

标准

中华人民共和国国家标准

59—2018

GB/T 369

信息安全技术 网络安全等级保护

能力要求和评估规范

测评机构能力

Capability requirements and evaluation

Information security technology

Specification of classified protection of cybersecurity

Specification for assessment organi

2019-07-01 实施

2018-12-28 发布

国家市场监督管理总局  
国家标准化管理委员会 发布

国家市  
中国国



## 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 测评机构能力要求 .....	2
4.1 测评机构的分级 .....	2
4.2 等级测评人员的分级 .....	2
4.3 I级测评机构能力要求 .....	6
4.4 II级测评机构能力要求 .....	11
4.5 III级测评机构能力要求 .....	16
4.6 测评机构行为规范性要求 .....	16
5 测评机构能力评估 .....	16
5.1 评估流程 .....	18
5.2 初次评估 .....	18
5.3 期间评估 .....	19
附录A 测评机构和增强要求等级对应情况一览表 .....	19
附录B 强制性附录B—网络安全等级保护 .....	20



## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会归口。本标准的主要起草人及

# 引 言

《中华人民共和国网络安全法》第二十一条规定，国家实行网络安全等级保护制度。等级保护制度

的等级保护制度，是指国家实行网络安全等级保护制度，根据网络在国家安全、国民经济、社会公共利益中的重要性，以及网络运营者、网络使用者、网络数据所有者、网络数据控制者的身份、数量、分布、行为等因素，对网络进行等级划分，并依据等级采取相应的网络安全保护措施。

等级保护制度是网络安全工作的基本制度，是网络安全工作的基础。等级保护制度的实施，对于提高网络安全防护能力，保障网络安全，具有重要意义。

网络安全等级保护制度，是指国家实行网络安全等级保护制度，根据网络在国家安全、国民经济、社会公共利益中的重要性，以及网络运营者、网络使用者、网络数据所有者、网络数据控制者的身份、数量、分布、行为等因素，对网络进行等级划分，并依据等级采取相应的网络安全保护措施。

# 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

## 1 范围

本标准规定了网络安全等级保护测评机构的能力要求和评估规范。

定等级保护。

## 2 规范性引用文件

的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是未注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

下列文件对于本文件的  
应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是未注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 28448 信息安全技术 网络安全等级保护测评机构能力要求

GB/T 28449 信息安全技术 网络安全等级保护测评规范

## 3 术语和定义

GB/T 28448 界定的以及下列术语和定义适用于本文件。

### 3.1

**能力评估 capability evaluation**

依据标准和(或)其他规范性文件,对测评机构申请单位的能力进行评审、验证和评价的过程。

### 3.2

**评估机构 evaluation organization**

对申请成为测评机构的企事业单位进行能力评估的专业技术机构。

### 3.3

**初次评估 first-time evaluation**

评估机构依据本规范和相关文件,首次对测评机构能力进行核查、验证和评价的过程。

### 3.4

**期间评估 continuous evaluation**

为已经获得推荐证书的测评机构是否持续地符合能力要求而在证书有效期内安排的定期或不定期  
的评估、抽查等活动。

### 3.5

**能力复评 capability review**

测评机构推荐证书有效期结束前,由评估机构对其实施全面评估以确认其是否持续符合能力要求,  
为延续到下一个推荐有效期提供依据的活动。

### 3.6

**评估员 evaluator**

由评估机构委派,对测评机构实施能力评估的人员。



至销毁的各项记录。应包含机构人员在测评文档(含电子文档)管理中的相关要求,档案借阅、保管直

接负责。

d) 人力资源管理

应包括人员录用、考核、日常管理以及离职等方面的内容和要求。

e) 培训教育制度

应包括培训计划的制定、培训工作的实施、培训的考核与考核以及人员培训档案建立等内容和要求。

f) 申诉、投诉及争议处理制度

应明确包括测评机构各岗位人员在申诉、投诉和争议处理活动中相应的职责,建立从受理、确认到处置、答复等环节的完整程序。

4.3.3 测评实施能力

4.3.3.1 人员能力

4.3.3.1.1 测评机构从事等级测评工作的专业技术人员(以下简称测评人员)应具有把握国家政策法规、理解测评标准、掌握测评系统原理、测评流程、测评工具使用、测评报告编写等能力,并能根据测评需求制定测评方案、组织实施测评、出具测评报告。

4.3.3.1.2 测评人员应参加由监管部门组织的测评、考核并取得等级测评师证书。等级测评师人员需持证上岗。

4.3.3.1.3 测评技术负责人、测评项目组长和技术主管岗位人员应分别取得初、中、高级等级测评师证书。测评师数量本应不少于15人。

4.3.3.1.4 测评人员除具备等级测评师资格外,每年应参加多种形式的测评业务和技术培训。测评师每年培训时长累计不少于40学时。

4.3.3.1.5 测评机构应指定一名技术主管,全面负责等级测评方面的技术工作。

4.3.3.2 测评能力

4.3.3.2.1 测评机构应通过提供案例、过程记录等资料,证明其具有从事网络安全相关工作2年以上的

工作经历。

具体要求,具体

4.3.3.2.2 测评机构应保证在其能力范围内从事测评工作,并有足够的资源来满足测评工作。体现在以下方面:

a) 安全技术测评实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、

安全管理、人员安全和业务连续性等方面。

b) 安全管理测评实施能力,包括安全策略和制度、安全管理机构和人员、

运维管理、风险评估、应急响应、业务连续性、灾难恢复和安全管理。

此外,测评机构还应具备以下能力:

1) 能够制定测评方案,包括测评目标、测评范围、测评方法、测评工具、测评报告等。

2) 能够制定测评计划,包括测评时间、测评地点、测评人员、测评设备等。

3) 能够制定测评报告,包括测评过程、测评结果、测评结论等。

4) 能够制定测评方案,包括测评目标、测评范围、测评方法、测评工具、测评报告等。

4.3.3.2.3 测评机构应建立测评项目管理制度,明确测评项目的工作流程,并定期组织测评项目

考核和绩效评价工作,具体要求如下:

a) 测评准备阶段,应收集被测系统的相关资料,填写规范的系统调查表,全面了解被测系统的详细情况,为测评工作做好准备。

b) 方案编制阶段,应明确合理地确定测评对象、测评指标及测评内容等,并依据现有有效的技术

准、规范开发测评方案、测评指导书、测评结果记录表格等。测评方案应通过技术评审并有相关记录,测评指导书应进行版本有效性维护,且满足以下要求:

