商用密码应用安全性评估相关标准简介

2023年7月7日

目录 CONTENTS

一、前言

◆ 互联网的创新性

新四大发明覆盖和触及我们能够想到的任何场景，已经成为中国社会正常运行的“基础设施“。

◆ 虚拟世界与物理世界最大的差别

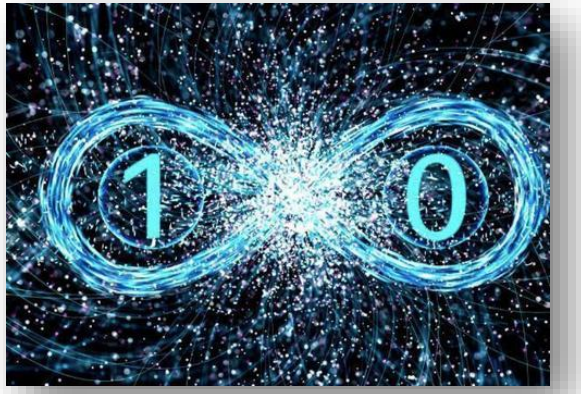
密码技术为虚拟世界提供信任和安全支撑，是阻止数据“裸奔”的最后一道防线。

一、前言

物联网是大数据的产生方式

5G开启了大数据高性能传输

云计算是大数据的使用方式



量子计算推进了大数据的高性能计算

人工智能发展了大数据的分析方法

谁来保障大数据产生、传输、使用过程中的安全？怎样保障个人隐私的安全使用？

目录 CONTENTS

密码发展沿革

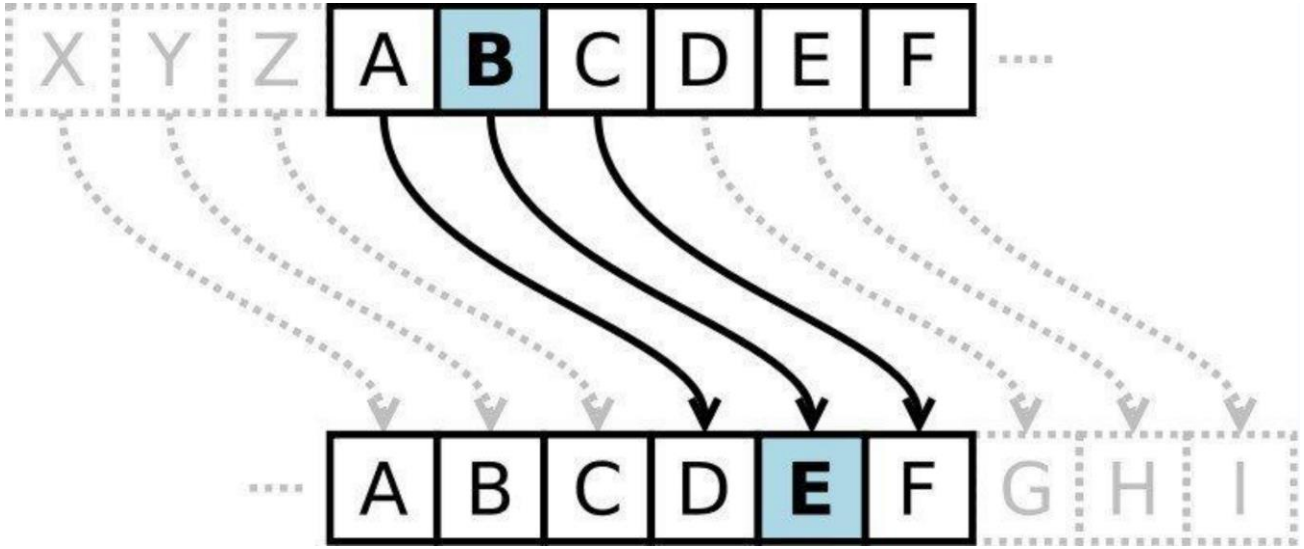
密码学（cryptography），源于希腊语kryptós“隐藏的”，和gráphein“书写”，是研究信息安全保密的学科，涉及**密码编码**与**密码分析**。

密码学的发展一般分为**传统密码学**和**现代密码学**两个阶段。

2.1 传统密码——古典密码

古典密码阶段从古代到19世纪末，长达上千年，主要采用**代换及置换**的方式，并通过手工或简单器械实现的。

斯巴达棒



凯撒密码

密码发展沿革

2.1 传统密码——近代密码

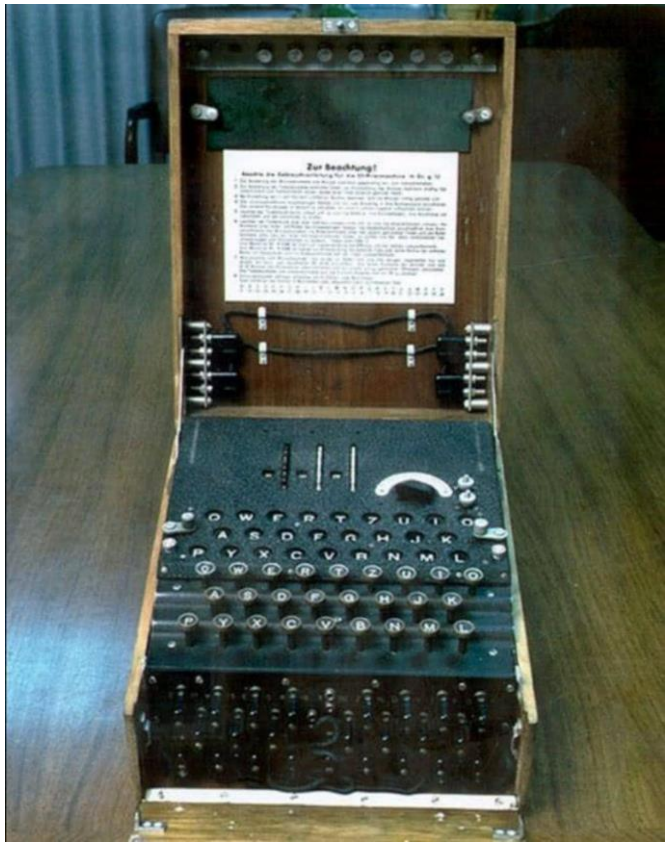
近代密码时期从20世纪初到20世纪50年代，工业革命为复杂密码的实现提供了先决条件，而战争对于保密通信的需求加速了密码技术的发展。

这段时期，加解密一般通过**机械或电动设备**实现，虽然技术上有了很大进步，但并未形成理论体系，加密仍然依靠替代及置换的方式。

典型的密码体制主要是单表代换密码（如仿射密码）、多表代换密码（如Vigenère 密码和Hill 密码等）。

世界上第一台转轮机在1918年由美国加州的EdwardHebern由一台打字机改造而成。

随后，Edward Hebern设计出一系列的转轮机，并为美国海军采用，在长达50年左右时间成为美军主要密码设备。

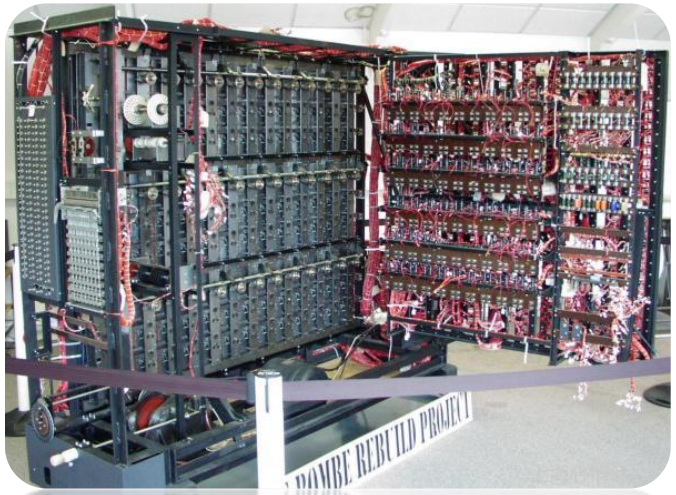


转轮密码机

二、密码的发展

密码发展沿革

计算机科学之父、人工智能之父，是计算机逻辑的奠基者



协助英国军方破解德国的著名密码系统“谜”(Enigma)，帮助盟军取得了二战的胜利

二、密码的发展

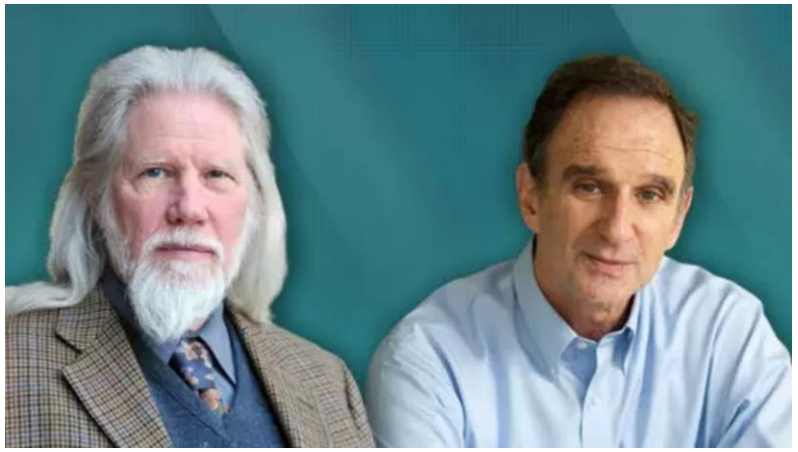
密码发展沿革

2.2 现代密码

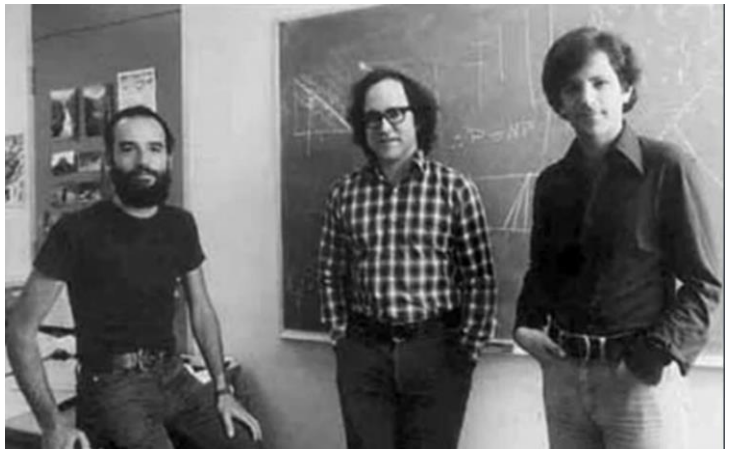
1949年香农发表论文《保密系统的通信理论》（Communication Theory of Secrecy System），标志着现代密码学的开端。

香农通过将信息理论引入到密码学中，为密码学奠定了坚实的理论基础，形成了**科学的密码学体系**。

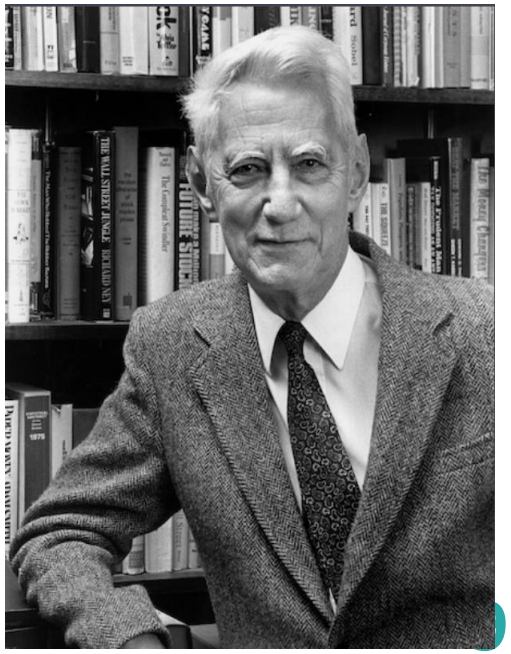
1976年，Diffie和Hell man 在《IEEE Transactions on Information Theory》发表的经典论文《密码学的新方向》（New Directions in Cryptography）提出了著名的公钥密码体制思想。**公钥密码体制**的诞生为现代密码学的发展开辟了一个崭新的方向，带来了密码学的**第二次飞跃**。



