

1 概述

1.1 背景

2018 年 5 月，习近平主席在出席两院院士大会时强调“努力实现关键核心技术自主可控，把创新主动权、发展主动权牢牢掌握在自己手中。关键核心技术事关创新主动权、发展主动权，也事关国家经济安全、国防安全和其他安全。”

以密码系统设计和密码安全测评为核心的商用密码技术，是构建网络空间安全保障体系、实现国家网络空间安全自主可控的基础。利用密码在安全认证、加密保护、信任传递等方面的重要作用，构建以密码为基石的安全可控信息技术体系，能够有效消除或控制网络安全问题，实现被动防御向主动免疫的战略转变。

商用密码应用安全性评估主要对重要信息系统和关键信息基础设施（CII）的密码安全进行整体的专项测试和综合评估，以形成科学准确的评估结果，评估涉及密码算法、协议、产品、技术体系、密码管理、密码与应用结合等诸多方面。通过以评促改、以评促用，逐步规范网络运营者的密码使用和管理行为，最终确保密码在重要信息系统和关键信息基础设施中使用的正确、合规、有效。商用密码应用安全性评估工作是密码检测认证体系的重要组成部分，也是《密码法》和中央有关文件的明确要求，是落实总体国家安全观和网络强国战略的具体行动，是深入推进重要领域密码应用的必然要求。

1.2 标准和规范

依据标准和规范

1.	《信息系统密码应用基本要求》（GM/T 0054-2018）
2.	《信息系统密码测评要求》（试行）
3.	《商用密码应用安全性评估测评过程指南》（试行）
4.	《商用密码应用安全性评估测评作业指导书》（试行）
5.	《密码应用标识规范》（GM/T 0006-2012）
6.	《SM2 密码算法使用规范》（GM/T 0009-2012）
7.	《SM2 密码算法加密签名消息语法规则》（GM/T 0010-2012）
8.	《数字证书认证系统密码协议规范》（GM/T 0014-2012）

9.	《基于 SM2 密码算法的数字证书格式规范》（GM/T 0015-2012）
10.	《密码设备应用接口规范》（GM/T 0018-2012）
11.	《IPSec VPN 技术规范》（GM/T 0022-2014）
12.	《IPSec VPN 网关产品规范》（GM/T 0023-2014）
13.	《SSL VPN 技术规范》（GM/T 0024-2014）
14.	《SSL VPN 网关产品规范》（GM/T 0025-2014）
15.	《安全认证网关产品规范》（GM/T 0026-2014）
16.	《智能密码钥匙技术规范》（GM/T 0027-2014）
17.	《服务器密码机技术规范》（GM/T 0030-2014）
18.	《基于 SM2 密码算法的证书认证系统密码及相关安全技术规范》（GM/T 0034-2014）
19.	《采用非接触卡的门禁系统密码应用技术指南》（GM/T 0036-2014）

2 密码应用安全性评估项目内容

2.1 项目需求

为保证密码应用安全性评估项目建设质量，防止验收时定性评价的随意性，参照相关法律法规，同时按照密码应用要求，需要进行项目的第三方测评。

（1）密码应用差距测评需求

依据《信息系统密码应用基本要求》（GM/T 0054-2018）、《信息系统密码测评要求（试行）》，组织开展密码应用安全性评估，衡量信息系统的密码安全管理措施和密码应用技术措施是否符合信息系统密码应用基本要求，是否具备了相应的密码保护能力。未达到密码应用保护要求的，提出改进建议，制定整改方案并进一步进行整改。

结合被测评单位实际需求与密码应用相关标准与法规进行合理的整改方案设计，同时对整改的流程与整改过程的可能风险及控制措施提供成熟的解决方案，确保最后信息系统整改后的符合信息系统密码应用基本要求。

（2）信息系统数据安全评估需求

网络安全日益强调全域安全，强信任、强安全、强可控、强防护成为必然要求，必须以规范使用国家认可的密码技术为基础，以系统性、整体性和协同性为原则，构建以

密码为基石的网络空间新安全。信息系统必须注重密码应用的合规性、正确性、有效性，依法开展密码应用安全性评估，确认系统使用密码技术实现真实性、机密性、完整性和不可否认性，保障信息系统中重要数据的安全性。针对评估中发现的安全问题，要立即整改。完善系统密码应用各项管理制度，增强信息系统信息安全技术。