- 1) 符合相关的等级测评标准;
- 2) 提供足够详细的信息以确保测评数据获取过程的规范性和可操作性。

施和设备安全与保障能力

4.3.4 设

理系统使用的技术装备应符合下列

4.3.4.0 测评机构应必须具备国家认证认可监督管理委员会

合格证书。

国家投资或者控股的,在中华人民共和国境

a) 产品研制、生产单位是由中国公民、法人投资或者  
内具有独立的法人资格;

b) 产品的核心技术、关键部件具有我国自主知识产权

c) 产品研制、生产单位及其主要业务技术人员无犯

罪记录;

4.3.4.2 测评机构应配备符合下列条件的测评专家

4.3.4.3 测评机构应

4.3.4.4 测评机构应

4.3.4.5 测评机构

理能力

4.3.5 质量管

本体系建设

4.3.5.1 管理体

机构应建立、实施和维护符合等级测评工作需要的文件化的管理体系,并确保测评机构理解和执行。

4.3.5.1.1 测评

各级人员能够理

机构应当制定相应的质量目标,不断提升自身的测评质量和管理水平。

4.3.5.1.2 测评

机构应当制定相应的质量目标,不断提升自身的测评质量和管理水平。

4.3.5.1.3 测评

机构应当制定相应的质量目标,不断提升自身的测评质量和管理水平。

4.3.5.1.4 测评

理体系维护

4.3.5.2 管

测评机构应保证管理体系的有效运行,发现问题及时反馈并采取纠正措施,确保其有效性。

4.3.5.2.1 测

测评机构应当严格遵守申诉、投诉及争议处理制度,并应记录采取的措施。

4.3.5.2.2 测

4.3.6 保证能力

4.3.6.1 公正性保证能力

4.3.6.1.1 测评机构及其测评人员应当严格执行测评服务。

4.3.6.1.2 测评机构的人员应不受可能影响其测评

4.3.6.2 可靠与保密性保证能力

4.3.6.2.1 测评机构的单位法人记录。

4.3.6.2.2 测评机构应通过提供其机构合规、产权关系明晰,资

4.3.6.2.3 测评机构应建立并保

有关管理规范和技术标准,开展客观、公正、安全的测  
评结果的来自于商业、财务和其他方面的压力。

人及主要工作人员仅限于中华人民共和国境内的中国公民,且无犯罪  
单位性质、股权结构、出资情况、法人及股东身份等信息的文件材料,证  
资金注册达到要求(500万元)。  
存工作人员的人员档案,包括人员基本信息、社会背景、工作经历、培训

4.3.6.2.4 测评机构使用的测试设备和工具应具有全面的**功能列表**,且不存在**功能列表之外**的**隐蔽**  
功能。

4.3.6.2.5 测评机构应重视**安全保密**工作,指派**安全保密**工作的**责任人**。

4.3.6.2.6 测评机构应依据**保密管理制度**,定期对**工作人员**进行**保密教育**,测评机构和测评人员应当保  
守在测评活动中知悉的**国家秘密**、**工作秘密**、**商业秘密**、**个人隐私**等。

4.3.6.2.7 测评机构应建立**数据备份**和**灾难恢复**计划,并定期**演练**和**更新**,确保在发生**数据丢失**或**灾难**时,能够**及时**恢复数据。

4.3.6.2.8 测评机构应采取**技术**和**管理**措施来确保**等级测评**和**安全保密**工作,这些措施包  
括但不限于:

- a) 被测评单位提供的资料;
- b) 等级测评活动生成的数据和记录;
- c) 依据上述信息做出的分析和专业判断。

4.3.6.2.9 测评机构应借助**所有**有效的**技术手段**,确保**等级测评**和**安全保密**工作**整个**生命周期期间的**安全**和**完整**。

4.3.6.3 测评方法与程序的规范性

与等级测评工作有关的所有工作程序,应符合**标准要求**,并**记录**或**备案**。测评机构应保  
证**在**等级测评**前**测评**方案**已**完成**。

4.3.6.4 测评记录的规范性

测评机构应保证测评记录内容和管理的规范性:

a) 测评记录应当**清晰**规范,并获得被测评方的**书面**确认;

测评机构应具有**安全**保管记录的能力,所有**测评记录**应**保存**3年以上。

b) 测

测评报告的规范性

4.3.6.5 测

机构应保证测评报告内容和出具过程管理的规范性:

测评机

测评机构应按照**公安**行政主管部门统一制订的**网络安全**等级保护**测评报告**模版格式出具**测**  
**评**报告;

a) 测

测评报告应包括所有**测评**结果、根据这些结果做出的**专业**判断以及**理解**和**解释**这些结果所需  
的所有**信息**,以上**信息**均应**正确**、**准确**、**清晰**地表述;

b) 测

要由

- c) 测评报告由测评项目组长作为第一编制人,技术主管(或质量主管)负责审核,机构管理者或其授权人员签发或批准;
- d) 能力评估合格的测评机构应对出具的等级测评报告统一加盖测评机构能力合格专用标识并登记归档。

### 4.3.7 风险控制能力

4.3.7.1 测评机构应充分估计测评可能给被测系统带来的风险,风险包括但不限于以下方面:

- a) 测评机构由于自身能力或资源不足造成的风险;
- b) 测试验证活动可能对被测系统正常运行造成影响的风险;
- c) 测试设备和工具接入可能对被测系统正常运行造成影响的风险;
- d) 测评过程中可能发生的被测系统重要信息(如网络拓扑、IP 地址、业务流程、安全机制、安全隐患和有关文档等)泄漏的风险等。

4.3.7.2 测评机构应通过多种措施对上述被测系统可能面临的风险加以规避和控制。

### 4.3.8 可持续性发展能力

4.3.8.1 测评机构应根据自身情况制定战略规划,通过不断的投入保证测评机构持续建设和发展。

4.3.8.2 测评机构应根据国家法律法规、标准规范和客户要求,制定年度、中期、长期发展目标,逐步提升质量管理能力。

4.3.8.3 测评机构应根据自身能力做好资源规划,并在项目实施前进行审核。

## 4.4 II级测评机构能力要求

### 4.4.1 基本条件

测评机构应当具备以下基本条件:

a) 在中华人民共和国境内注册成立,由中国公民、法人投资或者国家投资的企事业单位;

c) 具有网络安全的检测实验室,具备一定规模的网络安全检测能力;

d) 具有网络安全和信息安全检测认证技术支撑能力;

e) 具有固定的办公场所,配备满足测评业务需要的检测评估工具、实验环境等;

f) 具有完备的安全保密管理、项目管理、质量管理、人员管理、档案管理和培训教育等规章制度;

g) 不涉及网络安全产品开发、销售或信息安全系统集成等可能影响测评结果公正性的业务(自用);