1978年，美国麻省理工学院的Rivest、Shamir 和 Adleman提出**RSA公钥密码体制**。这是第一个成功的公钥密码体制，其安全性是基于数论中的大整数因子分解困难问题。



克劳德•艾尔伍德•香农



我国密码发展历程

《密码法》第四条指出坚持中国共产党对密码工作的领导。坚持党对密码工作的绝对领导，是在任何时候，任何情况下都必须毫不动摇坚持的根本原则，党的密码工作创建于1930年，一直由党中央直接领导和管理，**党管密码原则是密码工作长期实践和历史经验的深刻总结，是密码工作最重要，最核心，最根本的要求。**

- 半部电台起家：1930年12月，红军缴获一部电台，发报机被砸坏，用只能收报的电台，获得了国民党的很多围剿信息。
- 周恩来同志一直领导和关心党的密码事业，亲自编制密码——“豪密”。
- **我国密码政策一直是党管密码**，负责密码通信的机要局设立在中共中央办公厅。
- 1993年，中央政治局召开会议，提出要对商用领域密码进行管理，在中央办公厅机要局下筹备商用密码管理办公室，密码分类也增加了第三类“**商用密码**”。

密码共分为**核心密码、普通密码和商用密码。**国家电网公司使用的是商用密码。

二、密码的发展

商用密码发展历程

1993 中央政治局召开会议，提出对商用领域密码进行管理，密码分类也增加了第三类“商用密码”

1999 时任总理朱镕基发布273号总理令，颁布《商用密码管理条例》

2005 国家密码管理委员会办公室更名国家密码管理局

2008 国家密码管理局纳入国务院序列管理

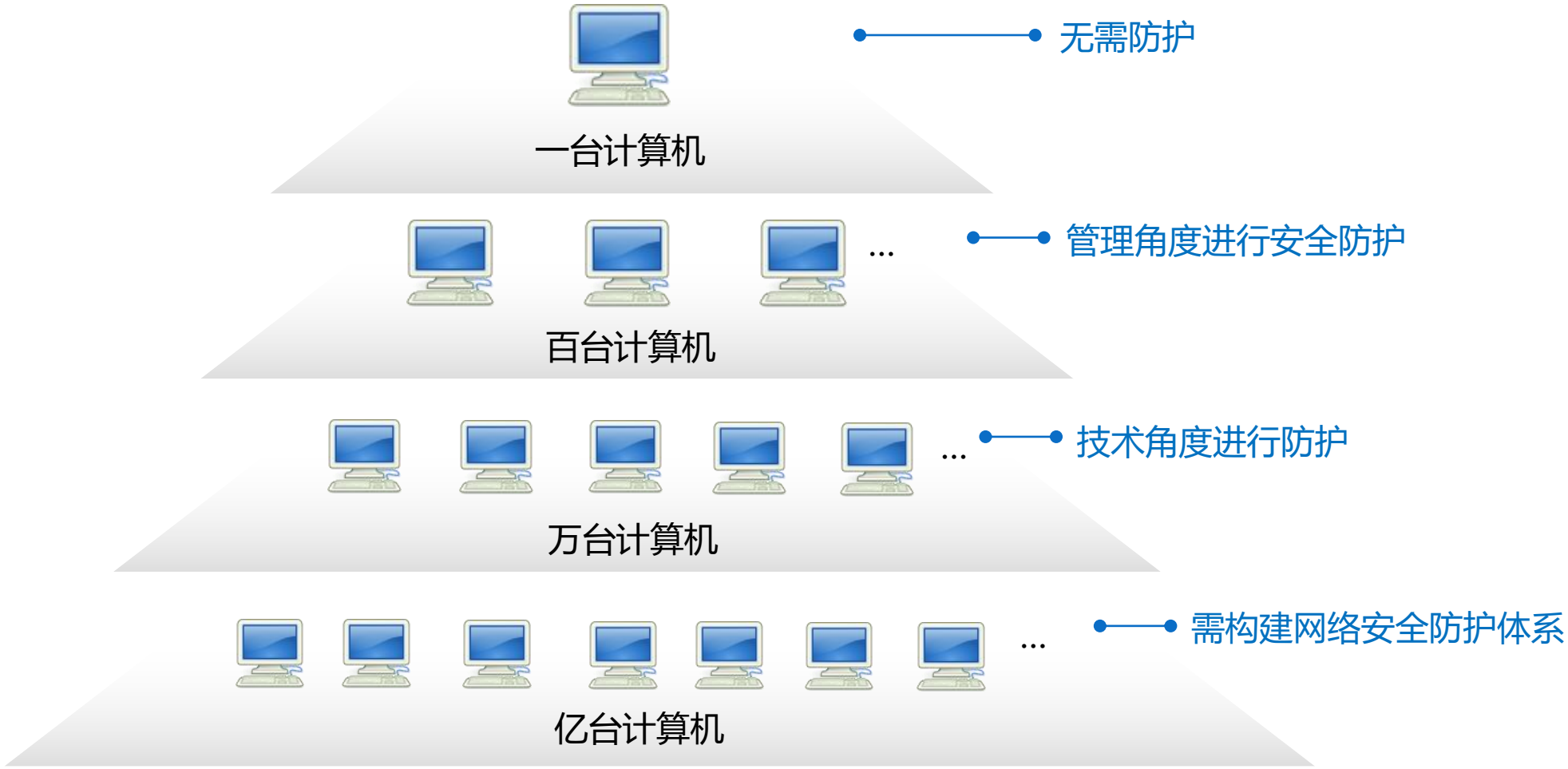
2006-2012 国家相继公布SM2/3/4密码算法，推进密码公开管理

2012 密码行业标准化技术委员会成立

2019 《密码法》颁布,规范密码应用和管理，促进密码事业发展，保障网络与信息安全

2021 《数据安全法》 和《个人信息保护法》颁布

三、密码与网络安全



网络安全的**实质即保护信息的安全**（机密性、完整性、可用性、不可否认性），密码技术是网络安全的**核心技术**和**基础支撑**，在解决网络信息系统的身份认证、加解密等发挥着不可替代作用，同时，该技术具有**可验证性**，因此，需构建以密码技术为网络信任基石的安全体系，实现对整个系统的网络安全风险控制。

目录 CONTENTS

密码标准基本框架

算法相关	GM/T 0001-2012 ZUC算法、GM/T 0002-2012 SM4分组、GM/T 0003-2012 SM2椭圆曲线、GM/T 0004-2012 SM3杂凑、GM/T 0044-2016 SM9标识密码……
基础规范	随机数：GM/T 0005-2021、GM/T 0062-2018、GM/T 0078-2020、GM/T 0103—2021、GM/T 0105—2021；标识使用规范：GM/T 0006-2012； 算法使用规范：GB/T 17964-2021、GM/T 0009-2012、GM/T 0010-2012……
基础设施	GM/T 0014-2012、GM/T 0015-2012、GM/T 0034-2014、GM/T 0037-2014、GM/T 0038-2014、GM/T 0043-2015、GM/T 0043-2015、GM/T 0092-2020……
接口规范	GM/T 0016-2012、GM/T 0018-2012、GM/T 0019-2012、GM/T 0020-2012、GM/T 0033-2014……
产品&协议	产品基础：GM/T 0008-2012、GM/T 0028-2014、GM/T 0039-2015 产品及协议：GM/T 0017-2012、GM/T 0021-2012、GM/T 0022-2014、GM/T 0023-2014、GM/T 0024-2014、GM/T 0025-2014、GM/T 0026-2014、GM/T 0027-201421、GM/T 0029-2014、GM/T 0030-2014……
密码测评	GB/T 39786-2021　　GM/T 0115-2021　　GM/T 0116-2021 《信息系统密码应用高风险判定指引》《商用密码应用安全性评估量化评估规则》

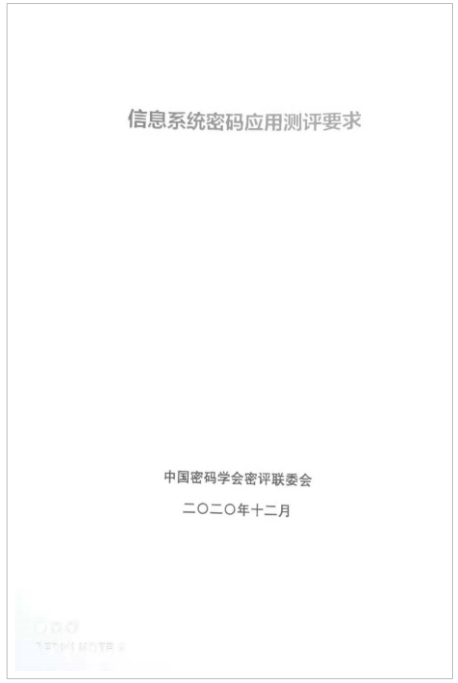
三、商用密码应用安全性评估标准简介

信息系统密码应用测评相关标准

1.《GB/T 39786 信息系统密码应用基本要求》

2.《信息系统密码应用高风险判定指引》

3.《商用密码应用安全性评估量化评估规则》



4.GM/T 0115《信息系统密码应用测评要求》

5. GM/T 0116《信息系统密码应用测评过程指南》

三、商用密码应用安全性评估标准简介

风险判定及量化评估依据 —《信息系统密码应用高风险判定指引》《商用密码应用安全性评估量化评估规则》

本文件依据GB/T 39786《信息安全技术 信息系统密码应用基本要求》有关条款，给出了信息系统密码应用过程中可能存在的高风险安全问题。适用于指导、规范信息系统密码应用的规划、建设、运行及测评。

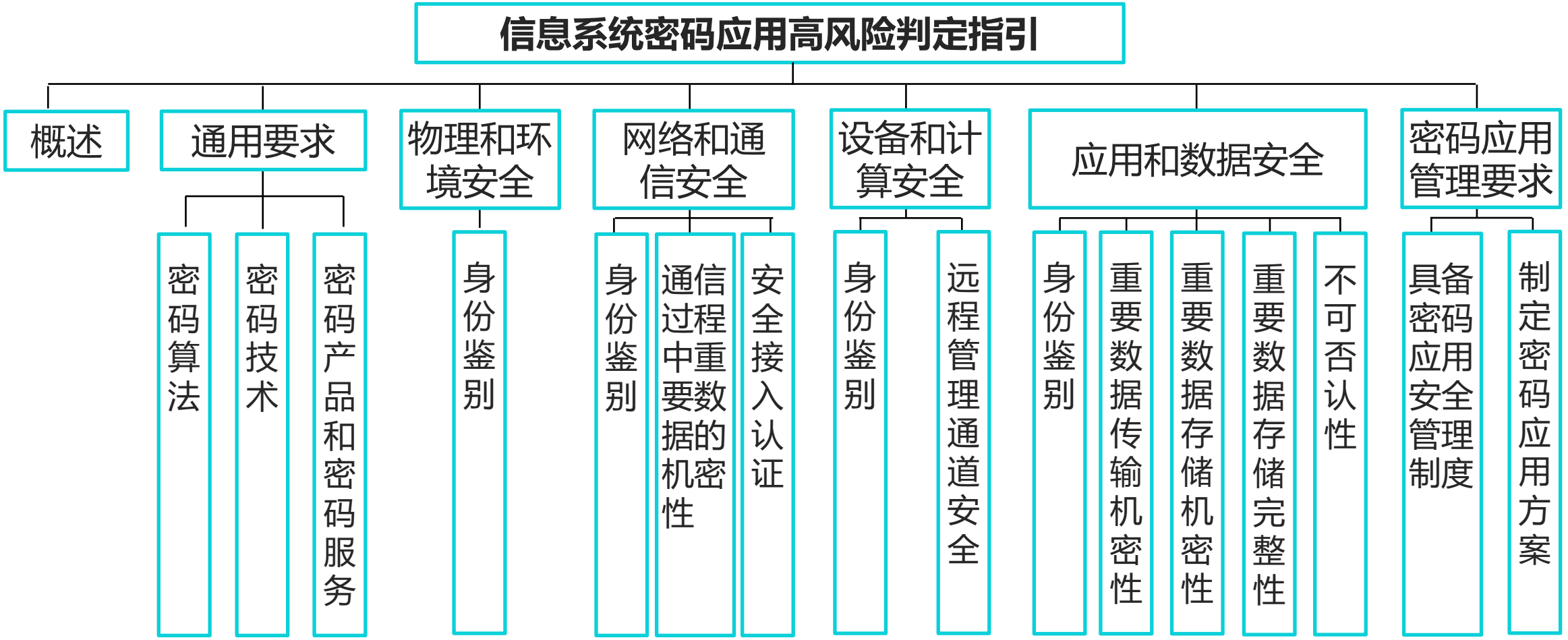
本文件依据 GB/T 39786《信息安全技术 信息系统密码应用基本要求》和GM/T 0115-2021《信息系统密码应用测评要求》，对信息系统的密码应用情况给出定量评估结果。适用于指导、规范信息系统密码应用的规划、建设、运行及测评。