（3）密码应用安全验收需求

在被测评系统进行完成差距测评和整改实施之后，需要再次通过测试手段对信息系统的密码应用安全技术和安全管理上各个层面的安全控制进行整体性验证，提供的测评服务需要协助用户完成密码应用安全性评估工作，对系统的密码应用和合规情况及整改情况进行评审，出具测评报告。

2.2 项目目标

通过开展密码应用安全性评估项目密评工作，确保密码应用的正确、合规、有效，以系统性、整体性和协同性为原则，构建以密码为基石的网络空间新安全，使系统平台安全管理更加突出重点、统一规范、科学合理，提高信息安全保障能力，维护国家安全、社会稳定和公共利益，保障和促进信息化建设。

通过对相关系统的进行调研，根据系统安全等级和调研结果，制定商用密码应用安全性评估方案和测评计划，并实施商用密码应用安全性评估，评判系统密码应用与信息系统密码应用基本要求之间的差距，并给出测评结论，以便指导系统运维单位进一步明确系统密码应用安全风险所在，有针对性的对业务信息系统进行密码应用安全方面的调整和改进，并对所发现问题进行整改时提供帮助，确保被测系统在密码应用方面的合规、正确、有效。

2.3 项目内容

本次项目范围包括：

阶段名称	阶段工作内容
密码应用安全方案评审	依据系统定级情况，审查被测系统密码应用设计方案或系统安全设计方案中的密码应用设计部分是否涵盖了所有需采用密码保护的核心资产及敏感信息，已设计的密码保护措施是否均能达到相应等级的密码使用要求或规定。
密码应用安全方案评估报告	测评机构对被测系统的密码应用方案进行评估，对密码技术方案的正确性、密码技术对信息系统安全保护的有效性、密码产品选取的合规性等方面进行评估，给出整改建议，被测单位反馈整改结果，整改通

阶段名称	阶段工作内容
	过后，测评机构出具评估报告。
密码技术应用、密钥管理和安全管理差距分析	针对单位定级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 4 个技术层面；制度、人员、实施、应急 4 个管理层面，以及密钥管理进行现场测评和差距分析，记录相关的测评结果。
差距分析记录撰写、评审、定稿	依照《现场测评记录》中所记录的针对单位定级系统的密码技术、密钥管理和安全管理测评结果，结合系统整体差距分析结果，按照国家密码管理部门标准测评报告模板撰写测评记录，完成初稿后交由单位，经确认后最终定稿，为下阶段自行开展整改加固工作提供可信依据。
整改建议方案指导、评审	依照《差距分析报告》中的测评结论和整改建议，结合针对单位定级系统的实际情况，指导设计系统密码应用安全整改方案，并由第三方测评机构就方案内容进行沟通和协商，提交整改建议方案。
安全整改、加固服务（甲方自主完成，第三方测评机构不参与整改工作）	依照《整改建议方案》中的具体建议，第三方测评机构将建议开展基于各差距的整改及加固的项目。整改内容包括针对密码设备采购部署的安全技术要求及针对管理体系的风险控制要求。 第三方测评机构将协助指导对新建或迁移的信息系统密码应用层面进行局部整改。
密码应用安全性评估	针对单位定级系统在《差距分析记录》及《整改建议方案》的基础上进行全面的密码应用安全性评估。 密码应用安全性评估包括：密码技术应用、密钥管理及安全管理评估三个方面。 根据现场访谈、配置核查的基础上通过密码应用安全测试工具进行安全检测及人工核查。
形成密码应用安全性评估结论及报告	根据各类测评结果记录表，分析和汇总各类测评数据，形成商用密码应用安全性测评报告，说明被测系统现有密码应用安全状况与国家密码应用安全要求之间的差距，形成《商用密码应用安全性测评报告》。

2.4测评目标

由第三方测评机构安全服务部门组成的测评团队，依据《信息系统密码应用基本要求》（GM/T 0054-2018）、《信息系统密码测评要求》（试行）、《商用密码应用安全性评估测评过程指南》（试行），与信息系统备案等级相对应的测评项，对信息系统进行信息系统密码应用安全性测评，出具是否满足信息系统安全保护等级的测评报告。

