ICS 35.020
CCS A 16

DB34

安　徽　省　地　方　标　准

DB34/T 5160—2025

网络安全等级保护测评服务规范

Specification for evaluation service of classified protection of cybersecurity

2025－05－06 发布　　2025－06－06 实施

安徽省市场监督管理局　　发 布

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。

本文件由安徽省公安厅提出并归口。

本文件起草单位：合肥市公安局、安徽省公安厅网络安全保卫总队、合肥天帷信息安全技术有限公司、安徽省电子产品监督检验所、安徽科测信息技术有限公司、安徽祥盾信息科技有限公司、安徽溯源电子科技有限公司、安徽万弗检测技术有限公司、安正网络安全技术有限公司、华测风雪检测技术有限公司、安徽国康网络安全测评有限公司、安徽信科共创信息安全测评有限公司、安徽省大数据中心、合肥市信息中心、淮北市公安局网络安全保卫支队、六安市公安局网络安全保卫支队、六安市数据资源管理局、亳州市数据资源管理局、淮北市数据资源管理局、凤阳县数据资源管理局。

本文件主要起草人：冯响林、左晓坤、杨波、王亮、唐珂、任仁、方雪峰、汪正文、郝雪元、王亭亭、唐远航、王智海、胡兴元、武建双、郭凯、朱克涛、姜思思、刘芝影、陈萌、方成成、许阿伟、罗晓军、张春辉、路安、张锦睿、朱典、胡飞、丁晓、韩程程、白修灵、程博、翁挡挡、刘伟、刘智伟、许客、胡朋子、翟清颖。

网络安全等级保护测评服务规范

1 范围

本文件规定了网络安全等级保护测评服务的流程及要求。

本文件适用于网络安全等级保护测评服务。

注：在不引起混淆的情况下，本文件中的“网络安全等级保护测评”简称为“等级测评”。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2022 信息安全技术 术语

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

GB/T 28449 信息安全技术 网络安全等级保护测评过程指南

GB/T 36959—2018 信息安全技术 网络安全等级保护测评机构能力要求和评估规范

3 术语和定义

GB/T 22239—2019、GB/T 28448—2019、GB/T 25069—2022和GB/T 36959—2018界定的以及下列术语和定义适用于本文件。

3.1

网络安全等级保护测评服务 evaluation service for classified protection of cybersecurity

测评机构依据国家网络安全保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密测评对象的网络安全等级保护状况进行检测评估的过程。

4 基本要求

4.1 机构

4.1.1 从事等级测评服务的机构应具有独立法人资格或为独立法人组织中的独立部门。

4.1.2 从事等级测评服务的机构应取得等级测评服务认证证书。

4.2 人员

4.2.1 从事等级测评服务的人员应满足 GB/T 36959—2018 的人员要求。

4.2.2 从事等级测评服务的人员应具有信息安全或网络安全等级保护测评师证书，并由测评机构配发上岗证。

4.3 场地和工具

4.3.1　测评机构应具有固定的办公场所。
4.3.2　测评机构应配备满足测评业务需求的设施设备和检测工具。

4.4　管理制度

测评机构应建立项目管理、质量管理、设备管理、人员管理、教育培训管理、文档管理、保密管理、申诉投诉及争议处理等制度。

4.5　档案管理

等级测评服务过程中形成的文档、记录、资料等应保存三年以上，并由专人负责保管。

5　服务流程

等级测评服务流程见图1。

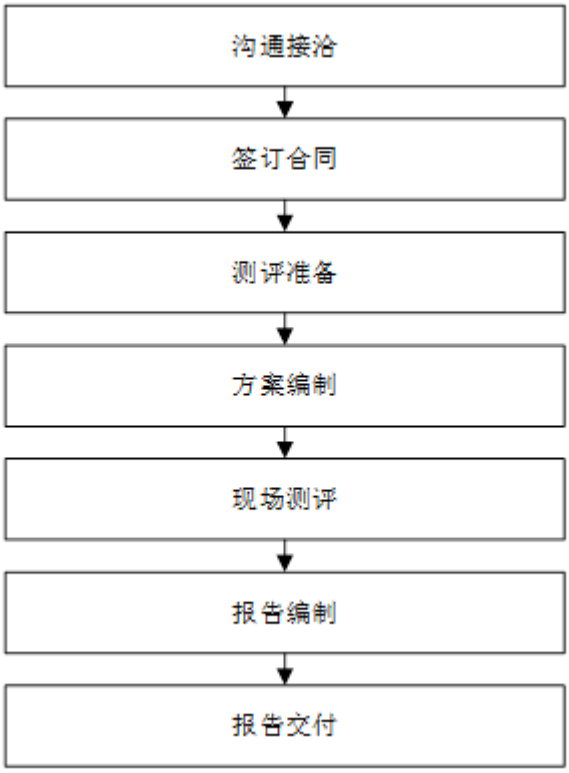

图1　等级测评服务流程图

6　服务要求

6.1　沟通接洽

6.1.1　测评机构应通过面谈、电话、邮件、即时通讯等方式与被测评单位进行沟通接洽。
6.1.2　沟通接洽时应主动介绍服务内容、服务流程、服务时限、服务价格以及需要配合的相关事项。
6.1.3　沟通接洽过程应收集被测评单位的基本信息、系统定级情况、系统之前的测评情况等。