三、商用密码应用安全性评估标准简介

《信息系统密码应用高风险判定指引》内容目次

三、商用密码应用安全性评估标准简介

《信息系统密码应用高风险判定指引》总体框架



《信息系统密码应用高风险判定指引》概述

本文件中判定内容由指标要求、适用范围、 安全问题、 可能的缓解措施和风险评价构成。其中，指标要求源自 GB/T 39786 的部分指标，对于本文件未覆盖的其他指标，仍需核查本文件第 5 章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题是否存在。

由于信息系统密码应用场景的复杂性，本文件无法涵盖密码应用的所有高风险安全问题， 对于本文件未涉及但确实可能会对信息系统造成严重安全隐患的安全问题， 应结合信息系统的实际情况对相关安全问题所引发的风险等级做出客观判断。 在某些情况下，受限于具体场景的安全需求和各项条件，本文件给出的安全问题也可能不会导致信息系统面临较高安全风险，在信息系统密码应用的规划、建设、运行及测评时应结合具体场景进行合理判定。

三、商用密码应用安全性评估标准简介

《信息系统密码应用高风险判定指引》— 通用要求

通用要求： **1、密码算法** **2、密码技术** **3、密码产品和密码服务**

	密码算法	密码技术	密码产品和密码服务
a) 指标要求	信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。	信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。	信息系统中使用的密码产品、密码服务应符合法律法规的相关要求。
b) 适用范围	所有级别信息系统。		
c) 安全问题	1) 采用存在安全问题或安全强度不足的密码算法对重要数据进行保护，如MD5、 DES、SHA-1、 RSA（不足2048比特）等密码算法； 2) 采用安全性未知的密码算法，如自行设计的密码算法、 经认证的密码产品中未经安全性论证的密码算法。	1) 采用存在缺陷或有安全问题警示的密码技术，如SSH 1.0、 SSL 2.0、 SSL 3.0、TLS 1.0等； 2) 采用安全性未知的密码技术，如未经安全性论证的自行设计的密码通信协议、 经认证的密码产品中未经安全性论证的密码通信协议等。	1) 采用自实现且未提供安全性证据的密码产品； 2) 采用存在高危安全漏洞的密码产品，如存在Heartbleed漏洞的OpenSSL产品； 3) 密码产品的使用不满足其安全运行的前提条件，如其安全策略或使用手册说明的部署条件； 4) 选用的密码服务提供商不具有相关资质； 5) 存在密钥管理相关安全问题（参见附录A） 。
d) 可能的缓解措施	无		
e) 风险评价：	上述安全问题一旦被威胁利用后， 可能会导致信息系统面临高等级安全风险。		

《信息系统密码应用高风险判定指引》— 物理和环境安全

物理和环境安全：　1、身份鉴别

身份鉴别	
a) 指标要求	采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性。
b) 适用范围	第二级及以上级别信息系统。
c) 安全问题	1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题； 2) 未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对重要区域进入人员进行身份鉴别； 3) 针对人员身份真实性的密码技术实现机制不正确或无效。
d) 可能的缓解措施	1) 基于生物识别技术（如指纹等） 对进入人员进行身份鉴别； 2) 重要区域出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控等。
e) 风险评价：	1) 若未采用密码技术对重要区域进入人员进行身份鉴别， 但基于生物识别技术（如指纹等）保证了人员身份真实性，可酌情降低风险等级； 2) 若未采用密码技术对重要区域进入人员进行身份鉴别，或针对人员身份真实性的密码技术实现机制不正确或无效，但在重要区域出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控等，可酌情降低风险等级。

三、商用密码应用安全性评估标准简介

《信息系统密码应用高风险判定指引》— 网络和通信安全

	身份鉴别	通信过程中重要数据的机密性	安全接入认证
a) 指标要求	采用密码技术对通信实体进行身份鉴别（第二级到第三级） /双向身份鉴别（第四级），保证通信实体身份的真实性。	采用密码技术保证通信过程中重要数据的机密性。	采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性。
b) 适用范围	第二级及以上级别信息系统。		第四级信息系统。
c) 安全问题	1) 存在第 5 章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题； 2) 信息系统与网络边界外建立网络通信信道时，未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对通信实体进行身份鉴别（第二级和第三级） /双向身份鉴别（第四级） ； 3) 通信实体身份真实性实现机制不正确或无效； 4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。	1) 存在第 5 章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题； 2) 信息系统与网络边界外的通信实体建立网络通信信道时，未采用密码技术的加解密功能对通信过程中重要数据进行机密性保护； 3) 敏感信息或通信报文机密性实现机制不正确或无效； 4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。	1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题； 2) 未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对从外部连接到内部网络的设备进行接入 认证； 3) 安全接入认证的实现机制不正确或无效； 4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。

三、商用密码应用安全性评估标准简介

《信息系统密码应用高风险判定指引》— 网络和通信安全

网络和通信安全： **1、身份鉴别** **2、通信过程中重要数据的机密性** **3、安全接入认证**

	身份鉴别	通信过程中重要数据的机密性	安全接入认证
d) 可能的缓解措施	无	在“应用和数据安全” 层面针对重要数据传输采用符合要求的密码技术进行机密性保护	无
e) 风险评价	上述安全问题一旦被威胁利用后， 可能会导致信息系统面临高等级安全风险。	若未采用密码技术的加解密功能对通信过程中敏感信息或通信报文进行机密性保护，或机密性实现机制不正确或无效，但在“应用和数据安全”层面针对重要数据传输采用符合要求的密码技术进行机密性保护，可视为等效措施。	上述安全问题一旦被威胁利用后， 可能会导致信息系统面临高等级安全风险。

《信息系统密码应用高风险判定指引》— 设备和计算安全

设备和计算安全：　1、身份鉴别　2、远程管理通道安全

	身份鉴别	远程管理通道安全
a) 指标要求	采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。	远程管理设备时，采用密码技术建立安全的信息传输通道。
b) 适用范围	第二级及以上级别信息系统。	第三级及以上级别信息系统。
c) 安全问题	1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题； 2) 未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对登录设备的用户进行身份鉴别； 3) 用户身份真实性的密码技术实现机制不正确或无效。	1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题； 2) 远程管理设备时， 未采用密码技术建立安全的信息传输通道； 3) 信息传输通道所采用密码技术实现机制不正确或无效； 4) 通过不可控网络环境进行远程管理，且鉴别数据以明文形式传输。
d) 可能的缓解措施	基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性。	1) 搭建了与业务网络隔离的管理网络进行远程管理； 2) 在“网络和通信安全” 层面使用SSL VPN网关/IPSec VPN网关等建立集中管理通道，且使 用的密码技术符合要求。
e) 风险评价：	若未采用密码技术对登录设备的用户进行身份鉴别，或用户身份真实性的密码技术实现机制不正确或无效，但基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性，可酌情降低风险等级。	1) 若远程管理设备时未采用密码技术建立安全的信息传输通道，或远程管理信道所采用密码技术实现机制不正确或无效，但通过搭建与业务网络隔离的管理网络进行远程管理，可视为等效措施； 2) 若在“网络和通信安全” 层面使用SSL VPN网关/IPSec VPN网关等建立集中管理通道，且使用的密码技术符合要求，可视为等效措施。

三、商用密码应用安全性评估标准简介

《信息系统密码应用高风险判定指引》— 应用和数据安全

应用和数据安全：1、身份鉴别　　2、重要数据传输机密性　　3、重要数据存储机密性

4、重要数据存储完整性　　5、不可否认性

	身份鉴别	重要数据传输机密性
a) 指标要求	采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。	采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。
b) 适用范围	第二级及以上级别信息系统。	
c) 安全问题	1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题； 2) 未采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对登录用户进行身份鉴别； 3) 用户身份真实性的密码技术实现机制不正确或无效； 4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。	1）同。 2）未采用密码技术的加解密功能对重要数据在传输过程中进行机密性保护； 3）重要数据传输机密性实现机制不正确或无效； 4) 同。
d) 可能的缓解措施	基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性。	在“网络和通信安全” 层面采用符合要求的密码技术保证重要数据在传输过程中的机密性。
e) 风险评价：	若未采用密码技术对登录用户进行身份鉴别， 或用户身份真实性的密码技术实现机制不正确或无效，但基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性， 可酌情降低风险等级。	若未采用密码技术的加解密功能对重要数据在传输过程中进行机密性保护，或重要数据机密性实现机制不正确或无效，但在“网络和通信安全”层面采用符合要求的密码技术保证重要数据在传输过程中的机密性，可酌情降低风险等级。

三、商用密码应用安全性评估标准简介

《信息系统密码应用高风险判定指引》— 应用和数据安全

应用和数据安全：1、身份鉴别　　2、重要数据传输机密性　　3、重要数据存储机密性

4、重要数据存储完整性　　5、不可否认性

	重要数据存储机密性	重要数据存储完整性
a) 指标要求	采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。	采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。
b) 适用范围	第二级及以上级别信息系统。	
c) 安全问题	1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题； 2) 未采用密码技术的加解密功能对重要数据在存储过程中进行机密性保护； 3) 重要数据存储机密性实现机制不正确或无效； 4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。	1) 同。 2) 未采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对重要数据在存储过程中进行完整性保护； 3) 重要数据存储完整性实现机制不正确或无效； 4) 同。
d) 可能的缓解措施	无	应用系统具有符合要求的身份鉴别措施，保证只有授权人员才能访问应用系统的重要数据，且定期对重要数据进行备份。
e) 风险评价：	上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。	若未采用密码技术保证信息系统应用的重要数据在存储过程中的完整性，或重要数据存储完整性实现机制不正确或无效，但应用系统具有符合要求的身份鉴别措施，保证只有授权人员才能访问应用系统的重要数据，且定期对重要数据进行备份，可酌情降低风险等级。

《信息系统密码应用高风险判定指引》— 应用和数据安全

应用和数据安全 1、身份鉴别 2、重要数据传输机密性 3、重要数据存储机密性 4、重要数据存储完整性 5、不可否认性

不可否认性	
a) 指标要求	在可能涉及法律责任认定的应用中，采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。
b) 适用范围	第三级及以上级别信息系统。
c) 安全问题	1) 存在第5章通用要求中密码算法、密码技术、密码产品和密码服务相关安全问题； 2) 在可能涉及法律责任认定的应用中，未采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为和接收行为实现不可否认性； 3) 不可否认性的密码技术实现机制不正确或无效； 4) 采用的密码产品未获得商用密码认证机构颁发的商用密码产品认证证书（适用时）。
d) 可能的缓解措施	无。
e) 风险评价：	上述安全问题一旦被威胁利用后， 可能会导致信息系统面临高等级安全风险。

《信息系统密码应用高风险判定指引》— 密码应用管理要求

密码应用管理要求： 1、具备密码应用安全管理制度

2、制定密码应用方案

	具备密码应用安全管理制度	制定密码应用方案
a) 指标要求	具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。	依据密码相关标准和密码应用需求，制定密码应用方案。
b) 适用范围	第二级及以上级别信息系统。	
c) 安全问题	未建立任何与密码应用安全管理活动相关的管理制度，或相关管理制度不适用于当前被测信息系统。	对于新建信息系统，在规划阶段未制定密码应用方案或密码应用方案未通过评审。
d) 可能的缓解措施	无	
e) 风险评价：	上述安全问题一旦被威胁利用后， 可能会导致信息系统面临高等级安全风险。	