2.5测评实施流程

密码应用安全性评估过程分为四个基本测评活动：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。测评双方之间的沟通与洽谈贯穿整个密码应用安全性评估过程。

测评工作流程如下图所示。

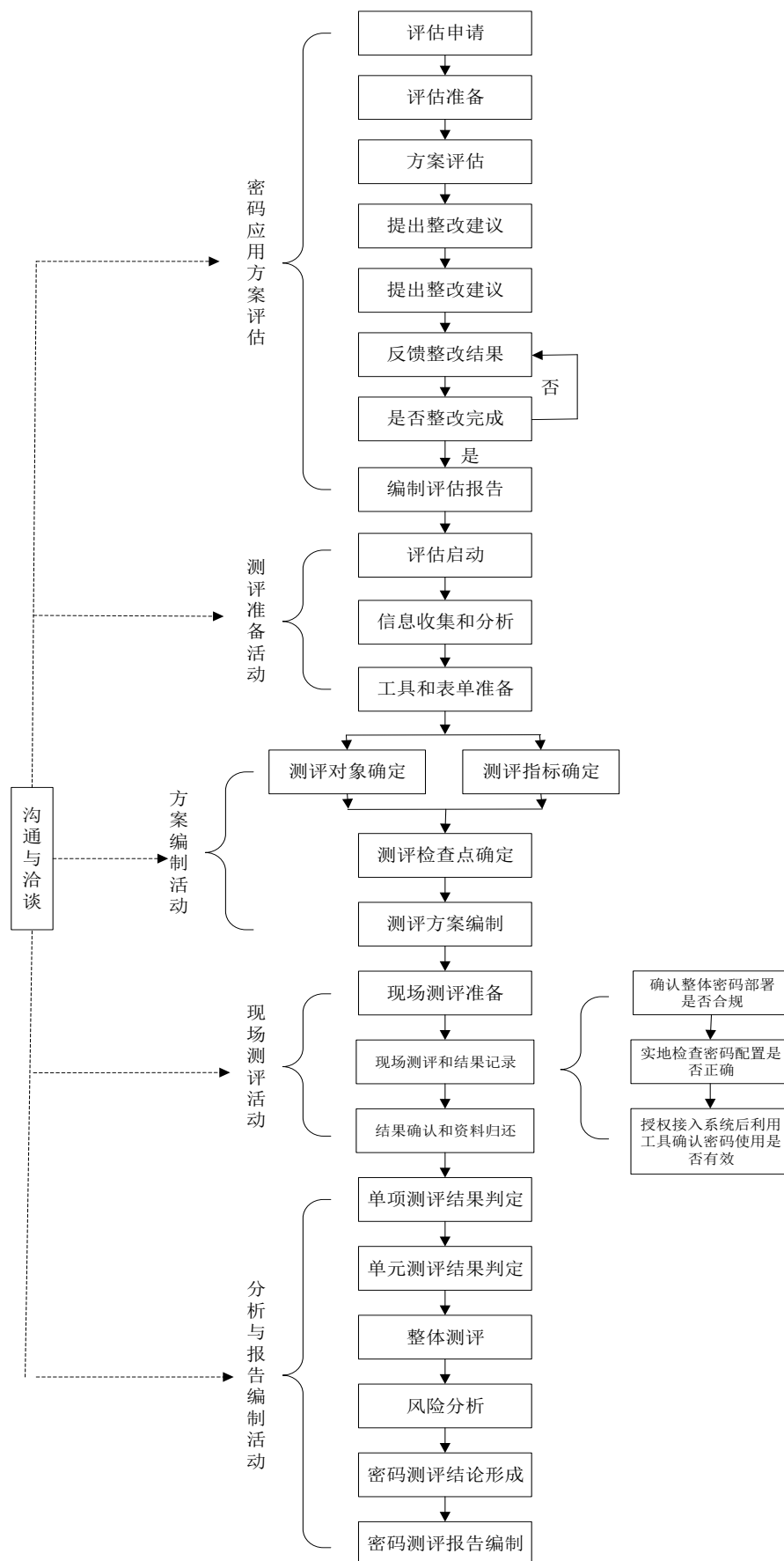


图 测评实施流程图

2.6 测评过程

2.6.1 密码应用方案评估

密码应用方案评估主要是依据系统定级情况，审查被测系统责任单位的密码应用设计方案或系统安全设计方案中的密码应用设计部分是否涵盖了所有需采用密码保护的核心资产及敏感信息，已设计的密码保护措施是否均能达到相应等级的密码使用要求或规定。

