派专人负责密码设备运行的安全管理；
b) 正确实施为密码设备可靠运行而采取的各种检测、监控、审计、分析、备份及容错方法和措施；
c) 对密码设备的运行安全进行监督检查；
d) 明确密码安全管理人员和普通用户对密码相关资源的访问权限；
e) 按照风险管理计划和操作规程定期对密码设备的运行进行风险分析与评估；
f) 对密码设备运行进行风险控制，包括但不限于对关键岗位的人员实施严格的背景调查和管理控制，落实最小授权原则和分权制衡原则，对密码设备的关键操作要求多人共管；
g) 对外部服务方实施严格的访问控制，对其访问实施监视，并定期对外部服务方访问的风险进行分析和评估；
h) 对系统中的关键密码设备和密钥数据采取可靠的备份措施；
i) 对密码设备的日志进行管理。

8.6 应急管理

8.6.1 应急策略

8.6.1.1 控制措施

制定密码应用应急策略，做好应急资源准备。

8.6.1.2 实施指南

具体实施指南如下：
a) 确定密码应用应急管理部门并明确其职责；
b) 围绕密码应用安全事件进行影响分析；
c) 制定密码应用应急处置计划；
d) 明确应急事件处理流程及其他管理措施；
e) 制定密码应用恢复策略，包括恢复密码应用所需的资源和操作规程；
f) 定期开展应急演练；
g) 定期维护密码应用应急策略。

8.6.2 应急处置

8.6.2.1 控制措施

制定具体的应急处置措施，密码应用安全事件发生后，按流程开展应急处置。

8.6.2.2 实施指南

具体实施指南如下：
a) 对信息系统密码应用的应急处置提出明确要求，制定具体的应急处理措施；
b) 密码应用安全事件发生后，根据其危害和发生的部位，迅速确定事件等级，并根据等级启动相应的响应和处置预案；
c) 事件发生后，及时向信息系统主管部门及归属的密码管理部门进行报告；
d) 事件处置完成后，及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况；
e) 留存相应的事件处置记录；
f) 分析和鉴定事件产生的原因，制定防止再次发生的补救措施；
g) 收集相关证据，分析事件发生的技术原因和管理责任，形成分析报告，并进行必要的评估。

8.6.3 应急保障

8.6.3.1 控制措施

做好应急管理保障工作，确保应急处置高效有序进行。

8.6.3.2 实施指南

具体实施指南如下：

a) 确定应急管理机构和应急处置实施人员，明确应急处置过程中的职责分工；
b) 加强对相关人员的业务和技能培训，确保应急处置人员熟练掌握应急处置控制手段及恢复措施；
c) 定期检查应急策略、应急计划、应急措施的正确性、完整性和适用性，并适时进行完善和调整。

8.7 监督和检查管理

8.7.1 法律法规要求

8.7.1.1 控制措施

充分了解密码相关法律法规要求，防止出现违法违规行为。

8.7.1.2 实施指南

具体实施指南如下：

a) 充分认识密码相关法律法规和政策标准要求；
b) 在密码应用的设计、操作、使用和管理中自觉遵守相关法律法规，防止出现违法违规行为；
c) 保护组织的重要数据和个人隐私信息；
d) 密码应用中采用的密码技术、产品和服务应符合密码相关法律法规和政策标准要求。

8.7.2 符合性检查

8.7.2.1 控制措施

定期对密码应用安全管理活动的各个方面进行检查和评估，改进问题和不足。

8.7.2.2 实施指南

具体实施指南如下：

a) 依据管理制度进行自管、自查、自评，定期检查和评估密码应用安全管理活动；
b) 定期检查密码应用安全策略的遵守情况，重点检查密码应用相关岗位，确保相关人员能够正确履行其岗位责任，遵守相关密码应用安全策略；
c) 定期检查密码应用是否达到相应密码应用等级技术基本要求；
d) 定期检查有关密码设备使用情况和操作过程，并持续改进完善；
e) 建立检查和改进制度，根据检查过程中发现的问题不断完善密码应用安全管理体系。

8.8 安全审计

8.8.1 密码应用安全管理体系运行审计

8.8.1.1 控制措施

定期对信息系统密码应用安全管理体系实施审计，持续完善管理体系。

8.8.1.2 实施指南

具体实施指南如下：

a） 每年对管理体系运行情况进行审计；

b） 制定年度管理体系运行审计计划，并经密码应用安全工作委员会或领导小组会议通过；

c） 对运行和维护管理体系的有效性和正确性进行审计；

d） 对密码应用安全工作委员会或领导小组是否健全进行审计；

e） 对密码应用管理职能和管理职责是否明确进行审计；

f） 对管理制度的制定和实施情况进行审计。

8.8.2 信息系统密码应用活动审计

8.8.2.1 控制措施

定期对信息系统密码应用活动实施审计，持续优化信息系统密码应用活动。

8.8.2.2 实施指南

具体实施指南如下：

a） 每年对信息系统密码应用活动进行审计；

b） 制定年度审计计划；

c） 对组织内信息系统数量、规模、信息系统安全保护等级、信息系统密码应用整体情况进行审计；

d） 对信息系统密码应用安全风险管理进行审计；

e） 密码应用安全事件发生后，需单独对该系统进行审计；

f） 对信息系统密码应用相关岗位职责和权限进行审计；

g） 对信息系统密码应用关键安全岗位人员进行上岗、调岗、离岗、离职审计；

h） 对信息系统中密码设备设施的运行进行审计；

i） 对信息系统中密码设备设施的操作和维护进行审计。

9 有效性测量和持续改进

9.1 监视、测量和分析

组织应监视和测量密码应用安全控制和管理体系运行的有效性。

组织应确定：

a） 需要被监视和测量的内容，包括密码应用安全过程和控制、管理体系运行等；

b） 适用的监视、测量、分析和评价的方法，以确保得到有效的结果，包括但不限于内部审核、管理评审、绩效指标监测、数据收集与分析、客户满意度调查、法律法规合规性评估等；