三、商用密码应用安全性评估标准简介

《商用密码应用安全性评估量化评估规则》内容目次

- 1.范围
- 2.规范性引用文件
- 3.原则
- 4.量化评估框架
- 5.量化规则
- 6.整体结论判定

三、商用密码应用安全性评估标准简介

《商用密码应用安全性评估量化评估规则》原则

本文件按如下原则设计量化评估规则：

1. 遵循法律法规和最新相关指导性文件的总体要求；
2. 遵循 GB/T 39786 和 GM/T 0115-2021；
3. 鼓励使用密码技术；
4. 特别鼓励使用合规的密码算法/技术/产品/服务；
5. 优先在网络和通信安全层面、应用和数据安全层面进行密码技术应用。

三、商用密码应用安全性评估标准简介

《商用密码应用安全性评估量化评估规则》量化评估框架

参考 GM/T 0115-2021，本规则从三个方面进行量化评估：

量化评估框架

密码使用安全	密码技术是否被正确、有效使用，以满足信息系统的安全需求， 有效提供机密性、完整性、真实性和不可否认性的保护；
密钥管理安全	密钥管理的全生命周期是否安全，用于密码计算或密钥管理的密码产品/密码服务是否安全。
密码算法 / 技术安全	信息系统中使用的密码算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，信息系统中使用的密码技术是否遵循密码相关国家标准和行业标准或经国家密码管理部门核准。

《商用密码应用安全性评估量化评估规则》量化规则

1、各测评对象的测评结果量化规则

密码应用技术要求中，第i 个安全层面的第 j 测评单元的第k 测评对象Ti,j,k ，其量化评估结果Si,j,k ∈ {0, 0.25, 0.5, 1}，其中 0 表示不符合， 1 表示符合，其它表示部分符合。Si,j,k的取值分别见表1。通用要求和密码应用技术要求各安全层面的“密码服务”和“密码产品”指标不单独评价。

密码应用管理要求不针对各个测评对象的测评结果进行量化评估。

符合情况	涉及情况			示例	分值 $S_{i,j,k}$
	密码使用安全 *D*	密码算法/技术合规性 *A*	密钥管理安全 *K*		
符合	√	√	√	全部符合相关的要求	1
部分符合	√	×	√	使用认证合格的密码产品，但使用的密码算法/技术不合规	0.5
	√	√	×	使用未经认证或不满足安全等级要求的密码产品，但使用的密码算法/技术合规	
	√	×	×	使用未经认证或不满足安全等级要求的密码产品，且使用的密码算法/技术不合规	0.25
不符合	×	/	/	使用的密码技术无法满足信息系统的安全需求，或未使用密码技术等	0

表2 测评指标权重表

《商用密码应用安全性评估量化评估规则》量化规则

2、测评单元的测评结果量化规则

第 i 个安全层面的第 j 测评单元Ui,j 的量化评估结果Si,j 为该测评单元内所有ni,j 个测评对象测评结果的算术平均值（四舍五入，取小数点后 4 位），即：

$$S_{i,j} = \frac{\sum_{1 \le k \le n_{i,j}} S_{i,j,k}}{n_{i,j}}$$

密码应用管理要求中，第i 个安全层面的第 j 测评单元，根据 GM/T 0115-2021 给出判定结果Si,j，符合为 1 分，不符合为 0 分，部分符合为 0.5 分。

序号	测评单元			安全层面权重（w_i）	指标权重 w_{ij}			
					第一级	第二级	第三级	第四级
1	密码技术应用要求	物理和环境安全	身份鉴别	10	0.4	0.7	1	1
2			电子门禁记录数据存储完整性		0.4	0.4	0.7	1
3			视频记录数据存储完整性		/	/	0.7	1
4		网络和通信安全	身份鉴别	15	0.4	0.7	1	1
5			通信数据完整性		0.4	0.4	0.7	1
6			通信过程中重要数据的机密性		0.4	0.7	1	1
7			网络边界访问控制信息的完整性		0.4	0.4	0.7	1
8			安全接入认证		/	/	0.4	0.7
9		设备和计算安全	身份鉴别	15	0.4	0.7	1	1
10			远程管理通道安全		/	/	1	1
11			系统资源访问控制信息完整性		0.4	0.4	0.7	1
12			重要信息资源安全标记完整性		/	/	0.7	1
13			日志记录完整性		0.4	0.4	0.7	1

表2 测评指标权重表

《商用密码应用安全性评估量化评估规则》量化规则

3、安全层面的测评结果量化规则

本文件为每个安全层面分配了相应的权重wi，如表 2 所示。量化评估结果 S 为所有 n个安全层面测评结果 S_i 的加权平均值（四舍五入，取小数点后 2 位），即：

$$S_i = \frac{\sum_{1\le j\le n_i} w_{i,j} S_{i,j}}{\sum_{1\le j\le n_i} w_{i,j}}$$

若某测评指标不适用，则不参与量化评估过程。

14			重要可执行程序完整性、重要可执行程序来源真实性		/	/	0.7	1
15		应用和数据安全	身份鉴别	30	0.4	0.7	1	1
16			访问控制信息完整性		0.4	0.4	0.7	1
17			重要信息资源安全标记完整性		/	/	0.7	1
18			重要数据传输机密性		0.4	0.7	1	1
19			重要数据存储机密性		0.4	0.7	1	1
20			重要数据传输完整性		0.4	0.7	1	1
21			重要数据存储完整性		0.4	0.7	1	1
22			不可否认性		/	/	1	1
23	安全管理	管理制度	具备密码应用安全管理制度	8	1	1	1	1
24			密钥管理规则		0.7	0.7	0.7	0.7
25			建立操作规程		/	0.7	0.7	0.7
26			定期修订安全管理制度		/	/	0.7	0.7

表2 测评指标权重表

《商用密码应用安全性评估量化评估规则》量化规则

4、整体测评结果量化规则

本文件为每个测评单元分配了相应的权重wi,j，如表 2 所示。第i 个安全层面 Li 的量化评估结果Si 为该安全层面内所有ni 个适用测评单元测评结果Si,j 的加权平均值（四舍五入，取小数点后 4 位），即：

$$S=\frac{\sum_{1\le i\le n} w_i \cdot S_i}{\sum_{1\le i\le n} w_i}\times 100$$

本文件为每个安全层面分配了相应的权重wi，如表 2 所示。量化评估结果 S 为所有 n个安全层面测评结果 Si 的加权平均值（四舍五入，取小数点后 2 位），即：

27			明确管理制度发布流程		/	/	0.7	0.7
28			制度执行过程记录留存		/	/	0.7	0.7
29		人员管理	了解并遵守密码相关法律法规和密码管理制度	8	0.7	0.7	0.7	0.7
30			建立密码应用岗位责任制度		/	1	1	1
31			建立上岗人员培训制度		/	0.7	0.7	0.7
32			定期进行安全岗位人员考核		/	/	0.7	0.7
33			建立关键岗位人员保密制度和调离制度		0.7	0.7	0.7	0.7
34		建设运行	制定密码应用方案	8	1	1	1	1
35			制定密钥安全管理策略		1	1	1	1
36			制定实施方案		0.7	0.7	0.7	0.7
37			投入运行前进行密码应用安全性评估		1	1	1	1
38			定期开展密码应用		/	/	0.7	0.7

表2 测评指标权重表

《商用密码应用安全性评估量化评估规则》整体结论判定

整体量化评估结果S为100分，则判定被测信息系统符合GB/T 39786相应等级要求；S 低于 100 分、不低于阈值，且经风险评估发现没有高风险，则判定被测信息系统基本符合GB/T 39786 相应等级要求；否则，判定被测信息系统不符合 GB/T 39786 相应等级要求。

三、商用密码应用安全性评估标准简介

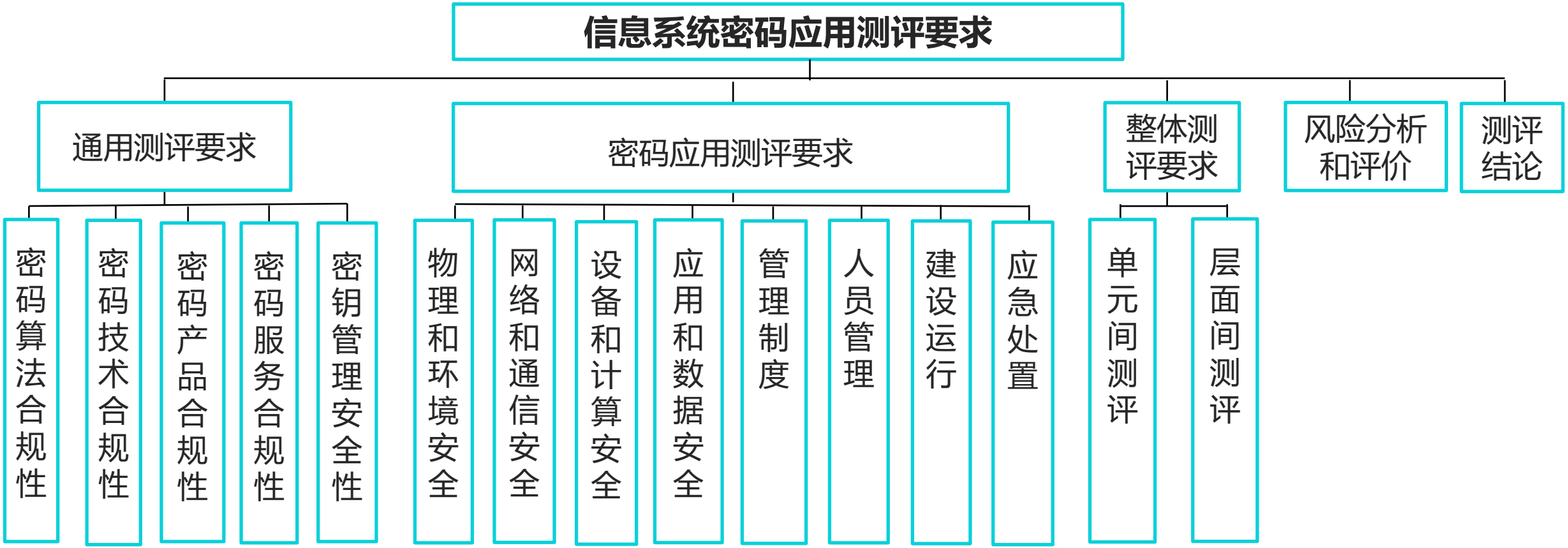
密码应用测评要求依据 —《信息系统密码应用测评要求》

本文件规定了信息系统不同等级密码应用的测评要求，从密码算法合规性、密码技术合规性、密码产品合规性、密码服务合规性以及密钥管理安全性等方面，提出了第一级到第五级的密码应用通用测评要求；从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等**四个技术层面**提出了第一级到第四级的密码应用技术测评要求；从管理制度、人员管理、建设运行和应急处置等**四个管理方面**提出了第一级到第四级的密码应用管理测评要求，并给出了整体测评、风险分析和评价、测评结论等测评环节的要求。

《信息系统密码应用测评要求》内容目次

三、商用密码应用安全性评估标准简介

《信息系统密码应用测评要求》总体框架



三、商用密码应用安全性评估标准简介

通用测评要求

通用测评要求： 1、密码算法合规性　2、密码技术合规性　3、密码产品合规性
4、密码服务合规性　5、密钥管理安全性

	密码算法合规性	密码技术合规性
a) 测评指标	•信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求（第一级到第五级）。	•信息系统中使用的密码技术应遵循密码相关国家标准和行业标准（第一级到第五级）。
b) 测评对象	信息系统中使用的密码产品、密码服务以及密码算法实现。	信息系统中的密码产品、密码服务以及密码技术实现。
c) 测评实施	了解系统使用的算法名称、用途、何处使用、执行设备及其实现方式（软件、硬件或固件），核查密码算法是否以国家标准或行业标准形式发布，或取得国家密码管理部门同意使用的证明文件。	核查系统所使用的密码技术是否以国家标准或行业标准形式发布，或取得国家密码管理部门同意使用的证明文件。
d) 结果判定	本单元测评指标不单独判定符合性。	