h) 应配备的其他条件。

### 4.4.2 组织管理能力

4.4.2.1 测评机构管理者应掌握等级保护政策文件,熟悉相关的标准规范。

4.4.2.2 测评机构管理者应掌握等级测评业务,测评项目的实施应确保测评过程的独立性。

4.4.2.3 测评机构应设置满足等级测评工作需要的基本岗位,如测评技术人员、测评项目组长、技术主管、质量主管、

保密安全员、设备管理员和档案管理员等,岗位职责明确,人员稳定,其中技术主管、质量主管应为

4.4.2.4 测评机构应设置满足等级测评工作需要的基本岗位,如测评技术人员、测评项目组长、技术主管、质量主管、

保密安全员、设备管理员和档案管理员等,岗位职责明确,人员稳定,其中技术主管、质量主管应为

专职人员,不得兼任。

4.4.2.5 测评机构应制定完善的规章制度,包括但不限于以下内容:

a) 保密管理制度

应根据国家有关保密规定制定保密管理制度,制度中应明确保密对象的范围、人员保密职责

b) 项目管理制度

测评机构应依据GB/T 28149规定完备的符合自身特点的测评项目管理程序,主要应包括测

c) 设备管理制度

应包括机构人员在仪器设备管理中的相关职责、仪器设备的购置、使用和维保

d) 文档管理制度

应包括机构人员在文件档案管理中的相关职责、文件档案借阅、保管及不销毁

e) 人员管理制度

应包括人员录用、考核、培训管理以及离职等管理工作的内容和要求

f) 培训计划制度

应包括培训计划的制定、培训工作的实施、培训的考核与评价以及

g) 申诉及异议处理制度

应明确包括测评机构各岗位人员申诉、投诉和异议的

4.4.3 测评实施能力

4.4.3.1 人员能力

4.4.3.1.1 测评机构从事等级

解和掌握相关技术标准,熟悉

果做出专业判断以及出具等级

4.4.3.1.2 测评人员应参加日

人员需持证上岗

4.4.3.1.3 测评机构应配备与等级测评相适应的测评人员,测评人员应

学历和工作经验应符合下列要求:

4.4.3.1.3.1 测评机构应指定一名或数名具备全面负责等级测评实施的技术骨干,测评机构技术骨干应具备大学本科及以上学历,应在近3年内承担信息安全专业刊物发表过省部级及以上论文(或申请过著作版权)或主持过一项省部级或行业级科研项目。

4.4.3.2 测评能力

4.4.3.2.1 测评机构应具备每年开展等级测评的第三级(含)等级保护对象数量不应少于30个的能力。

4.4.3.2.2 测评机构应保证在其能力范围内从事测评工作,并有足够的资源来满足测评工作要求

在现有条件下:

a) 安全技术测评实施能力:包括物理和环境安全、网络和

通信安全、设备和计算安全、应用和数据

前主流语言和网络技术

b) 安全管理测评实施能力,包括安全策略和管理制度、安全管理机构和人员、安全建设管理、安全

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

测评准备阶段,收集被测系统的相关资料信息,填写规范的系统调查表,全面掌握被测系统

的测评需求和测评要求,开发测试和评估脚本,进行漏洞扫描和渗透测试等。

4.4.4 设施和设备安全与保障能力

4.4.4.1 测评机构应具备必要的办公环境、设备、设施和管理系统,使用的技术装备、设施原则上应当符合以下条件:

- a) 产品研发、生产单位是由中国公民、法人投资或者国家投资或者控股的,在中华人民共和国境内具有独立的法人资格;
- b) 产品的核心技术、关键部件具有我国自主知识产权;
- c) 产品研发、生产单位及其主要业务、技术人员无犯罪记录;
- d) 产品研发、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能;
- e) 对国家安全、社会秩序、公共利益不构成危害;

f) 应配备经安全认证合格或者安全检测符合要求的网络关键设备和网络安全专用产品。

4.4.4.2 测评机构应配备符合相应等级测评所需的技术装备、设施和管理系统。

测评工具应具有网络协议分析、主机漏洞扫描、安全审计、入侵检测、流量分析、设备配置、漏洞扫描、恶意代码检测等功能,可提供检测报告。

4.4.4.3 测评机构应具备符合相关要求的机房以及必要的软、硬件设备,应搭建由主流网络设备、安全设备、操作系统和数据库系统组成的基础环境,以满足网络仿真、技术培训和模拟测试的需要。