6.2　合同签订

6.2.1 测评机构应与被测评单位直接签署等级测评服务合同，并签定保密协议。

6.2.2 等级测评服务合同的内容应包括但不限于测评服务范围、测评服务时间、测评对象的名称和数量、单价和总价、双方责任和义务、交付物。

6.3 测评准备

6.3.1 人员准备

6.3.1.1 测评机构应组建项目组，配备测评组长 1 名，测评师不少于 2 人，渗透测试人员不少于 1 人；测评内容含三级以上等级保护对象的测评项目，测评师应不少于 4 名，渗透测试人员不少于 1 人，其中高级测评师、中级测评师各不少于 1 名。

6.3.1.2 测评组长应由中级测评师以上人员担任，测评师应具有初级以上测评师资格。

6.3.1.3 项目组应编制项目计划书，内容应包括但不限于项目背景、测评范围依据、测评整体计划、测评风险提示。具体内容和格式参见附录 A。

6.3.2 现场调研

6.3.2.1 应将制定的项目计划书告知被测评单位，并由被测评单位确认。

6.3.2.2 等级测评人员应依据《信息系统基本情况调研表》进行现场调研，《信息系统基本情况调研表》格式参见附录 B。

6.3.2.3 对于云计算、物联网、移动互联、工业控制、大数据等安全扩展要求的测评对象，应进行专门调研。

6.3.2.4 对于金融、交通运输、民用航空、证券期货、广电、电力等行业，以及容器扩展、区块链扩展的测评对象，应调研执行的行业标准及其特殊要求。

6.3.3 表单准备

项目组准备的模板、资料等表单应包括但不限于：

——独立、公正、诚信声明；
——测评人员保密协议；
——选用的测评工具清单；
——风险告知书；
——文档交接单；
——会议记录表；
——会议签到表；
——现场测试授权书；
——测评作业指导书；
——工具测试（漏洞扫描、渗透测试）授权书；
——工具测试特殊事项说明；
——整改建议书；
——现场测评结果记录表；
——会议小结记录表；
——现场测评过程及用户确认表。

6.3.4 工具准备

项目组准备的测评工具应包括但不限于：

——漏洞扫描工具；
——渗透测试工具；
——性能测评工具；
——协议分析工具；
——网络数据抓包工具；
——测评自动化工具和综合管理平台。

6.4 方案编制

6.4.1 项目组应根据现场调研情况编制项目《等级测评服务方案》，内容包括但不限于项目概述、测评对象、测评指标、测评内容、测评方法、项目管理。《等级测评服务方案》格式参见附录C。
6.4.2 测评机构应对项目《等级测评服务方案》进行论证，并审核批准。
6.4.3 项目组应将批准的项目《等级测评服务方案》提交给被测评单位进行确认。

6.5 现场测评

6.5.1 召开首次会

6.5.1.1 项目组应组织召开测评首次会，参会人员应包括但不限于被测单位的安全主管、信息系统开发人员、信息系统维护人员和项目组所有人员。
6.5.1.2 首次会的主要内容应包括通报《项目计划书》和《等级测评服务方案》内容；宣读《独立、公正、诚信声明》和《风险告知书》；签署《现场测评授权书》、《风险告知书》和《测评人员保密协议》；对接现场测评需要的人员、资料和环境等各类资源。
6.5.1.3 首次会结束后，项目组应收集、整理和汇总首次会议形成的所有资料，包括但不限于会议签到表，会议记录表，经确认的《项目计划书》和《等级测评服务方案》，经现场签署的《现场测评授权书》、《风险告知书》和《测评人员保密协议》。

6.5.2 实施测评

6.5.2.1 等级测评人员应对被测单位相关人员进行访谈，并核查被测评单位的相关制度文件及记录表单。
6.5.2.2 等级测评人员应协助、指导被测单位相关技术人员查看相关测评对象的配置，并进行记录。
6.5.2.3 等级测评人员应依据操作规程使用测评设备和工具，按照《测评作业指导书》逐项进行核查。
6.5.2.4 等级测评过程中应完整、准确记录核查结果。
6.5.2.5 等级测评人员应按照《等级测评服务方案》开展验证测试工作，并完整、准确记录验证测试结果。被测单位对特殊系统拒绝测试工具接入的，应签署《工具测试特殊事项说明》。
6.5.2.6 验证测试结果应和被测单位进行沟通，并口头确认。
6.5.2.7 现场测评完成后，应由被测单位对《现场测评过程及用户确认表》签字确认。
6.5.2.8 现场测评结束后，应归还被测单位提供的证据资料，由被测单位相关人员在《文档交接单》上签字确认，并告知现场测评工作完成情况。
6.5.2.9 等级测评人员应保留现场测评证据和测评结果记录，涉及敏感内容应进行脱敏处理后留存。

