

T/SDASTC

团 体 标 准

T/SDASTC XXXX—XXXX

商用密码应用安全性评估服务项目工作量 测算指南

Guidelines for Workload Calculation of Commercial Cryptography Application
Security Assessment Services

（征求意见稿）

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

发 布

目 次

前 言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 工作内容 1

 4.1 内容概述 1

 4.2 测评准备 1

 4.3 方案编制 1

 4.4 现场测评 1

 4.5 分析与报告编制 1

5 工作量测算方法 2

 5.1 测算原则 2

 5.2 测算公式 2

 5.3 测算步骤 3

参 考 文 献 4

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。

本文件由新潮睿石信息技术有限公司提出。

本文件由山东科技咨询协会归口。

本文件起草单位：

本文件主要起草人：

商用密码应用安全性评估服务项目工作量测算指南

1 范围

本文件提供了商用密码应用安全性评估服务项目（以下简称“密评”）工作内容和工作量测算方法，适用于商用密码检测机构、信息系统运营者及第三方服务采购方在项目规划、预算编制与合同履行阶段的工作量评估。

本标准不适用于涉密信息系统项目的密码应用安全性评估工作量测算。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1 测评方案

用于指导商用密码应用安全性评估服务项目现场测评工作实施的指导性文件，内容一般由项目概述、测评对象、测评指标、测评检查点及单元测评实施等内容组成。

3.2 测评单元

一组相对独立和完整的测评内容，由测评指标、测评对象、测评实施和结果判定组成。

3.3 测评指标

测评单元中第一级到第四级密码应用测评的具体要求。

3.4 测评对象

测评单元中密码应用的测评实施对象。

4 工作内容

4.1 内容概述

密评工作的组织实施，严格遵循标准化作业程序，划分为测评准备、方案编制、现场测评、分析与报告编制四项内容，每项内容均设有明确的输入条件、输出成果以及工作活动。

4.2 测评准备

4.2.1 密评机构依据委托测评协议与被测系统规模组建项目组，编制项目计划书。

4.2.2 测评项目组通过查阅资料、发放调查表摸清被测系统构成与密码应用基础情况。

4.2.3 项目组完成人员就位、工具调试、表单筹备等前置准备工作。

4.3 方案编制

4.3.1 结合前期摸排情况梳理被测系统及关联业务的密码应用现状，确定本次测评对象。

4.3.2 依据系统定级结果明确测评指标，锁定需现场核查的关键安全点。

4.3.3 充分评估现场操作风险，确定适配的现场实施内容，完成正式测评方案编制。

4.4 现场测评

4.4.1 组织召开现场首次会，确认资源配置、系统备份状态，完成测评授权签署，同步更新现场执行表单。

4.4.2 项目组按既定方案完成全流程现场测评，同步归集所有现场原始记录。

4.4.3 召开现场末次会完成问题现场确认，归还全部借阅资料并由被测方签字核验。

4.5 分析与报告编制

- 4.5.1 归集全部现场测评数据，完成单单元初判、全系统整体测评两轮结果校验。
- 4.5.2 结合校验后的数据开展量化评估与风险分析，形成最终评估结论。
- 4.5.3 按规范完成正式密码应用安全性评估报告的编制工作。

5 工作量测算方法

5.1 测算原则

- 5.1.1 基准核定原则。以单一非云上无额外子系统、测评报告质量达标的密评项目为基准，通过工作量估算表的四个标准工作阶段额定值核算得到基准工作量H。
- 5.1.2 系数适配原则。依据项目实际属性，逐一匹配系统部署、子系统规模、人员技能、方案评估、复测场景、驻场地域、实施难度7类调整系数的对应取值，不得随意赋值。
- 5.1.3 合规核算原则。将核定的基准工作量与全部调整系数代入统一测算公式计算总工作量，测算过程可追溯、结果可复现。