4.4.4.4 测评机构应确保测评设备和工具运行状态良好,并通过持续更新、升级等手段保证其提供准确

4.4.4.5 测评设备和工具均应有正确的标识。

4.4.4.5 测评设备和工具均应有正确的标识。

4.4.4.6 测评机构应建立专门的制度,对用于测评数据处理的计算机进行有效的运行维护,并保证计算机中数据记录的完整性、可控性。

4.4.5 质量管理能力

4.4.5.1 管理体系建设

4.4.5.1.1 测评机构应建立、实施和维护符合等级测评工作需要的文件化的管理体系,并确保测评机构各级人员能够理解和执行。

4.4.5.1.2 测评机构应制定相应的质量目标,并不断提升自身的测评质量和管理水平。

4.4.5.1.3 测评机构应明确质量管理的职责,质量主管不应受可能有损于质量

管理层沟通。

4.4.5.1.4 测评机构应建立并实施内部

4.4.5.1.5 测评机构应建立并实施内部

4.4.5.1.6 测评机构应建立并实施内部

4.4.5.2 管理体系维护

有效运行,发现问题及时反馈并采取纠正措施,确保其有效性。

4.4.5.2.1 测评机构应保证管理体系的

、投诉及争议处理制度,并应记录采取的措施。

4.4.5.2.2 测评机构应当严格遵守申诉

管理审核机制,以验证管理体系的符合性及有效性,执行审核的

4.4.5.2.3 测评机构应建立并实施内部

人员应独立于被审核部门。

4.4.5.3 质量监督能力

实施质量监督,监督员应具备丰富的安全测评经验、精通安全

测评机构应指定监督员对测评活动

4.4.6 保证能力

4.4.6.1 公正性保证能力

标准,开展客观、公正、安全的测

4.4.6.1.1 测评机构及其测评人员应当严格执行有关管理规范和技术

财务和其他方面的压力。

4.4.6.1.2 测评机构的人员应不受可能影响其测评结果的来自于商业、

4.4.6.2 可靠与保密性保证能力

4.4.6.2.1 测评机构的单位法人及主要工作人员仅限于中华人

人民共和国境内的中国公民,且无犯罪

记录。

4.4.6.2.2 测评机构应通过

明确机构名称、产权关系明

4.4.6.2.3 测评机构应建立并保存

4.4.6.2.4 测评机构应建立并保存

4.4.6.2.5 测评机构应建立并保存

4.4.6.2.6 测评机构应建立并保存

4.4.6.2.7 测评机构应建立并保存

4.4.6.2.8 测评机构应建立并保存

4.4.6.2.9 测评机构应建立并保存

4.4.6.2.10 测评机构应建立并保存

4.4.6.2.11 测评机构应建立并保存

4.4.6.2.12 测评机构应建立并保存

4.4.6.2.13 测评机构应建立并保存

4.4.6.2.14 测评机构应建立并保存

4.4.6.2.15 测评机构应建立并保存

4.4.6.2.16 测评机构应建立并保存

4.4.6.2.17 测评机构应建立并保存

4.4.6.2.18 测评机构应建立并保存

4.4.6.2.19 测评机构应建立并保存

4.4.6.2.20 测评机构应建立并保存

4.4.6.2.21 测评机构应建立并保存

4.4.6.2.22 测评机构应建立并保存

4.4.6.2.23 测评机构应建立并保存

4.4.6.2.24 测评机构应建立并保存

4.4.6.2.5 测评机构应重视安全保密工作,指派安全保密工作的责任人。

4.4.6.2.6 测评机构应依据保密管理制度,定期对工作人员进行保密教育,测评机构和测评人员应当保守在测评活动中知悉的国家秘密、工作秘密、商业秘密、个人隐私等。

4.4.6.2.7 测评机构应明确岗位保密要求,与全体人员签订《保密责任书》,规定其应当履行的安全保密义务和承担的法律 responsibility,并负责检查落实。

4.4.6.2.8 测评机构应采取技术和管理措施来确保等级测评相关信息的安全、保密和可控,这些信息包括但不限于:

- a) 被测单位提供的资料;
- b) 等级测评活动生成的数据和记录;
- c) 依据上述信息做出的分析与专业判断。

4.4.6.3 测评机构应制定等级测评活动管理程序,明确测评活动的管理职责,并应定期评审和更新。

4.4.6.4 测评机构应制定等级测评活动记录管理制度,明确记录的范围、内容、格式、保存期限等。

4.4.6.5 测评方法与程序的保证能力

4.4.6.5.1 测评机构应制定程序,保证与等级测评工作相关的所有工作程序、指导书、标准规范、工作表、核查记录表等现行有效并便于测评人员获得。

4.4.6.5.2 上述文件的发布实施应履行统一的审批程序,文件的变更和修订应有授权并及时进行版本控制。

4.4.6.6 安全管理能力

4.4.6.6.1 测评机构应制定等级测评活动安全管理制度,明确安全管理的范围、内容、格式、保存期限等。

4.4.6.6.2 测评报告的规范性

测评机构应保证测评报告内容和格式符合相关标准的要求。

4.4.6.6 安全管理能力

4.4.7 风险控制能力

4.4.7.1 测评机构应充分估计测评可能给被测系统带来的风险,风险包括但不限于以下方面:

- a) 测评机构由于自身能力或资源不足造成的风险;

- b) 测试验证活动可能对被测系统正常运行造成影响的风险；
- c) 测试设备和工具接入可能对被测系统正常运行造成影响的风险；
- d) 测评过程中可能发生的被测系统重要信息(如网络拓扑、IP 地址、业务流程、安全机制、安全隐患和有关文档等)泄漏的风险等。

4.4.7.2 测评机构应通过多种措施对上述被测系统可能面临的风险加以规避和控制。

#### 4.4.8 可持续性发展能力

4.4.8.1 测评机构应根据自身情况制定战略规划,通过不断的投入保证测评机构的持续建设和发展。

4.4.8.2 测评机构应定期对管理体系进行评审并持续改进,不断提高管理要求。设定中、远期目标(如获得相应管理体系认定资质),通过目标的实现,逐步提升质量管理能力。

4.4.8.3 测评机构应制定并实施持续改进策略,以确保其提供在专业技能和信  
息安全方面的培训,并应  
测评工作的需要。除常规培训外,应根据人员的工作岗位需求,制定详细和有针对性  
的岗位培训、考核和评定。

4.4.8.4 测评机构应投入一定的力量从事测评实践总结和测评技术研究工作,测  
评机构和人员应定期参加行业交流,并应

### 4.5 Ⅲ级测评机构能力要求

#### 4.5.1 基本条件

网络安全等级保护测评机构(以下简称测评机构)应具备以下基本条件:

- a) 具有独立法人资格,注册资本或国家投资资金应不少于 1000 万元,独立经营核算;无违法违规记录;
- b) 产权关系明晰;注册地在中国境内;
- c) 从事网络安全服务两年以上,具备一定的网络安全检测评估能力;
- d) 从事网络安全服务的人员应不少于 10 人,其中从事网络安全检测评估的人员应不少于 5 人;
- e) 具有固定的办公场所,配备必要的检测评估工具;
- f) 具有完备的安全保密管理制度;
- g) 本不涉及网络安全产品买卖;
- h) 具备的其他条件。

#### 4.5.2 组织管理能力

4.5.2.1 测评机构管理者应掌握网络安全法律法规,并具有网络安全检测评估经验;

4.5.2.2 测评机构应制定并实施质量管理体系,并应定期开展内部审核;

4.5.2.3 测评机构应具有符合要求的检测评估工具;

4.5.2.4 测评机构应制定并实施信息安全管理制度,并应定期开展内部审核;

4.5.2.5 测评机构应具有符合要求的检测评估工具;

4.5.2.6 测评机构应具有符合要求的检测评估工具;

4.5.2.7 测评机构应具有符合要求的检测评估工具;

4.5.2.8 测评机构应具有符合要求的检测评估工具;

4.5.2.9 测评机构应具有符合要求的检测评估工具;

4.5.2.10 测评机构应具有符合要求的检测评估工具;

4.5.2.11 测评机构应具有符合要求的检测评估工具;

4.5.2.12 测评机构应具有符合要求的检测评估工具;