6.5.3 召开末次会

6.5.3.1 现场测评工作全部结束后，测评组应组织召开末次会，参会人员应包括但不限于被测单位的安全主管、信息系统开发人员、信息系统维护人员和项目组所有人员。

6.5.3.2 末次会议内容应包括通报现场测评情况、证据源和测评记录、高风险问题、整改事项及优先级和期限、等级测评报告预计交付时间；交付给被测单位《现场测评结果记录表》和《整改建议书》，并确认。

6.5.3.3 《整改建议书》的内容应包括但不限于发现的问题、风险等级、整改优先级、整改建议、整改时限、整改预期等内容。

6.5.3.4 末次会期间项目组应通过拍照、会议签到、会议小结记录的形式留存会议证据。末次会结束时，项目组应收集、整理和汇总末次会议形成的所有资料。

6.5.4 验证整改结果

6.5.4.1 末次会议结束后，项目组应督促、指导被测单位按照《整改建议书》进行整改。

6.5.4.2 被测单位整改结束后，项目组应对整改完成情况进行现场验证。

6.5.4.3 现场验证的技术和方法应与现场测评过程中采取的技术和方法一致。

6.5.4.4 现场验证的结果应进行记录，修改前期的《现场测评结果记录表》。

6.6 报告编制

6.6.1 项目组应编制《网络安全等级测评报告》,《网络安全等级测评报告》格式和内容参见 GB/T 28449，或按照行业主管部门给出的格式和内容进行编制。

6.6.2 测评机构应对《网络安全等级测评报告》进行审核、批准。

6.6.3 纸质《网络安全等级测评报告》应加盖测评机构代码标识，报告应粘贴防伪标识。

6.7 报告交付

6.7.1 应根据合同要求交付《网络安全等级测评报告》给被测单位，同时提交给所辖公安机关。

6.7.2 交付给被测单位的《网络安全等级测评报告》应由被测评单位签收确认。

6.7.3 测评机构应留存纸质《网络安全等级测评报告》归档。

7 评价与改进

7.1 评价

7.1.1 等级测评服务应进行自我评价、客户满意度评价和第三方评价。

7.1.2 等级测评服务评价应包括服务的全生命周期所涉及的内容。

7.1.3 自我评价应每季度进行一次；每个服务对象都应进行客户满意度评价；第三方评价宜每两年进行一次。

7.2 改进

7.2.1 根据评价结果梳理存在问题，提出整改措施。

7.2.2 落实整改措施，持续改进服务质量。

附 录 A
（资料性）
等级测评服务项目计划书

下面给出了等级测评服务项目计划书的示例。

示例：

项目编号：

网络安全等级保护测评服务计划书

被测单位：_____

测评单位：_____

日　　期：_____

网络安全等级保护测评服务计划书

第一章 项目背景

第二章 测评范围依据

第三章 测评整体计划

3.1.现场测评实施计划

3.2.工具测试计划

第四章 测评人员安排

第五章 测评风险提示

附 录 B
（资料性）
信息系统基本情况调研表

下面给出了信息系统基本情况调研表示例。

示例：

文档编号：

项目编号：

信息系统基本情况调查表
等级保护测评服务

XXXX 年 XX 月

文档编号：

一、文档提交要求

受贵单位正式委托，XX 对贵单位信息系统实施等级测评，为了使测评人员在现场测评前期就能够对被评估系统有清晰而全面地了解，委托机构应准备相关的文档。

需准备的测评文档包括但不限于以下几类：

- 系统调查表格
- 被测信息系统总体描述文件
- 详细描述文件
- 定级报告
- 系统验收报告
- 安全需求分析报告
- 安全总体方案
- 自查或上次等级测评报告
- 其他相关材料

具体内容请见正文。

文档编号：

二、准备文档时需注意的问题

- 保证提交文档内容真实、全面、详细、准确
- 文档材料，纸版和电子版文档均可
- 提交文档时做好详细的文档交接记录

文档编号：

附件一　信息系统基本情况调查表

1　项目基本信息

1.1　单位基本信息

填表人：XXX　日期：XXXX 年 XX 月 XX 日

被测评单位				
单位全称			单位简称	
单位情况简介				
单位所属类型			上级主管部门	
单位地址			邮政编码	
单位负责人			联系电话	
联系人	姓名		职务/职称	
	所 属部门		联系电话	
	移 动电话		电子邮件	