密码应用方案评估可由责任单位委托测评机构进行评估或组织专家进行论证，其中委托测评机构进行密码应用方案评估的情况，适用于本章。

信息系统的密码应用方案应当进行评估，经过评估的密码应用方案是测评的重要依据。密码应用方案经过评估后，应上报主管部门审核，由密码管理部门备案。

输入：信息系统密码应用方案。

任务描述：

a) 测评机构对被测系统的密码应用方案进行评估，对密码技术方案的正确性、密码技术对信息系统安全保护的有效性、密码产品选取的合规性等方面进行评估。

b) 对于没有通过评估的密码应用方案，由测评机构给出整改建议，被测系统责任单位根据方案不符合程度决定对设计方案进行修改完善或重新设计，并向测评机构反馈整改结果，直至整改通过，测评机构出具评估报告。

c) 密码应用方案经过评估或者整改通过后，可进入系统建设阶段。

输出/产品：密码应用方案评估报告。

密码应用方案评估的输出文档及其内容如下表所示：

任务	输出文档	文档内容
密码应用方案评估	密码应用方案评估报告	密码方案的正确性,密码技术对信息系统安全保护的有效性,选取密码产品的合规性等

2.6.2 测评准备阶段

根据测评双方签订的委托测评协议书和系统规模，测评机构组建测评项目组，从人员方面做好准备，并编制项目计划书。测评机构通过查阅被测系统已有资料并使用调查表格的方式，了解整个系统的构成和商用密码保护情况，为编写测评方案和开展现场测评工作奠定基础。测评项目组成员在进行现场测评之前，熟悉与被测系统相关的各种组件、调试测评工具、准备各种表单等。

2.6.3 方案编制阶段

根据已经了解到的被测系统信息，分析整个被测系统及其涉及的业务应用系统，以及与此相关的商用密码应用情况，确定出本次测评的测评对象；根据已经了解到的被测系统定级结果，确定出本次测评的测评指标；测评过程中，确认现场检查的关键安全点，并且充分考虑到检查的可行性和风险，最低限度的避免对被测系统，尤其是在线运行业务系统的影响；确定现场测评的具体实施内容，即单元测评内容；最终完成测评方案的编制。

2.6.4 现场测评阶段

现场测评准备：召开测评现场首次会，测评机构介绍测评工作，交流测评信息，进一步明确测评计划和方案中的内容，说明测评过程中具体的实施工作内容，测评时间安排，测评过程中可能存在的安全风险等，以便于后面的测评工作开展。测评双方确认现场测评需要的各种资源，包括测评委托单位的配合人员和需要提供的测评条件等，确认被测系统已备份过系统及数据。测评委托单位签署现场测评授权书。测评人员根据会议沟通结果，对测评结果记录表单和测评程序进行必要的更新。

测评小组根据测评方案以及现场测评准备的结果，安排测评人员在现场完成测评工作，汇总现场测评的测评记录；召开测评现场结束会，测评双方对测评过程中发现的问题进行现场确认；测评机构归还测评过程中借阅的所有文档资料，并由测评委托单位文档资料提供者签字确认。

2.6.5 分析与报告编制阶段

在现场测评工作结束后，测评机构对现场测评获得的测评结果进行汇总分析，形成测评结论，并编制评估报告。

测评人员在初步判定单元测评结果后，进而进行整体测评，经过整体测评后，进行风险分析和评价，形成测评结论。

测评机构完成测评结果记录的整理、密码应用安全问题分析，并与评估系统建设、开发单位进行问题反馈，开发人员针对存在的密码应用安全问题进行相应的整改，经最终整改确认，编制完成评估报告。