评工作的组织形式、工作职责,测评各阶段的工作内容和管理要求等。

c) 设备管理制度

应包括机构人员在仪器设备(含测评设备和工具)管理中的相关职责、仪器设备的购置、使用和

d) 文档管理制度

e) 人员管理制度

f) 培训教育制度

4.5.3 测评实施能力

4.5.3.1 人员能力

4.5.3.1.1 测评机构从事等级测评工作的专业技术人员(以下简称测评人员)应具有把握国家政策、理

解和掌握相关技术标准,熟悉等级测评业务流程和工作规范,能识别和依据测评标准

4.5.3.1.2 测评人员应参加由指定评估机构

人员资格认证培训。

4.5.3.1.3 测评技术人员、测评项

测评实施能力和测评人员

4.5.3.1.4 测评机构应指定一名技术主管,全面负责等级测评方面的技术工作。测评机构技

术主管应具有大学本科及以上学历,从事信息安全等级保护或等级测评工作

不少于5年,主持过2项国家或部委级科研项目。

4.5.3.2 测评能力

测评能力包括测评工具、测评方法、测评过程、测评结果、测评报告、测评

测评实施能力

a) 测评实施能力

安全等级

前五类产

安全管理

运维管理

c) 安全等级



4.5.4.5 测评设备和工具均应有正确的标识。

4.5.4.6 测评机构应建立专门的制度,对用于测评数据处理的计算机进行有效的运行维护,并保证计算机中数据记录的完整性、可控性。

### 4.5.5 质量管理能力

#### 4.5.5.1 管理体系建设

4.5.5.1.1 测评机构应建立、实施和维护符合管理测评工作需要的文件化的管理体系,并确保测评机构

可追溯,并能有效识别和记录管理体系的变更。

各层级人员能识别所

4.5.5.1.2 测评机构应建立、实施和维护符合管理测评机构和人员的能力。

4.5.5.1.2 测评机构

4.5.5.1.3 测评机构应指定一名质量主管,明确其质量保障职责,质量主管应受可能影响工作质

4.5.5.1.3 测评机

量与测评机构最高管理

量的影响,并有权

### 维护

#### 4.5.5.2 管理体系

机构应保证管理体系的有效运行,发现问题及时反馈并采取纠正措施,确保其有效性。

4.5.5.2.1 测评机

4.5.5.2.2 测评机构应建立、实施和维护符合管理测评机构和人员的能力。

4.5.5.2.3 测评机构应指定一名质量主管,明确其质量保障职责,质量主管应受可能影响工作质

### 监督能力

#### 4.5.5.3 质量监督

指定监督员对全体测评技术人员开展监督,监督内容包括现场测评活动、测评过程规范

测评机构应指

定测评结论的评审等。

#### 4.5.6 规范性保证能力

##### 4.5.6.1 公正性保证能力

客观、公正、安全的测

4.5.6.1.1 测评机构及其测评人员应当严格执行有关管理规范和技术标准,开展测评服务。

方面的压力。

4.5.6.1.2 测评机构的人员应不受可能影响其测评结果的来自于商业、财务和其他

非所依据的政策法规、

4.5.6.1.3 测评机构应以公开方式,向社会公布其开展网络安全等级保护测评工作标准和规范。

##### 4.5.6.2 可靠与保密性保证能力

中国公民,且无犯罪

4.5.6.2.1 测评机构的单位法人及主要工作人员仅限于中华人民共和国境内的

记录系统。

商、出资情况、法人及股东身份等信息的文件材料,证

4.5.6.2.2 测评机构应通过提供单位性质、股权结构

明其机构合规,产权关系明晰,资金注册达到要求。

测评机构应建立测评工作安全制度,档案记录系统安全等,并应建立测评人员身份识别、测评过程记录、测评结果记录、测评报告记录等,保障测评的稳定和可靠。

记录,专项资

测评机构使用的测试设备和工具应具备全面的功能列表,且不存在功能列表之外的隐藏

4.5.6.2.4 测

功能。

测评机构应重视安全保密工作,将安全保密工作落实到

4.5.6.2.5 测

测评机构应建立保密管理制度,定期对测评人员进行保密教育,测评机构和测评人员应保

4.5.6.2.6 测

守国家秘密、工作秘密、商业秘密、个人隐私等。

守在测评

测评机构应明确岗位保密要求,与全体人员签订保密责任书,规定其应当履行的安全保密

4.5.6.2.7 测

义务和承担的法律 responsibility, 并负责检查落实。

4.5.6.2.8 测评机构应采取技术和管理措施来确保等级测评相关信息的安全、保密和可控。这些信息包

括: a) 被测单位提供的资

b) 等级测评活动生成的

c) 依据上述信息做出的

数据

和记录

分析与专业判断。

有效的技术手段, 确保等级测评相关信息的整个数据生命周期的安全和

4.5.6.2.9 测评机构应借助有

保密

的立档存储场所和数据加密环境, 严格管理测评相关数据信息。

4.5.6.2.10 测评机构应建立

### 程序的规范性

### 4.5.6.3 测评方法与

应制定程序, 保证与等级测评工作相关的所有工作程序、指导书、标准规范、工作表  
行有效并便于测评人员获得。

#### 4.5.6.3.1 测评机构

格、核查记录表等现行

三、七、五、五、二、一、值

### 4.5.6.4 测评记录的规范性

测评机构应保证测评记录内容和管理过程的规范。

### 4.5.6.5 测评报告的规范性

测评机构应保证测评报告内容和出具过程管理的规

a) 测评机构应按照公安行政主管部门统一制定的  
报告。

d) 能力评估合格的测评机构应对出具的等级测评报告统  
一归档。

### 4.5.6.6 安全管理能力

测评机构应当制定安全方针和目标, 并在其指导下建立、实

### 4.5.7 风险控制能力

#### 4.5.7.1 测评机构应充分估计

测评可能给被测系统带来的风险, 风险包括但不限于以下方面:

a) 测评机构自身自身能力或资源不足造成的风险;

b) 测评过程可能给被测系统正常运行造成影响的

c) 测评设备和工具使用不当对被测系统正常运行造成的

d) 测评过程可能发生的被测系统重要信息泄露、数据篡改、安全故

风险等。  
对上述被测系统可能面临的风险加以规避和控制。

制定战略规划,通过不断的投入保证测评机构的持续建设和发展。  
系进行评审并持续改进,不断提高管理要求。设定中、远期目标(如  
目标的实现,逐步提升质量管理能力。

训制度,以确保其人员在专业技术和管理方面持续满足等级测评工  
作的需要。测评机构应对测评人员定期进行考核,考核不合格者应进行  
培训、考核和奖惩。

4.5.8.4 测评机构应跟踪国内外新技术、新应用的发展,通过专项课题研究和实践确保技术能力与当前  
前的技术发展同步。

#### 4.6 测评机构行为规范性要求

测评机构不得从事下列活动:

a) 影响被测等级保护对象正常运行,危害被测等级保护对象安全;

对象的商业秘密和工作秘密;

,或者在测评过程中弄虚作假,未如实出具等级测评

或泄露知悉的测评单位及被测等级保护

c) 故意隐瞒测评过程中发现的安全问题  
报告;

d) 未按规定格式出具等级测评报告;

e) 非授权占有、使用等级测评相关资料及

f) 分包或转包等级测评项目;

g) 信息安全产品(专用测评设备和工具以

h) 限定被测单位购买、使用其指定的信

i) 其他危害国家安全、社会秩序、公共利益

数据文件;