三、商用密码应用安全性评估标准简介

通用测评要求

通用测评要求： 1、密码算法合规性　2、密码技术合规性　3、密码产品合规性
4、密码服务合规性　5、密钥管理安全性

	密码产品合规性	密码服务合规性
a) 测评指标	信息系统中使用的密码产品应符合法律法规和密码相关国家标准和行业标准的要求（第一级到第五级）。 若采用的密码产品遵循密码模块相关标准，则应 •达到密码模块安全等级一级及以上安全要求（第二级）。 •达到密码模块安全等级二级及以上安全要求（第三级）。 •达到密码模块安全等级三级及以上安全要求（第四级）。	•信息系统中使用的密码服务应符合法律法规和密码相关国家标准和行业标准的要求（第一级到第五级）。
b) 测评对象	信息系统中的密码产品。	信息系统中的密码服务。
c) 测评实施	了解信息系统中密码产品的型号和版本等配置信息，核查密码产品是否经商用密码认证机构认证合格，并核查密码产品的使用是否满足其安全运行的条件，如其安全策略或使用手册说明的部署条件；遵循了密码模块相关标准的密码产品，还要核查其是否满足密码模块相应安全等级及以上安全要求。	核查信息系统中密码服务是否经商用密码认证机构认证合格或取得国家密码管理部门同意使用的证明文件。
d) 结果判定	本单元测评指标不单独判定符合性。	

三、商用密码应用安全性评估标准简介

通用测评要求

通用测评要求： **1、密码算法合规性** **2、密码技术合规性** **3、密码产品合规性** **4、密码服务合规性** **5、密钥管理安全性**

密钥管理安全性	
a) 测评指标	•信息系统的密钥管理采用的密码产品、密码服务应符合法律法规和密码相关国家标准和行业标准的要求（第一级到第五级）。 •信息系统的密钥管理应符合密码相关国家标准和行业标准的要求（第一级到第五级）。
b) 测评对象	密钥管理采用的密码产品、密码服务及密钥管理实现。
c) 测评实施	•核查密钥管理使用的密码产品、密码服务是否满足第5章通用测评要求中“密码产品合规性”“密码服务合规性”的要求。 •核查信息系统中密钥管理安全性实现技术是否正确有效。例如：非公开密钥是否不能被非授权的访问、使用、泄露、修改和替换，公开密钥是否不能被非授权的修改和替换。
d) 结果判定	本单元测评指标不单独判定符合性。

密码应用测评要求 — 物理和环境安全

物理和环境安全：1、身份鉴别 2、电子门禁记录数据存储完整性 3、视频监控记录数据存储完整性

	身份鉴别	电子门禁记录数据存储完整性	视频监控记录数据存储完整性
a) 测评指标	采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性。 （第一级到第四级）	采用密码技术保证电子门禁系统进出记录数据的存储完整性。 （第一级到第四级）	采用密码技术保证视频监控音像记录数据的存储完整性。 （第三级到第四级）
b) 测评对象	信息系统所在机房等重要区域及其电子门禁系统。		信息系统所在机房等重要区域及其视频监控系统。
c) 测评实施	1）核查是否符合第5章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求； 2）核查是否符合第5章通用测评要求中“密码产品合规性” “密码服务合规性”和“密钥管理安全性”的测评要求； 3）核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对电子门禁系统进出记录数据进行存储完整性保护，并验证完整性保护机制是否正确和有效。		
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施3）为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。		

密码应用测评要求 — 网络和通信安全

网络和通信安全：1、身份鉴别　2、通信数据完整性　3、通信过程中重要数据的机密性
4、网络边界访问控制信息的完整性　5、安全接入认证

	身份鉴别	通信数据完整性
a) 测评指标	• 采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。（第一级到第三级） •采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性。（第四级）	•采用密码技术保证通信过程中数据的完整性。（第一级到第四级）
b) 测评对象	信息系统与网络边界外建立的网络通信信道， 以及提供通信保护功能的设备或组件、密码产品。	
c) 测评实施	1）核查是否符合第5章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求； 2）核查是否符合第5章通用测评要求中“密码产品合规性” “密码服务合规性”和“密钥管理安全性”的测评要求； 3）核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对通信实体进行身份鉴别（第一级到第三级）/双向身份鉴别（第四级），并验证通信实体身份真实性实现机制是否正确和有效。	1）2）同左 3）核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对通信过程中的数据进行完整性保护，并验证通信数据完整性保护机制是否正确和有效。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施3）为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 网络和通信安全

网络和通信安全：1、身份鉴别　2、通信数据完整性　3、通信过程中重要数据的机密性
4、网络边界访问控制信息的完整性　5、安全接入认证

	通信过程中重要数据的机密性	网络边界访问控制信息的完整性	安全接入认证
a) 测评指标	采用密码技术保证通信过程中重要数据的机密性。（第一级到第四级）	采用密码技术保证网络边界访问控制信息的完整性。（第一级到第四级）	采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入设备身份的真实性。（第三级到第四级）
b) 测评对象	信息系统与网络边界外建立的网络通信信道，以及提供网络边界访问控制功能的设备或组件、密码产品。		信息系统内部网络，以及提供设备入网接入认证功能的设备或组件、密码产品。
c) 测评实施	1）核查是否符合第5章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求； 2）核查是否符合第5章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求； 3）核查是否采用密码技术的加解密功能对通信过程中敏感信息或通信报文进行机密性保护，并验证敏感信息或通信报文机密性保护机制是否正确和有效。	1）2）同左 核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对网络边界访问控制信息进行完整性保护，并验证网络边界访问控制信息完整性保护机制是否正确和有效。	
d) 结果判定	同前		

密码应用测评要求 — 设备和计算安全

设备和计算安全：

1、身份鉴别
2、远程管理通道安全
3、系统资源访问控制信息完整性
4、重要信息资源安全标记完整性
5、日志记录完整性
6、重要可执行程序完整性和重要可执行程序来源真实性

	身份鉴别	远程管理通道安全
a) 测评指标	采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。（第一级到第四级）	远程管理设备时，采用密码技术建立安全的信息传输通道。（第三级到第四级）
b) 测评对象	通用设备、网络及安全设备、密码设备、 各类虚拟设备，以及提供身份鉴别功能的密码产品。	
c) 测评实施	1）核查是否符合第5章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求； 2）核查是否符合第5章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求； 3）核查是否采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备操作人员等登录设备的用户进行身份鉴别，并验证登录设备的用户身份真实性实现机制是否正确和有效。	1）2）同左 3）核查远程管理时是否采用密码技术建立安全的信息传输通道，包括身份鉴别、传输数据机密性和完整性保护，并验证远程管理信道所采用的密码技术实现机制是否正确和有效。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施3）为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 设备和计算安全

设备和计算安全：

1、身份鉴别
2、远程管理通道安全
3、系统资源访问控制信息完整性
4、重要信息资源安全标记完整性
5、日志记录完整性
6、重要可执行程序完整性和重要可执行程序来源真实性

	系统资源访问控制信息完整性	重要信息资源安全标记完整性
a) 测评指标	采用密码技术保证系统资源访问控制信息的完整性。（第一级到第四级）	采用密码技术保证设备中的重要信息资源安全标记的完整性。（第三级到第四级）
b) 测评对象	通用设备、网络及安全设备、密码设备、 各类虚拟设备，以及提供完整性保护功能的密码产品。	
c) 测评实施	1）核查是否符合第5章通用测评要求中“密码算法合规性”和“密码技术合规性” 的测评要求； 2）核查是否符合第5章通用测评要求中“密码产品合规性” “密码服务合规性”和“密钥管理安全性”的测评要求； 3）核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备上系统资源访问控制信息进行完整性保护，并验证系统资源访问控制信息完整性保护机制是否正确和有效。	1）2）同左 3）核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备中的重要信息资源安全标记进行完整性保护，并验证安全标记完整性保护机制是否正确和有效。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施3）为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 设备和计算安全

设备和计算安全：

1、身份鉴别
2、远程管理通道安全
3、系统资源访问控制信息完整性
4、重要信息资源安全标记完整性
5、日志记录完整性
6、重要可执行程序完整性和重要可执行程序来源真实性

	日志记录完整性	重要可执行程序完整性和重要可执行程序来源真实性
a) 测评指标	采用密码技术保证日志记录的完整性。 （第一级到第四级）	采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。 （第三级到第四级）
b) 测评对象	通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护功能的密码产品。	通用设备、网络及安全设备、密码设备、各类虚拟设备，以及提供完整性保护和来源真实性功能的密码产品。
c) 测评实施	1）核查是否符合第5章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求； 2）核查是否符合第5章通用测评要求中“密码产品合规性” “密码服务合规性”和“密钥管理安全性”的测评要求； 3）核查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备运行的日志记录进行完整性保护，并验证日志记录完整性保护机制是否正确和有效。	1）2）同左 3）核查是否采用密码技术对重要可执行程序进行完整性保护并实现其来源的真实性保护， 并验证重要可执行程序完整性保护机制和其来源真实性实现机制是否正确和有效。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施 2）为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 应用和数据安全

应用和数据安全：

1、身份鉴别
2、访问控制信息完整性
3、重要信息资源安全标记完整性
4、重要数据传输机密性
5、重要数据存储机密性
6、重要数据传输完整性
7、重要数据存储完整性
8、不可否认性

	身份鉴别	访问控制信息完整性
a) 测评指标	采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。（第一级到第四级）	采用密码技术保证信息系统应用的访问控制信息的完整性。（第一级到第四级）
b) 测评对象	业务应用，以及提供身份鉴别功能的密码产品。	业务应用，以及提供完整性保护功能的密码产品。
c) 测评实施	1）核查是否符合第5章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求； 2）核查是否符合第5章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求； 3）核查应用系统是否采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对登录用户进行身份鉴别，并验证应用系统用户身份真实性实现机制是否正确和有效。	1）2）同左 3）核查信息系统是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对应用的访问控制信息进行完整性保护，并验证应用的访问控制信息完整性保护机制是否正确和有效。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施3）为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 应用和数据安全

应用和数据安全：

1、身份鉴别
2、访问控制信息完整性
3、重要信息资源安全标记完整性
4、重要数据传输机密性
5、重要数据存储机密性
6、重要数据传输完整性
7、重要数据存储完整性
8、不可否认性

	重要信息资源安全标记完整性	重要数据传输机密性
a) 测评指标	采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。（第三级到第四级）	采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。（第一级到第四级）
b) 测评对象	业务应用，以及提供完整性保护功能的密码产品。	业务应用，以及提供机密性保护功能的密码产品。
c) 测评实施	1）核查是否符合第5章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求； 2）核查是否符合第5章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求； 3）核查应用系统是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对应用的重要信息资源安全标记进行完整性保护，并验证安全标记完整性保护机制是否正确和有效。	1）2）同左 3）核查应用系统是否采用密码技术的加解密功能对重要数据在传输过程中进行机密性保护，并验证传输数据机密性保护机制是否正确和有效。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施3）为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 应用和数据安全

应用和数据安全：

1、身份鉴别
2、访问控制信息完整性
3、重要信息资源安全标记完整性
4、重要数据传输机密性
5、重要数据存储机密性
6、重要数据传输完整性
7、重要数据存储完整性
8、不可否认性

	重要数据存储机密性	重要数据传输完整性
a) 测评指标	采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。（第一级到第四级）	采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。（第一级到第四级）
b) 测评对象	业务应用，以及提供机密性保护功能的密码产品。	业务应用，以及提供完整性保护功能的密码产品。
c) 测评实施	1)核查是否符合第5章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求； 2)核查是否符合第5章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求； 3)核查应用系统是否采用密码技术的加解密功能对重要数据在存储过程中进行机密性保护，并验证存储数据机密性保护机制是否正确和有效。	1）2）同左 3)核查应用系统是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对重要数据在传输过程中进行完整性保护，并验证传输数据完整性保护机制是否正确和有效。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施3）为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 应用和数据安全