表 1-1 单位基本信息表

1.2　项目背景以及被测系统业务介绍

文档编号：

1.3 等级保护对象基本情况

1.3.1 安全通用系统情况调研表

等级保护对象				
定级对象	名称		安全保护等级	
	业务信息安全保护等级		系统服务安全保护等级	
	功能描述		备案证明编号	
	新技术新应用涉及情况	□云计算 □工业控制系统 □容器	□移动互联 □大数据 □不涉及	□物联网 □区块链

表 1-2 安全通用系统情况调研表

1.3.2 新技术新应用系统情况调研

2 机房调研（主机房信息、灾备机房信息）

3 网络结构调研

3.1 网络拓扑结构图及网络描述

1） 系统网络拓扑如下：

2） 系统网络结构说明如下：

Page 4

3.2 网络结构情况

3.3 网络外联情况

4 网络互联设备基本情况调研

5 安全设备基本情况调研

6 承载的业务应用情况及业务数据流程调研

6.1 业务应用基本情况

6.2 主要业务数据流程

提供系统业务数据流程图

注：从不同类型业务用户的视角出发，给出关键业务处理流程图，并标注涉及应用组件/模块、主要处理动作，以及关键业务数据在主机设备（程序模块）之间的交换情况。可参考软件开发文档，如软件部署图，开发用例等。

7 服务器基本情况调研

8 终端基本情况调研

9 其他系统或设备调研

10 系统管理软件/平台调研

11 数据资源调研

12 密码产品调研

13 安全相关人员调研

人员角色主要包括：安全主管、系统建设负责人、系统运维负责人、物理安全负责人、人事负责人、系统管理员、网络管理员、安全管理员、系统开发人员、应用管理员、档案管理员、资产管理员，各管理员角色可以是很多名。

14 安全管理文档调研

15 安全服务调研

文档编号：

16 安全威胁情况调研

序号	安全事件调查	调查结果
1	是否发生过网络安全事件	□没有 □1 次/年□2 次/年□3 次以上/年□不清楚 安全事件说明(时间、影响)
2	发生的网络安全事件类型（多选）	□感染病毒/蠕虫/特洛伊木马程序 □拒绝服务攻击 □端口扫描攻击 □数据窃取 □破坏数据或网络 □篡改网页 □垃圾邮件 □内部人员有意破坏 □内部人员滥用网络端口、系统资源 □被利用发送和传播有害信息 □网络诈骗和盗窃 □其他 其他说明：
3	如何发现网络安全事件（多选）	□网络（系统）管理员工作检测发现 □通过事后分析发现 □通过安全产品发现 □有关部门通知或意外发现 □他人告知 □其他 其他说明：
4	网络安全事件造成损失评估	□非常严重 □严重 □一般 □比较轻微 □轻微 □无法评估
5	可能的攻击来源	□内部 □外部 □都有 □病毒 □其他原因 □不清楚 攻击来源说明：
6	导致发生网络安全事件的可能原因	□未修补或防范软件漏洞 □网络或软件配置错误 □登录密码过于简单或未修改 □缺少访问控制 □攻击者使用拒绝服务攻击 □攻击者利用软件默认设置 □利用内部用户安全管理漏洞或内部人员作案 □内部网络违规连接互联网 □攻击者使用欺诈方法 □不知原因 □其他 其他说明：
7	是否发生过硬件故	□有 （注明时间、频率） □无

文档编号：

序号	安全事件调查	调查结果
	障	造成的影响是：
8	是否发生过软件故障	□有　　（注明时间、频率）　　□无 造成的影响是
9	是否发生过维护失误	□有　　（注明时间、频率）　　□无 造成的影响是
10	是否发生过因用户操作失误引起的安全事件	□有　　（注明时间、频率）　　□无 造成的影响是
11	是否发生过物理设施/设备被物理破坏	□有　　（注明时间、频率）　　□无 造成的影响是
12	有无遭受自然性破坏（如雷击等）	□有　　（注明时间、频率）　　□无 有请注明时间、事件后果
13	有无发生过莫名其妙的故障	□有　　（注明时间、频率）　　□无 有请注明时间、事件后果

表 16-1 安全威胁情况表

附件二 云计算平台测评及整改情况

附 录 C
（资料性）
项目等级测评服务方案

下面给出了项目等级测评服务方案示例。

示例：

项目编号：

网络安全等级保护测评服务方案

被测单位：_____

测评单位：_____

日　　期：_____

网络安全等级保护测评服务方案

第一章 项目概述

第二章 测评对象

第三章 测评指标

第四章 测评内容

第五章 测评方法

第六章 项目管理

参 考 文 献

[1] TRIMPS-JSGF-003:2024 网络安全服务认证技术规范(等级保护测评)