外)开发、销售和网络安全集成;

息安全产品;

查以及被测单位利益的活动。

### 5 测评机构能力评估

#### 5.1 评估流程

段、评估准备阶段、审核阶段、现场评估阶段、整改阶段

如图 1 所示,初次评估流程包括委托受理阶

和报告编制阶段。

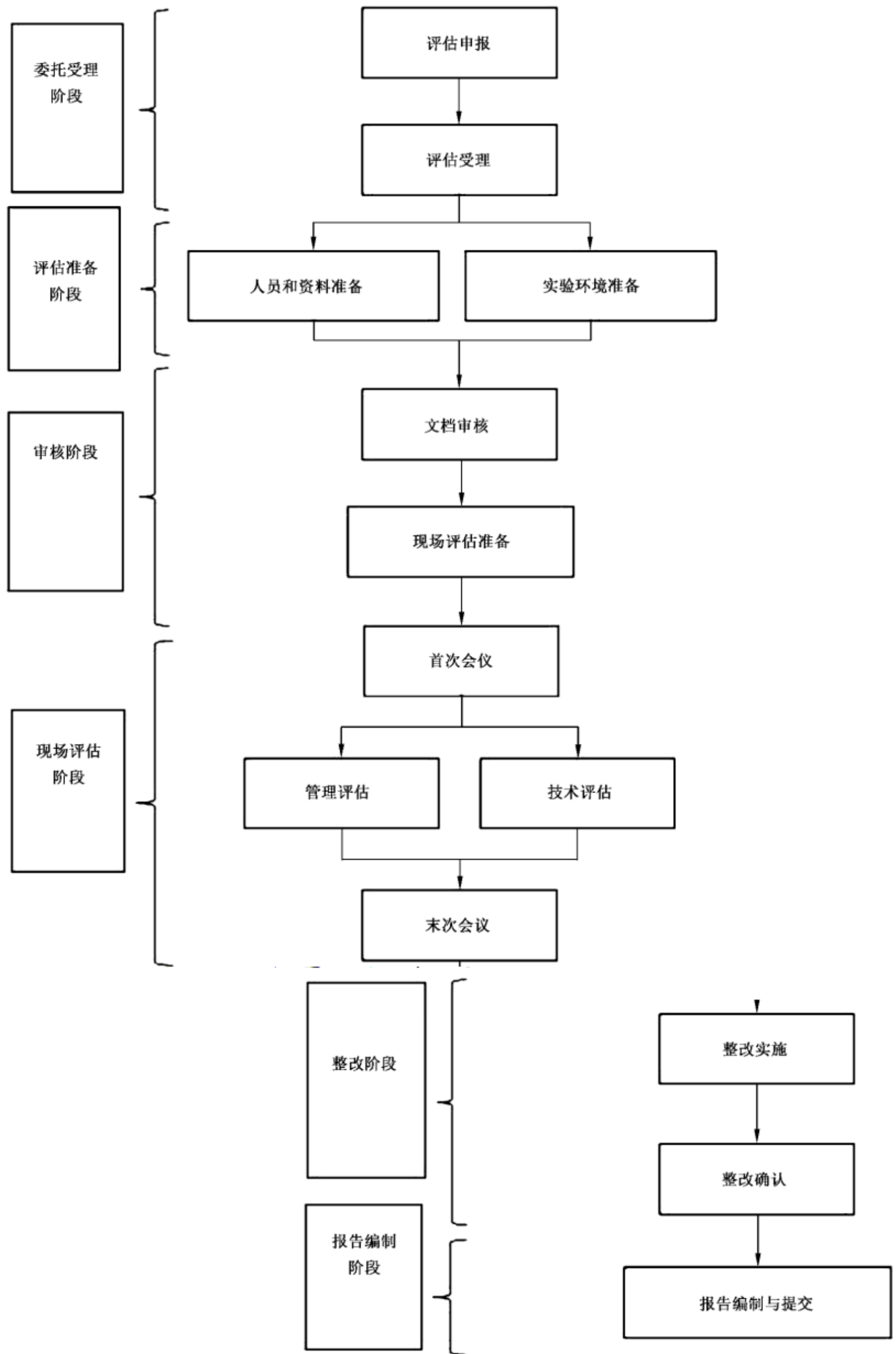


图 1 初次评估流程图

## 5.2 初次评估

### 5.2.1 委托受理阶段

#### 5.2.1.1 评估申报

测评机构向评估机构提交能力评估申报材料。

#### 5.2.1.2 评估受理

评估机构指定评估员受理测评机构的申请。评估员在确定能力评估申报材料齐全、内容符合要求后,评估机构给予受理确认。

### 5.2.2 评估准备阶段

#### 5.2.2.1 人员和资料准备

测评机构根据第4章的人员和专业技术人员做好配合

#### 5.2.2.2 实验环境准备

测评机构应建设测评能力见证实验环境,并依据等级保护相关技术标准,选取关键测评指标搭建模拟系统,并应制定等级测评前测评相关监督和管理记录等

### 5.2.3 审核阶段

#### 5.2.3.1 文档审核

管理制度、测评指导书、模拟环境的网络拓扑图、测评方案和测评计划提交评 测评机构将管理体系、管

理制度、测评指导书、模拟环境的网络拓扑图、测评方案和测评计划提交评 理制度、测评指导书、模拟环境的网络拓扑图、测评方案和测评计划提交评

#### 5.2.3.2 现场评估准备

评估组到达现场后,应以首次会议开始现场评估,首次会议上应明确评估目的、评估计划和注意事项,明确评估组人员分工和主要工作内容。

### 5.2.4 现场评估阶段

#### 5.2.4.1 首次会议

评估组到达现场后,应以首次会议开始现场评估,首次会议上应明确评估目的、评估计划和注意事项,明确评估组人员分工和主要工作内容。

#### 5.2.4.2 管理评估

评估员对测评机构管理能力相关的文档进行审核,对测评机构相关岗位人员进行访谈,根据审核情况填写能力评估管理检查表,并出具管理部分的不符合项记录。

#### 5.2.4.3 技术评估

评估员对测评机构技术能力相关文档进行审核,对测评机构技术能力进行现场见证,根据审核情况

填写能力评估技术检查表。

#### 5.2.4.4 末次会议

评估组应以末次会议结束现场评估,末次会议应总结现场评估情况和发现的问题,如对发现的问题  
有争议,测评机构可以在现场进行申述或补充证明材料,最终审核结论应得到双方确认。