应用和数据安全：

1、身份鉴别
2、访问控制信息完整性
3、重要信息资源安全标记完整性
4、重要数据传输机密性
5、重要数据存储机密性
6、重要数据传输完整性
7、重要数据存储完整性
8、不可否认性

	重要数据存储完整性	不可否认性
a) 测评指标	采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。（第一级到第四级）	在可能涉及法律责任认定的应用中，采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。（第三级到第四级）
b) 测评对象	业务应用，以及提供完整性保护功能的密码产品。	业务应用，以及提供不可否认性功能的密码产品。
c) 测评实施	1）核查是否符合第5章通用测评要求中“密码算法合规性”和“密码技术合规性”的测评要求； 2）核查是否符合第5章通用测评要求中“密码产品合规性”“密码服务合规性”和“密钥管理安全性”的测评要求； 3）核查应用系统是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对重要数据在存储过程中进行完整性保护，并验证存储数据完整性保护机制是否正确和有效。	1）2）同 3)核查应用系统是否采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为和接收行为实现不可否认性，并验证不可否认性实现机制是否正确和有效。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；如果测评实施3）为否，则不符合本单元的测评指标要求；否则，部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 管理制度

管理制度：

1、具备密码应用安全管理制度

2、密钥管理规则

3、建立操作规程

4、定期修订安全管理制度

5、明确管理制度发布流程

6、制度执行过程记录留存

	具备密码应用安全管理制度	密钥管理规则
a) 测评指标	具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。（第一级到第四级）	根据密码应用方案建立相应密钥管理规则。（第一级到第四级）
b) 测评对象	安全管理制度类文档。	密码应用方案、 密钥管理制度及策略类文档。
c) 测评实施	核查各项安全管理制度是否包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。	核查是否有通过评估的密码应用方案，并核查是否根据密码应用方案建立相应密钥管理规则（如密钥管理制度及策略类文档中的密钥全生存周期的安全性保护相关内容）且对密钥管理规则进行评审，以及核查信息系统中密钥是否按照密钥管理规则进行生存周期的管理。
d) 结果判定	针对单个测评对象，如果以上测评实施内容为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 管理制度

管理制度：

1、具备密码应用安全管理制度

2、密钥管理规则

3、建立操作规程

4、定期修订安全管理制度

5、明确管理制度发布流程

6、制度执行过程记录留存

	建立操作规程	定期修订安全管理制度
a) 测评指标	对管理人员或操作人员执行的日常管理操作建立操作规程。（第二级到第四级）	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。（第三级到第四级）
b) 测评对象	操作规程类文档。	安全管理制度类文档、操作规程类文档、记录表单类文档
c) 测评实施	核查是否对密码相关管理人员或操作人员的日常管理操作建立操作规程。	核查是否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；对经论证和审定后存在不足或需要改进的密码应用安全管理制度和操作规程，核查是否具有修订记录。
d) 结果判定	针对单个测评对象，如果以上测评实施内容为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 管理制度

管理制度：

1、具备密码应用安全管理制度

2、密钥管理规则

3、建立操作规程

4、定期修订安全管理制度

5、明确管理制度发布流程

6、制度执行过程记录留存

	明确管理制度发布流程	制度执行过程记录留存
a) 测评指标	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。（第三级到第四级）	具有密码应用操作规程的相关执行记录并妥善保存。（第三级到第四级）
b) 测评对象	安全管理制度类文档、操作规程类文档、记录表单类文档。	安全管理制度类文档、记录表单类文档。
c) 测评实施	核查相关密码应用安全管理制度和操作规程是否具有相应明确的发布流程和版本控制。	核查是否具有密码应用操作规程执行过程中留存的相关执行记录文件。
d) 结果判定	针对单个测评对象，如果以上测评实施内容为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 人员管理

人员管理：

1、了解并遵守密码相关法律法规和密码管理制度
2、建立密码应用岗位责任制度
3、建立上岗人员培训制度
4、定期进行安全岗位人员考核
5、建立关键岗位人员保密制度和调离制度

了解并遵守密码相关法律法规和密码管理制度	
a) 测评指标	相关人员了解并遵守密码相关法律法规、密码应用安全管理制度。（第一级到第四级）
b) 测评对象	系统相关人员（包括系统负责人、安全主管、密钥管理员、密码审计员、密码操作员等）。
c) 测评实施	核查系统相关人员是否了解并遵守密码相关法律法规和密码应用安全管理制度。
d) 结果判定	针对单个测评对象，如果以上相应等级的测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

密码应用测评要求 — 人员管理

人员管理：

1、了解并遵守密码相关法律法规和密码管理制度

2、建立密码应用岗位责任制度

3、建立上岗人员培训制度

4、定期进行安全岗位人员考核

5、建立关键岗位人员保密制度和调离制度

建立密码应用岗位责任制度	
a) 测评指标	•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（第二级）。 •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（第三级）。 •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（第四级）。
b) 测评对象	系统相关人员（包括系统负责人、安全主管、密钥管理员、密码审计员、密码操作员等）。
c) 测评实施	•第二级：核查是否建立了密码应用岗位责任制度，安全管理制度中是否明确了各岗位在安全系统中的职责和权限。 •第三级：核查安全管理制度类文档是否根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位并定义岗位职责；核查是否对关键岗位建立多人共管机制，并确认密码安全审计员岗位人员是否不兼任密钥管理员、密码操作员等关键安全岗位；核查相关设备与系统的管理和使用账号是否有多人共用情况。 •第四级：核查安全管理制度类文档是否根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位并定义岗位职责；核查是否对关键岗位建立多人共管机制，并确认密码安全审计员岗位人员是否不兼任密钥管理员、密码操作员等关键安全岗位；核查相关设备与系统的管理和使用账号是否有多人共用情况；核查密钥管理员、密码安全审计员和密码操作员是否由本机构的内部员工担任，是否具有人员录用时对录用人身份、背景、专业资格和资质等进行审查的相关文档或记录等。
d) 结果判定	针对单个测评对象，如果以上相应等级的测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

密码应用测评要求 — 人员管理

人员管理：

1、了解并遵守密码相关法律法规和密码管理制度
2、建立密码应用岗位责任制度
3、建立上岗人员培训制度
4、定期进行安全岗位人员考核
5、建立关键岗位人员保密制度和调离制度

	建立上岗人员培训制度	定期进行安全岗位人员考核
a) 测评指标	建立上岗人员培训制度，对于涉及密码的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。（第二级到第四级）	定期对密码应用安全岗位人员进行考核。（第三级到第四级）
b) 测评对象	安全管理制度类文档和记录表单类文档、系统相关人员（包括系统负责人、安全主管、密钥管理员、密码审计员、密码操作员等）。	
c) 测评实施	核查安全教育和培训计划文档是否具有针对涉及密码的操作和管理的人员的培训计划；核查安全教育和培训记录是否有密码培训人员、密码培训内容、密码培训结果等的描述。	核查安全管理制度文档是否包含具体的人员考核制度和惩戒措施；核查人员考核记录内容是否包括安全意识、密码操作管理技能及相关法律法规；核查记录表单类文档确认是否定期进行岗位人员考核。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 人员管理

人员管理：

1、了解并遵守密码相关法律法规和密码管理制度
2、建立密码应用岗位责任制度
3、建立上岗人员培训制度
4、定期进行安全岗位人员考核
5、建立关键岗位人员保密制度和调离制度

建立关键岗位人员保密制度和调离制度	
a) 测评指标	•及时终止离岗人员的所有密码应用相关的访问权限、操作权限。（第一级） • 建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。（第二级到第四级）
b) 测评对象	安全管理制度类文档和记录表单类文档、系统相关人员（包括系统负责人、安全主管、密钥管理员、密码审计员、密码操作员等）。
c) 测评实施	•第一级：核查人员离岗时是否具有及时终止其所有密码应用相关的访问权限、操作权限的记录。 •第二级到第四级：核查人员离岗的管理文档是否规定了关键岗位人员保密制度和调离制度等；核查保密协议是否有保密范围、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。
d) 结果判定	针对单个测评对象，如果以上相应等级的测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

密码应用测评要求 — 建设运行

建设运行：

1、制定密码应用方案

2、制定密钥安全管理策略

3、制定实施方案

4、投入运行前进行密码应用安全性评估

5、定期开展密码应用安全性评估及攻防对抗演习

	制定密码应用方案	制定密钥安全管理策略
a) 测评指标	依据密码相关标准和密码应用需求，制定密码应用方案。（第一级到第四级）	根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节， 各环节密钥管理要求参照 GB/T 39786-2021 附录 B。（第一级到第四级）
b) 测评对象	密码应用方案。	密码应用方案、密钥管理制度及策略类文档。
c) 测评实施	核查在信息系统规划阶段，是否依据密码相关标准和信息系统密码应用需求，制定密码应用方案，并核查方案是否通过评估。	•核查是否有通过评估的密码应用方案；核查密钥管理制度及策略类文档是否确定系统设计的密钥种类、体系及其生存周期环节，是否与密码应用方案一致；若信息系统没有相应的密码应用方案，则核查密钥管理制度及策略类文档是否根据 GB/T 39786-2021附录B进行制定。 •核查相关密钥管理过程记录，核查是否按照密钥管理制度及策略类文档完成密钥管理。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 建设运行

建设运行：

1、制定密码应用方案

2、制定密钥安全管理策略

3、制定实施方案

4、投入运行前进行密码应用安全性评估

5、定期开展密码应用安全性评估及攻防对抗演习

	制定实施方案	投入运行前进行密码应用安全性评估
a) 测评指标	按照应用方案实施建设。（第一级到第四级）	•投入运行前进行密码应用安全性评估。（第一级到第二级） •投入运行前进行密码应用安全性评估，评估通过后系统方可正式运行。（第三级到第四级）
b) 测评对象	密码实施方案。	密码应用安全性评估报告、系统负责人。
c) 测评实施	核查是否有通过评估的密码应用方案，并核查是否按照密码应用方案，制定密码实施方案。	•第一级到第二级：核查信息系统投入运行前，是否组织进行密码应用安全性评估；核查是否具有系统投入运行前编制的密码应用安全性评估报告。 •第三级到第四级：核查信息系统投入运行前，是否组织进行密码应用安全性评估；核查是否具有系统投入运行前编制的密码应用安全性评估报告且系统通过评估。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。	

密码应用测评要求 — 建设运行

建设运行：

1、制定密码应用方案

2、制定密钥安全管理策略

3、制定实施方案

4、投入运行前进行密码应用安全性评估

5、定期开展密码应用安全性评估及攻防对抗演习

	定期开展密码应用安全性评估及攻防对抗演习
a) 测评指标	•在运行过程中，严格执行既定的密码应用安全管理制度，定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改（第三级到第四级）。
b) 测评对象	密码应用安全管理制度、密码应用安全性评估报告、攻防对抗演习报告、整改文档。
c) 测评实施	•核查信息系统投入运行后，信息系统责任方是否严格执行既定的密码应用安全管理制度，定期开展密码应用安全性评估及攻防对抗演习，并具有相应的密码应用安全性评估报告及攻防对抗演习报告；核查是否根据评估结果制定整改方案，并进行相应整改。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