c） 执行监视和测量的时机，包括信息系统密码应用控制维度和管理体系运行维度；

d） 执行监视和测量的主体，例如信息系统运营者等；

e） 分析和评价监视和测量结果的时机，包含但不限于信息系统规划阶段（例如编制密码应用方案时）、建设阶段（例如新增密码设备时）、运行阶段（例如人员变动、设备更新时）等；

f） 分析和评价上述结果的主体，例如密码应用安全工作委员会或领导小组等。

组织应保留适当的文件记录作为监视和测量结果的证据。

注：所选的方法需产生可比较和可再现的有效结果。

9.2 持续改进

9.2.1 改进措施

组织应持续改进密码应用安全管理的适宜性、充分性和有效性。

当密码应用安全管理体系不符合组织实际时，组织应做到以下方面。

a) 采取措施，以控制并予以纠正。

b) 通过以下活动，对采取的措施进行分析和评价，以防止不符合再发生：

1) 评审不符合项；

2) 确定不符合原因；

3) 确定是否存在类似的不符合项；

4) 确定类似的不符合项发生的可能性。

c) 通过以下活动，对采取的措施进行分析和评价，以应对潜在风险和需求：

1) 评审分析政策变化带来的管理风险和管理需求；

2) 评审分析技术进步带来的管理风险和管理需求；

3) 评审分析密码应用需求增长带来的管理风险和管理需求；

4) 评审分析用户满意度。

d) 评审纠正措施的有效性。

e) 适时对密码应用安全管理体系进行变更。

9.2.2 证据保留

组织应保留文件记录作为以下方面的证据：

a) 不符合的性质及所采取的后续措施；

b) 纠正措施的结果。

10 密码应用安全管理体系评估

10.1 自评估

10.1.1 评估事项

组织应按计划对密码应用安全管理体系进行自评估，确定组织现有的密码应用安全管理体系：

a) 是否符合组织自身对密码应用安全管理的要求；

b) 是否符合本文件的要求；

c) 是否得到有效实现和维护。

10.1.2 评估流程

组织应：

a) 制定自评估计划；

b) 确保所有密码相关工作人员参与自评估；

c) 形成自评估报告；

d) 保留文件记录作为自评估的证据。

10.2 第三方评估

密码应用安全工作委员会或领导小组应定期邀请第三方评估机构对密码应用安全管理体系进行评

估，以确保组织能够保持体系要求的状态并持续改进，将安全影响控制到可接受水平。

第三方评估应考虑：

a） 既往自评估情况；

b） 既往第三方评估情况；

c） 与密码应用安全管理相关的外部和内部事项的变化；

d） 参与主体的反馈；

e） 持续改进的可能性。

第三方评估的输出应包括存在的问题和改进建议。

组织应保留文件记录作为第三方评估的证据。

附 录 A
（规范性）
信息系统密码应用安全管理体系过程文件

A.1 通则

根据第7章至第10章的规定，信息系统密码应用安全管理体系过程文档应涵盖以下材料。

A.2 信息系统密码应用安全风险管理类文件

具体文件如下：

a） 信息系统资产清单；
b） 信息系统威胁列表；
c） 信息系统风险列表；
d） 信息系统密码应用安全风险评估过程文档；
e） 信息系统密码应用安全风险处置方案及过程文档。

A.3 信息系统密码应用安全控制类文件

具体文件如下：

a） 信息系统密码应用安全管理制度；
b） 信息系统密钥管理规则；
c） 信息系统密码应用操作规程；
d） 信息系统密码设备操作手册；
e） 信息系统密码应用应急策略；
f） 信息系统密码应用应急处置计划；
g） 信息系统密码应用安全岗位职责文档；
h） 信息系统密码应用安全管理制度体系审定或论证记录；
i） 信息系统密码应用操作规程审定或论证记录；
j） 信息系统密码应用安全管理制度和信息系统密码应用操作规程发布文件或记录；
k） 信息系统密码应用安全管理制度和信息系统密码应用操作规程执行记录文件或表单；
l） 信息系统密码应用安全岗位人员培训记录；
m） 信息系统密码应用安全岗位人员考核记录；
n） 信息系统密码应用安全岗位人员保密协议；
o） 信息系统密码应用安全岗位人员调离记录；
p） 信息系统密码设备清单；
q） 信息系统密码设备的使用、转移、废弃及其授权记录；
r） 信息系统介质归档和查询记录；
s） 信息系统介质的保存和分发传递记录；
t） 信息系统密码应用方案；
u） 《信息系统密码应用方案》商用密码应用安全性评估报告或《信息系统密码应用方案》方案评审意见；
v） 信息系统商用密码应用安全性评估报告；
w） 信息系统密码应用攻防对抗演习方案、报告、整改文档；

x） 信息系统密码设备维修方案、维修过程及有关现象记录；

y） 信息系统密码应用安全事件处置记录。

A.4 有效性测量和持续改进类文件

具体文件如下：

a） 信息系统密码应用安全控制监视和测量结果记录；

b） 信息系统密码应用安全管理的适宜性、充分性和有效性记录。

A.5 密码应用安全管理体系评估类文件

具体文件如下：

a） 信息系统密码应用安全安全管理体系自评估计划及自评估报告；

b） 信息系统密码应用安全安全管理体系第三方评估报告。

中华人民共和国密码
行业标准
信息系统密码应用安全管理体系
GM/T 0139—2024
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.75　字数 40 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39031　定价 49.00 元

GM/T 0139-2024