#### 5.2.5 整改阶段

##### 5.2.5.1 整改实施

测评机构根据不符合项记录实施整改工作,并向评估组提交整改报告及相应证明资料作为工作有效性的证据。

##### 5.2.5.2 整改确认

评估组应分别从管理和技术两方面对测评机构提交的整改报告进行确认,整改内容不能满足要求  
的,则反馈测评机构对整改报告的修改意见,如需进行现场验证时,测评机构应予以配合。

#### 5.2.6 报告编制阶段

评估组根据能力评估管理核查表、能力评估技术核查表、现场验证记录、不符合项记录和整改报告,编制完成能力评估报告。

### 5.3 跟踪评估

或不定期的为已经获得推荐证书的测评机构是否持续地符合能力要求而在证书有效期内安排的定期

### 5.4 能力复证

测评机构获得测评机构推荐证书后,应保证测评质量和技术能力始终符合测评机构能力要求。推荐满3年应对测评机构进行能力复评,能力复评的工作流程应与初次评估的评估流程一致,评估内容应

求的总结情况见表 A.1。

各级能力增强要

1 网络安全等级保护测评机构能力增强要求各级总结情况一览表

表 A.1

I 级机构要求	II 级机构要求	III 级机构要求	序号	机构条件和能力
4.3.1 b) 产权关系明晰,注册 注册资金 500 万元以上	4.4.1 b) 产权关系明晰,注册 注册资金 1 000 万元以上	4.5.1 b) 同 II 级机构要求	1	
	基本条件			
	4.3.1 e) 具有网络安全相关 工作经历的技术和管理人 员不少于 15 人,专职渗透 测试人员不少于 2 人	4.4.1 e) 具有网络安全相关工 作经历的技术和管理人员不 少于 30 人,专职渗透测试人 员不少于 3 人		4.5.1 c) 具有网络安全相关工作经 历的技术和管理人员不少于 50 人,专职渗透测试人员不少于 5 人
	4.3.2.2 测评机构应按一定 方式组织并设立相关部门	4.4.2.2 测评机构应明确设立		4.5.2.2 同 II 级机构要求
	4.3.3.3 测评技术人员、测评项 目组长和技术主管岗位人员 应分别取得初、中、高级等级 测评师证书,测评师数量不应 少于 30 人	4.4.3.3 测评技术人员、测评项目组 长和技术主管岗位人员应分别取 得初、中、高级等级测评师证书,测 评师数量不应少于 50 人	6	4.5.3.1.3 测评技术人员、 项目组长和技术主管 人员应分别取得初、 中、高级等级测评师证书,测 评师数量不应少于 15 人
	4.5.3.1.4 同 I 级机构要求	4.5.3.1.4 测评人员除具备等级测 评师资格外,每年应参加多种形 式的测评业务和技术培训,测评师每 年培训时长累计不少于 60 学时	7	4.5.3.1.4 测评人员除 具备等级测评师资格外,每 年参加多种形式的测评 和技术培训,测评师每 年培训时长累计不少于 60 学

表 A.1 (续)

序号	机构条件和能力	I级机构要求	II级机构要求	III级机构要求	
4.5.3.1.5 等级测评机构	<p>4.5.3.1.5 测评机构应指定一名技术主管,全面负责等级测评方面的技术工作。测评机构技术主管应具有中级及以上专业技术职称,并具有下列条件:</p> <ul style="list-style-type: none"> <li>a) 具有从事信息安全领域相关工作5年以上经验;</li> <li>b) 具有主持或参与信息安全领域科研项目或工程项目的经历;</li> <li>c) 具有发表过信息安全领域学术论文或发明专利的经历。</li> </ul>			<p>4.5.3.1.5 测评机构应指定一名技术主管,全面负责等级测评方面的技术工作。测评机构技术主管应具有中级及以上专业技术职称,并具有下列条件:</p> <ul style="list-style-type: none"> <li>a) 具有从事信息安全领域相关工作5年以上经验;</li> <li>b) 具有主持或参与信息安全领域科研项目或工程项目的经历;</li> <li>c) 具有发表过信息安全领域学术论文或发明专利的经历。</li> </ul>	<p>4.5.3.1.5 测评机构应指定一名技术主管,全面负责等级测评方面的技术工作。测评机构技术主管应具有中级及以上专业技术职称,并具有下列条件:</p> <ul style="list-style-type: none"> <li>a) 具有从事信息安全领域相关工作5年以上经验;</li> <li>b) 具有主持或参与信息安全领域科研项目或工程项目的经历;</li> <li>c) 具有发表过信息安全领域学术论文或发明专利的经历。</li> </ul>
4.5.3.2.1	<p>4.5.3.2.1 测评机构应具备下列条件:</p> <ul style="list-style-type: none"> <li>a) 具有从事信息安全领域相关工作5年以上经验;</li> <li>b) 具有主持或参与信息安全领域科研项目或工程项目的经历;</li> <li>c) 具有发表过信息安全领域学术论文或发明专利的经历。</li> </ul>	<p>4.5.3.2.1 测评机构应具备下列条件:</p> <ul style="list-style-type: none"> <li>a) 具有从事信息安全领域相关工作5年以上经验;</li> <li>b) 具有主持或参与信息安全领域科研项目或工程项目的经历;</li> <li>c) 具有发表过信息安全领域学术论文或发明专利的经历。</li> </ul>	<p>4.5.3.2.1 测评机构应具备下列条件:</p> <ul style="list-style-type: none"> <li>a) 具有从事信息安全领域相关工作5年以上经验;</li> <li>b) 具有主持或参与信息安全领域科研项目或工程项目的经历;</li> <li>c) 具有发表过信息安全领域学术论文或发明专利的经历。</li> </ul>	<p>4.5.3.2.1 测评机构应具备下列条件:</p> <ul style="list-style-type: none"> <li>a) 具有从事信息安全领域相关工作5年以上经验;</li> <li>b) 具有主持或参与信息安全领域科研项目或工程项目的经历;</li> <li>c) 具有发表过信息安全领域学术论文或发明专利的经历。</li> </ul>	<p>4.5.3.2.1 测评机构应具备下列条件:</p> <ul style="list-style-type: none"> <li>a) 具有从事信息安全领域相关工作5年以上经验;</li> <li>b) 具有主持或参与信息安全领域科研项目或工程项目的经历;</li> <li>c) 具有发表过信息安全领域学术论文或发明专利的经历。</li> </ul>
4.5.3.2.2	<p>4.5.3.2.2 安全测试与分析实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面测评指南的开发、使用、维护及获取相关结果的分析和判断。测评指南应覆盖目前主流产品和相关技术。</p>	<p>4.5.3.2.2 安全测试与分析实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面测评指南的开发、使用、维护及获取相关结果的分析和判断。测评指南应覆盖目前主流产品和相关技术。</p>	<p>4.5.3.2.2 安全测试与分析实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面测评指南的开发、使用、维护及获取相关结果的分析和判断。测评指南应覆盖目前主流产品和相关技术。</p>	<p>4.5.3.2.2 安全测试与分析实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面测评指南的开发、使用、维护及获取相关结果的分析和判断。测评指南应覆盖目前主流产品和相关技术。</p>	<p>4.5.3.2.2 安全测试与分析实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面测评指南的开发、使用、维护及获取相关结果的分析和判断。测评指南应覆盖目前主流产品和相关技术。</p>
4.5.3.2.3	<p>4.5.3.2.3 安全测试与分析实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面测评指南的开发、使用、维护及获取相关结果的分析和判断。测评指南应覆盖目前主流产品和相关技术。</p>	<p>4.5.3.2.3 安全测试与分析实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面测评指南的开发、使用、维护及获取相关结果的分析和判断。测评指南应覆盖目前主流产品和相关技术。</p>	<p>4.5.3.2.3 安全测试与分析实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面测评指南的开发、使用、维护及获取相关结果的分析和判断。测评指南应覆盖目前主流产品和相关技术。</p>	<p>4.5.3.2.3 安全测试与分析实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面测评指南的开发、使用、维护及获取相关结果的分析和判断。测评指南应覆盖目前主流产品和相关技术。</p>	<p>4.5.3.2.3 安全测试与分析实施能力,包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面测评指南的开发、使用、维护及获取相关结果的分析和判断。测评指南应覆盖目前主流产品和相关技术。</p>