密码应用测评要求 — 应急处置

应急处置：1、应急策略　　2、事件处置　　3、向有关主管部门上报处置情况

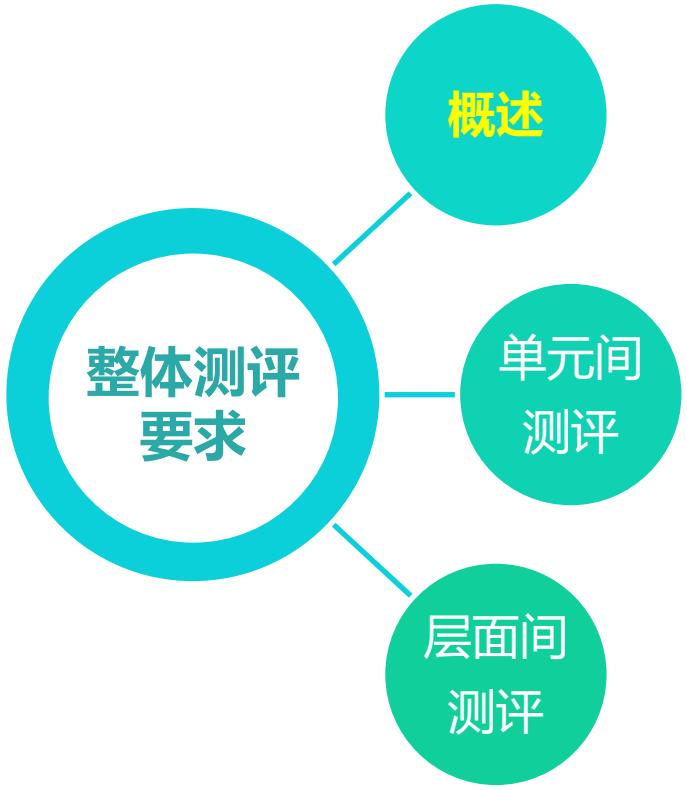
	应急策略	事件处置
a) 测评指标	•根据密码产品提供的安全策略，由用户自主处置密码应用安全事件。（第一级） •制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，按照应急处置措施结合实际情况及时处置。（第二级） •制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，立即启动应急处置措施，结合实际情况及时处置。（第三级到第四级）	•事件发生后，及时向信息系统主管部门进行报告。（第三级） •事件发生后，及时向信息系统主管部门及归属的密码管理部门进行报告。（第四级）
b) 测评对象	密码应用应急处置方案、应急处置记录类文档。	密码应用应急处置方案、安全事件报告。
c) 测评实施	•第一级：核查用户是否根据密码产品提供的安全策略处置密码应用安全事件。 •第二级：核查是否根据密码应用安全事件等级制定了相应的密码应用应急策略并对应急策略进行评审， 应急策略中是否明确了密码应用安全事件发生时的应急处理流程及其他管理措施，并遵照执行； 若发生过密码应用安全事件，核查是否具有相应的处置记录。 •第三级到第四级：核查是否根据密码应用安全事件等级制定了相应的密码应用应急策略并对应急策略进行评审， 应急策略中是否明确了密码应用安全事件发生时的应急处理流程及其他管理措施，并遵照执行； 若发生过密码应用安全事件，核查是否立即启动应急处置措施并具有相应的处置记录。	•第三级：核查密码应用安全事件发生后，是否及时向信息系统主管部门进行报告。 •第四级：核查密码应用安全事件发生后，是否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) 结果判定	同前。	

密码应用测评要求 — 应急处置

应急处置：1、应急策略　　2、事件处置　　3、向有关主管部门上报处置情况

向有关主管部门上报处置情况	
a) 测评指标	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。（第三级到第四级）
b) 测评对象	密码应用应急处置方案、安全事件发生情况及处置情况报告。
c) 测评实施	核查密码应用安全事件处置完成后，是否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，如事件处置完成后， 向相关部门提交安全事件发生情况及处置情况报告。
d) 结果判定	针对单个测评对象，如果以上测评实施内容均为是，则该测评对象符合本单元的测评指标要求；否则，不符合或部分符合本单元的测评指标要求。针对本测评单元，对该单元涉及的所有测评对象的判定结果进行汇总，如果判定结果均为符合，则本单元的测评结果为符合；如果判定结果均为不符合，则本单元的测评结果为不符合；否则，本单元的测评结果为部分符合。

整体测评要求 — 概述



- 整体测评应从单元间、 层面间等方面进行测评和综合安全分析。整体测评包括单元间测评和层面间测评。
- 单元间测评是指对同一安全层面内的两个或者两个以上不同测评单元间的关联进行测评分析，其目的是确定这些关联对信息系统整体密码应用防护能力的影响 。
- 层面间测评是指对不同安全层面之间的两个或者两个以上不同测评单元间的关联进行测评分析，其目的是确定这些关联对信息系统整体密码应用防护能力的影响。

整体测评要求 — 单元间测评

- 在单元测评完成后，应对单元测评结果中存在的不符合项或部分符合项进行单元间测评，重点分析信息系统中是否存在单元间的相互弥补作用。
- 根据测评分析结果，综合判定该测评单元所对应的信息系统密码应用防护能力是否缺失， 如果经过综合分析单元测评中的不符合项或部分符合项不造成信息系统整体密码应用防护能力的缺失，则对该测评单元的测评结果予以调整。**(内容和层面测评一样)**

整体测评要求 — 层面间测评

- 在单元测评完成后，应对单元测评结果中存在的不符合项或部分符合项进行层面间测评，重点分析信息系统中是否存在层面间的相互弥补作用。
- 根据测评分析结果，综合判定该测评单元所对应的信息系统密码应用防护能力是否缺失，如果经过综合分析单元测评中的不符合项或部分符合项不造成信息系统整体密码应用防护能力的缺失，则对该测评单元的测评结果予以调整。

风险分析和评价

密码应用安全性评估报告中应对整体测评之后单元测评结果中的不符合项或部分符合项进行风险分析和评价。

采用风险分析的方法， 针对单元测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性， 判断信息系统密码应用在合规性、正确性和有效性方面的不符合所产生的安全问题被威胁利用后对信息系统造成影响的程度，以及受到威胁利用的资产自身价值， 综合评价这些不符合项或部分符合项对信息系统造成的安全风险。

对于高风险的判定依据， 可参考其他相关标准或文件， 对未满足密码应用的正确性、有效性，或未使用经国家密码管理部门核准的密码技术且存在明显安全风险等措施，应结合具体业务场景做出高风险判定。

测评结论

密码应用安全性评估报告应给出信息系统的测评结论，确认信息系统达到相应等级保护要求的程度。

应结合整体测评和对单元测评结果的风险分析给出测评结论。

a) 符合：信息系统中未发现安全问题，测评结果中所有单元测评结果中部分符合和不符合项的统计结果全为 0， 综合得分为 100 分；

b) 基本符合：信息系统中存在安全问题，部分符合和不符合项的统计结果不全为 0， 但存在的安全问题不会导致信息系统面临高等级安全风险， 且综合得分不低于阈值；

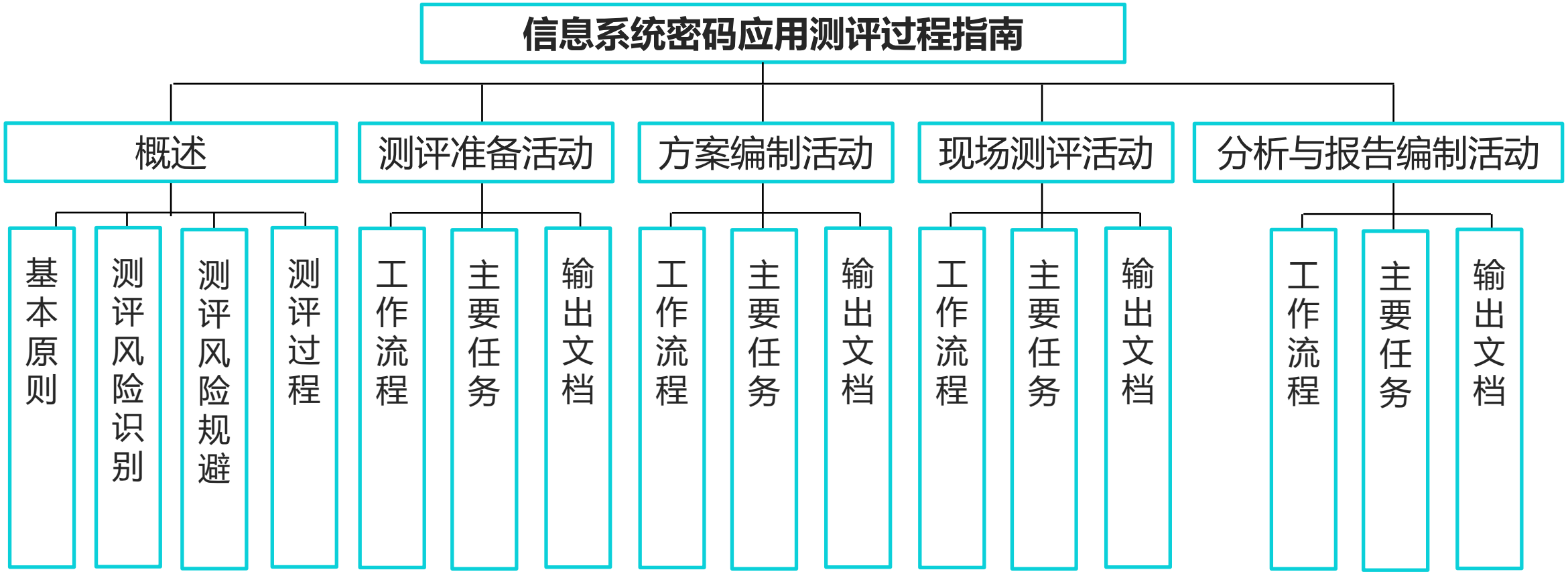
c) 不符合：信息系统中存在安全问题，部分符合项和不符合项的统计结果不全为 0， 而且存在的安全问题会导致信息系统面临高等级安全风险，或综合得分低于阈值。

密码测评过程依据 —《信息系统密码应用测评过程指南》

本文件规定了信息系统密码应用的测评过程，规范了测评活动及其工作任务。适用于商用密码应用安全性评估机构、信息系统责任单位开展密码应用安全性评估工作。

《信息系统密码应用测评过程指南》内容目次

《信息系统密码应用测评过程指南》总体框架



概述 — 基本原则

1、基本原则

测评方对信息系统开展密评时，应遵循以下原则：

- **客观公正性原则：**测评实施过程中，测评方应保证在符合国家密码主管部门要求及最小主观判断情形下，按照与被测单位共同认可的密评方案，基于明确定义的测评方式和解释，实施测评活动。
- **可重用性原则：** 测评工作可重用已有测评结果，包括商用密码检测认证结果和密码应用安全性评估的测评结果等。所有重用结果都应以已有测评结果仍适用于当前被测信息系统为前提，并能够客观反映系统当前的安全状态。
- **可重复性和可再现性原则：** 依照同样的要求，使用同样的测评方法，在同样的环境下，不同的密评人员对每个测评实施过程的重复执行应得到同样的结果。可重复性和可再现性的区别在于，前者关注同一密评人员测评结果的一致性，后者则关注不同密评人员测评结果的一致性。
- **结果完善性原则：**在正确理解 GB/T 39786 各个要求项内容的基础之上，测评所产生的结果应客观反映信息系统的密码应用现状。测评过程和结果应基于正确的测评方法，以确保其满足要求。

概述 — 测评风险识别

2、测评风险识别

测评工作的开展可能会给被测信息系统带来一定风险，测评方应在测评开始前及测评过程中及时进行风险识别。在测评过程中，面临的风险主要包括：

- **验证测试可能影响被测信息系统正常运行：**现场测评时，需对设备和系统进行一定的验证测试工作，部分测试内容需上机查看信息，可能对被测信息系统的运行造成不可预期的影响。
- **工具测试可能影响被测信息系统正常运行：**在现场测评时，根据实际需要可能会使用一些测评工具进行测试。 测评工具使用时可能会产生冗余数据写入，同时可能会对系统的负载造成一定的影响， 进而对被测信息系统中的服务器和网络通信造成一定影响甚至损害。
- **可能导致被测信息系统敏感信息泄漏：**测评过程中，可能泄露被测信息系统的敏感信息，如加密机制、业务流程、安全机制和有关文档信息等。
- **其他可能面临的风险：**在测评过程中，也可能出现影响被测信息系统可用性、 机密性和完整性的风险。