5.2 测算公式

总工作量(W)是基准工作量(H)与各类型调整系数合计的乘积，各类型调整系数主要包括系统部署环境系数A、子系统数量N、项目人员技能综合B、方案评估C、复测情况D、驻场地理位置E、实施难度F，W按公式(1)计算：

$$W = (A + N + C + D + E + B + F) * H \dots\dots\dots (1)$$

式中：

W—总工作量，单位为人·日；

A—系统部署环境系数，云上权重设置为0.8，非云设置为1.0；

N—子系统系数， $N \leq 1$ ；

C—方案评估系数， $C=0.1$ ；

D—复测情况系数，复测情况存在 $D=0.9$ ，不存在 $D=1$ ；

E—驻场地理位置系数，新疆、西藏、内蒙、宁夏、青海、甘肃地区 $E=1.1$ ，河北省、山西省、辽宁省、吉林省、黑龙江省、江苏省、浙江省、安徽省、福建省、江西省、山东省、河南省、湖北省、湖南省、广东省、四川省、贵州省、云南省、陕西省、海南省地区 $E=1$ ，不涉及港、澳、台地区业务；

B—关联人员技能系数， $B=B1*I1+B2*I2+B3*I3$ ，B1代表高级人员，I1代表高级人员人数，B2代表中级人员，I2代表中级人员人数，B3代表初级人员，I3代表初级人员人数；

F—实施难度系数，系统部署位置处于红区或其他限制区域， $F=1.1$ ；

H—核算基准工作量，测算依据见表1。

表1 工作量估算表

序号	工作阶段	工作任务	工作量(人日)
1	测评准备	项目启动 信息收集和分析 工具和表单准备	2-4
2	方案编制	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 密评方案编制	2-4

- 1) 1. 初级人员应具备条件：作为项目组成员，参与至少7个密评项目实施与交付；能够独立完成项目前期对接，判断目标系统是否满足测评条件；具有1年项目经验。2. 中级人员应具备条件：作为项目经理或项目组成员，参与至少3具备行业前沿信息检个大型项目实施与交付能力；具备独立的项目实施与管理能力，有较强的项目组织、沟通和协调能力，能够处理复杂的技术问题；具有2年项目经验。3. 高级人员应具备条件：作为项目经理，参与具备科研立项申请书至少3个大型项目实编制能力施与交付；能够系统培养团队，通过指导与培训提升团队整体能力；具有5年项目经验。

序号	工作阶段	工作任务	工作量（人日）
3	现场测评	现场测评准备 现场测评和结果记录 结果确认和资料归还	6-10
4	分析与报告编制	单元测评 整体测评 量化评估 风险分析 评估结论形成 密评报告编制	10-20

^a 该表格估算的是以单一非云上系统（N=1，即无额外子系统，仅主系统）、报告质量达标（Q=1）时工作量（H）

5.3 测算步骤

- 5.3.1 建立核算基准工作量 H，以单非云上无额外子系统、报告达标场景为基准，按工作量估算表核算基础人天工作量。
- 5.3.2 核定系统部署环境系数 A、子系统数量 N、项目人员技能综合 B、方案评估 C、复测情况 D、驻场地理位置 E、实施难度 F 等调整系数。
- 5.3.3 以核算基准工作量为基础，根据所涉项目实际情况增加调整系数权重，最终核算出总服务量。

参 考 文 献

- [1]国家密码管理局. 商用密码应用安全性评估管理办法[S]. 北京: 国家密码管理局, 2023.
- [2]中国密码学会密评联委会. 商用密码应用安全性评估测评实施指引[S]. 北京: 中国密码学会密评联委会, 2024.
- [3]中国密码学会密评联委会. 政务领域政务服务平台密码应用与安全性评估实施指南[S]. 北京: 中国密码学会密评联委会, 2024.
- [4]中国密码学会密评联委会. 政务领域政务云密码应用与安全性评估实施指南[S]. 北京: 中国密码学会密评联委会, 2024.
- [5]中国密码学会密评联委会. 政务信息系统密码应用与安全性评估[S]. 北京: 中国密码学会密评联委会, 2020.
- [6]中国密码学会密评联委会. 信息系统密码应用高风险判定指引[S]. 北京: 中国密码学会密评联委会, 2021.
- [7]GB/T 39786 信息安全技术 信息系统密码应用基本要求
- [8]GB/T 43206 信息安全技术 信息系统密码应用测评要求