概述 — 测评风险规避

3、测评风险规避

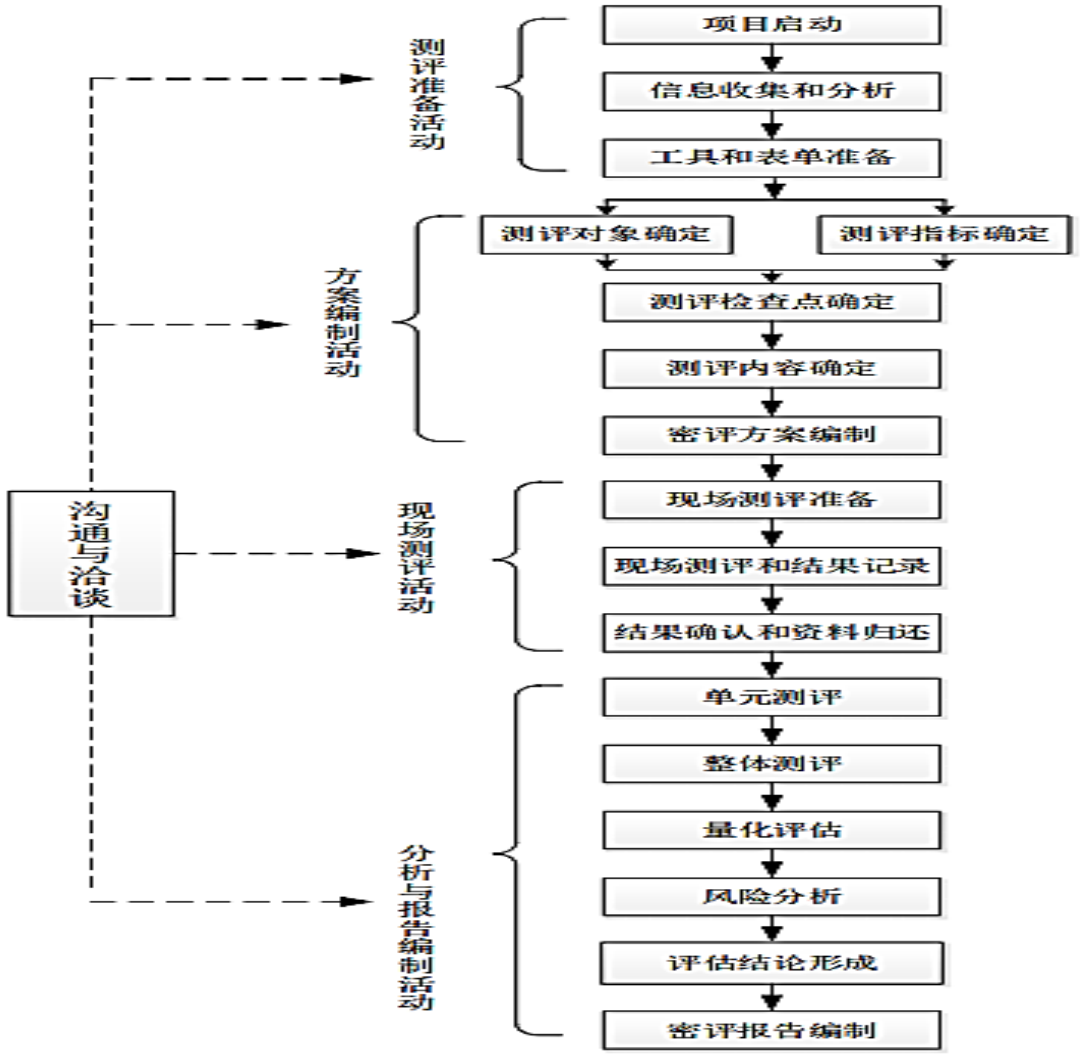
在测评过程中，可以通过采取以下措施规避风险：

- **签署委托测评协议书：**在测评工作正式开始之前，测评方和被测单位需要以委托协议的方式，明确测评工作的目标、范围、人员组成、计划安排、执行步骤和要求以及双方的责任和义务等，使得测评双方对测评过程中的基本问题达成共识。
- **签署保密协议：**测评相关方应签署合乎法律规范的保密协议，规定测评相关方在保密方面的权利、责任与义务。
- **签署现场测评授权书：**现场测评之前，测评方应与被测单位签署现场测评授权书，要求测评相关方对系统及数据进行备份，采取适当的方法进行风险规避，并针对可能出现的事件制定应急处理方案。
- **现场测评要求：**需进行验证测试和工具测试时，应避开被测信息系统业务高峰期，在系统资源处于空闲状态时进行测试，或配置与被测信息系统一致的模拟/仿真环境，在模拟/仿真环境下开展测评工作；需进行上机验证测试时，密评人员应提出需要验证的内容，由被测单位的技术人员进行实际操作。整个现场测评过程，由被测单位和测评方相关人员进行全程监督。测评工作完成后，密评人员应交回在测评过程中获取的所有特权，归还测评过程中借阅的相关资料文档，并将测评现场环境恢复至测评前状态。

概述 — 测评过程

4、测评过程

- 在测评活动开展前，需要对被测信息系统的密码应用方案进行评估，通过评估的密码应用方案可以作为测评实施的依据。
- 测评过程包括四项基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。
- 测评方与被测单位之间的沟通与洽谈应贯穿整个测评过程。测评过程如右图所示。



测评准备活动

工作流程

- 测评准备活动的目标是顺利启动测评项目，准备测评所需的相关资料，为编制密评方案提供条件。
- 测评准备活动包括项目启动、信息收集和分析、工具和表单准备三项主要任务。

主要任务

- **项目启动**：在项目启动任务中，测评方组建测评项目组，获取被测单位及被测信息系统的基本情况，从基本资料、人员、计划安排等方面为整个测评项目的实施做准备。
- **信息收集和分析**：测评方使用调查表格、查阅被测信息系统资料等方式，了解被测信息系统的构成和密码应用情况，为编写密评方案和开展现场测评工作奠定基础。
- **工具和表单准备**：测评项目组成员在进行现场测评之前，应熟悉与被测信息系统相关的各种组件、调试测评工具、准备各种表单等。

输出文档

任务	输出文档	文档内容
项目启动	项目计划书	项目概述、工作依据、技术思路、工作内容和项目组织等
信息收集和分析	完成的调查表格，各种与被测信息系统相关的技术资料	被测信息系统的网络安全保护等级、业务情况、软硬件情况、密码应用情况、密码管理情况和相关部门及角色等
工具和表单准备	选用的测评工具清单，打印的各类表单，如现场测评授权书、风险告知书、文档交接单、会议记录表单、会议签到表单等	测评工具、现场测评授权、测评可能带来的风险、交接的文档名称、会议记录表单、会议签到表单等

三、商用密码应用安全性评估标准简介

方案编制活动

工作流程

- 方案编制活动的目标是整理及分析测评准备活动中获取的被测信息系统相关资料，为现场测评活动提供最基本的文档和指导方案。
- 方案编制活动包括测评对象确定、测评指标确定、测评检查点确定、测评内容确定及密评方案编制五项主要任务。

主要任务

- **测评对象确定:**根据已经了解到的被测信息系统信息，分析整个被测信息系统及其涉及的业务应用系统，以及与此相关的密码应用情况，确定本次测评的测评对象。
- **测评指标确定:**根据已经了解到的被测信息系统定级结果，确定出本次测评的测评指标。
- **测评检查点确定:**测评过程中，需要对一些关键安全点进行现场检查确认，以防止密码产品、密码服务虽然被正确配置，但是未接入被测信息系统之类的情况发生。可通过抓包测试、查看关键设备配置等方法，来确认密码算法、密码技术、密码产品和密码服务的合规性、正确性和有效性。这些检查点应在方案编制时确定，并且充分考虑到检查的可行性和风险，最大限度地避免对被测信息系统的影响，尤其应避免对在线运行业务系统造成影响。
- **测评内容确定:**测评实施前，需确定现场测评的具体实施内容，即单元测评内容。
- **密评方案编制:**密评方案是测评工作实施的基础，用于指导测评工作的现场实施活动。密评方案应包括但不限于以下内容：项目概述、测评对象、测评指标、测评检查点以及单元测评实施等。

输出文档

任务	输出文档	文档内容
测评对象确定	密评方案的测评对象部分	被测信息系统的整体结构、边界、网络区域、核心资产、面临的威胁、测评对象等
测评指标确定	密评方案的测评指标部分	被测信息系统相应等级对应的适用和不适用的测评指标
测评检查点确定	密评方案的测评检查点部分	测评检查点、检查内容及测评方法
测评内容确定	密评方案的单元测评实施部分	单元测评实施内容
密评方案编制	经过评审和确认的密评方案文本	项目概述、测评对象、测评指标、测评检查点、单元测评实施内容、测评实施计划等

现场测评活动

工作流程

- 现场测评活动的目标是通过与被测单位进行沟通和协调，依据密评方案实施现场测评工作，获取分析与报告编制活动所需且足够的证据和资料。现场测评活动包括三项主要任务：现场测评准备、现场测评和结果记录、结果确认和资料归还。

主要任务

- **现场测评准备**：本任务启动现场测评，以保证测评方能够顺利实施测评。
- **现场测评和结果记录**：本任务主要是根据密评方案及现场测评准备的结果，测评方安排密评人员在现场完成测评工作。
- **结果确认和资料归还**

输出文档

任务	输出文档	文档内容
现场测评准备	会议记录、更新确认后的密评方案、确认的测评授权书和风险告知书等	工作计划和内容安排、双方人员的协调、被测单位应提供的配合与支持
现场测评和结果记录	各类测评结果记录	访谈、文档审查、实地察看和配置检查、工具测试的记录及测评结果
测评结果确认和资料归还	经过被测单位确认的各类测评结果记录	测评活动中发现的问题、问题的证据和证据源、每项测评活动中被测单位配合人员的书面认可文件

分析与报告编制活动 — 工作流程

1、工作流程

- 现场测评工作结束后，测评方应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成评估结论，并编制密评报告。

- 密评人员在初步判定各测评单元涉及的各个测评对象的测评结果后，还需进行单元测评、整体测评、量化评估和风险分析。经过整体测评后，有的测评对象的测评结果可能会有所变化，需进一步修订测评结果，而后进行量化评估和风险分析，最后形成评估结论。分析与报告编制活动包括单元测评、整体测评、量化评估、风险分析、评估结论形成及密评报告编制等六项主要任务。

分析与报告编制活动 — 主要任务

2、主要任务

- **单元测评**：本任务主要是针对各测评指标中的各个测评对象，客观、准确地分析测评证据，对每个测评对象分别进行测评实施和结果判定。 汇总各测评单元涉及的所有测评对象的测评实施结果， 得出各测评单元的判定结果，并以表格的形式逐一列出。
- **整体测评**：本任务针对测评结果为部分符合和不符合的测评对象，采取逐条判定的方法，给出整体测评的具体结果。
- **量化评估**：本任务综合单元测评结果和整体测评结果，计算修正后的各测评指标的各个测评对象的测评结果得分、各测评单元得分、各安全层面得分和整体得分，并对被测信息系统的密码应用情况安全性进行总体评价。
- **风险分析**：本任务依据相关规范和标准，采用风险分析的方法，分析测评结果中存在的安全问题以及可能对被测信息系统安全造成的影响。
- **评估结论形成**：本任务在测评结果汇总、量化评估以及风险分析的基础上，形成评估结论。
- **密评报告编制**：本任务根据分析与报告编制活动的各项任务输出形成密评报告。密评报告应符合信息系统密码应用安全性评估报告模板要求，包括但不限于以下内容：概述、被测信息系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、量化评估、风险分析、评估结论、改进建议等。其中，概述部分描述被测信息系统的总体情况、测评目的和依据等。

分析与报告编制活动 — 输出文档

3、输出文档

任务	输出文档	文档内容
单元测评	密评报告的单元测评部分	汇总统计各测评指标的各个测评对象的测评结果，给出单元测评结果
整体测评	密评报告的单元测评结果修正部分	分析被测信息系统整体安全状况及对各测评对象测评结果的修正情况
量化评估	密评报告中整体测评结果和量化评估部分，以及总体评价部分	综合单元测评和整体测评结果，计算得分，并对被测信息系统的密码应用情况安全性进行总体评价
风险分析	密评报告的风险分析部分	分析被测信息系统存在的安全问题风险情况
评估结论形成	密评报告的评估结论部分	对测评结果进行分析，形成评估结论
密评报告编制	经过评审和确认的密评报告	概述、被测信息系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、量化评估、风险分析、评估结论和改进建议等

谢谢大家！