表 A.1 (续)

序号	机构条件和能力	I级机构要求	II级机构要求	III级机构要求
4.4.3.2.4	测评实施能力	18.1	无要求	4.4.3.2.4 测评机构应建立完善的漏洞方法研发、维护和改进机制持续提高自身测评技术能力
4.4.3.2.5	测评实施能力	18.2	无要求	4.4.3.2.5 测评机构应结合被评系统的特点
4.3.4.2	测评实施能力	18.3	4.4.4.2 测评机构应配备满足等级测评工作需要的测评设备和工具,如WEB安全检测工具等;在测试过程中及时发现安全问题。测评设备和工具应通过权威机构的检测并提供检测报告。	4.5.4.2 测评机构应配备满足等级测评工作需要的测评设备和工具,如WEB安全检测工具等;在测试过程中及时发现安全问题。测评设备和工具应通过权威机构的检测并提供检测报告。
4.3.4.3	设施和设备安全与保障能力	18.4	4.4.4.3 测评机构应具备符合相关要求的机房以及必要的软、硬件设备,应搭建由主流网络设备、安全设备、操作系统和数据存储设备组成的网络环境,并满足等级测评的需要。	4.5.4.3 测评机构应具备符合相关要求的机房以及必要的软、硬件设备,应搭建由主流网络设备、安全设备、操作系统和数据存储设备组成的网络环境,并满足等级测评的需要。
4.3.5.1	测评实施能力	18.5	无要求	4.5.5.1 测评机构应建立完善的制度,对测评数据管理的流程进行有效的监督维护,并保证计算机中数据记录的完整性、可控性。
4.3.5.2.3	测评实施能力	18.6	无要求	4.5.5.2.3 测评机构应建立并实施内部管理体系审核和反馈处理机制,以验证管理体系的符合性及在发现问题及时解决,并有效实施改进。
4.3.5.2.3	测评实施能力	18.7	无要求	4.5.5.2.3 测评机构应建立并实施内部管理体系审核和反馈处理机制,以验证管理体系的符合性及在发现问题及时解决,并有效实施改进。

表 A.1 (续)

序号	机构条件和能力	I 级机构要求	II 级机构要求	III 级机构要求
20	质量管理能力	无要求	4.4.5.3 测评机构应指定监督员对测评活动实施质量监督。	4.5.5.3 测评机构应指定监督员对全体测评技术人员开展监督,监督
21	机构应以公开公布其开展网络测评工作所依据的标准和规范	4.5.6.1.3 同 II 级机构要求		无要求
22	机构应建立专门场所和数据加密管理测评相关数据的发布实施的审批程序,文件应有授权并维护	4.5.6.2.1 同 II 级机构要求		无要求
23	有通过计算机数据的转移、复制和传递,应核查手段的准确性和完整性	4.5.6.3.2 同 II 级机构要求	规范性保证能力	无要求
24	机构应制定安全方针和目标,并在其指导下建立、实施和维持安全管理能力	4.4.6.6 安全管理能力	4.4.6.6 安全管理能力 测评机构应重视自身的安全	4.5.6.6 安全管理能力 测评机构应当制定安全方针和目标,并在其指导下建立、实施和维持安全管理能力
25	机构应制定并实施完善的培训制度,以确保其人员在专业和管理方面持续满足等级测评工作的需要。除常规培训外,应根据人员的工作岗位要求,制定详细	4.3.8.3 测评机构应根据培训制度做好培训工作,并保存培训和考核记录	4.4.8.3 测评机构应制定并实施完善的培训制度,以确保其人员在专业和管理方面持续满足等级测评工作的需要。除常规培训外,应根据人员的工作岗位要求,制定详细	4.5.8.3 同 II 级机构要求
26	机构应跟踪国内外新技术、新应用的发展,通过专项课题研究和实践,确保测评能力与当前的技术发展同步	4.5.8.4 测评机构应跟踪国内外新技术、新应用的发展,通过专项课	4.5.8.4 测评机构应跟踪国内外新技术、新应用的发展,通过专项课	4.5.8.4 测评机构应跟踪国内外新技术、新应用的发展,通过专项课

附录 B  
(规范性附录)

网络安全等级保护测评师能力要求

B.1 初级等级测评师应具备以下条件或能力：

- a) 了解网络安全等级保护的相关政策、标准；
- b) 熟悉信息安全基础知识；
- c) 熟悉网络安全等级保护测评标准；
- d) 熟悉信息安全产品分类，了解其功能、特点和操作方法；
- e) 熟悉信息安全产品测评方法，了解其功能、特点和操作方法；

B.2 中级等级测评师应具备以下条件或能力：

- a) 熟悉网络安全等级保护相关政策法规；
- b) 正确理解网络安全等级保护标准体系主要内容，能够跟踪国内、国际的发展；
- c) 掌握信息安全基础知识，熟悉信息安全测评方法，具有信息安全技术研究基础；

B.3 高级等级测评师

- a) 熟悉和跟踪国内、外信息安全的相关政策、法规及标准的发展；
- b) 对网络安全等级保护标准体系有深入的研究；
- c) 具有信息安全理论研究基础；
- d) 具有丰富的高级测评经验；
- e) 熟悉等级保护工作程序；

应具备以下条件或能力：

- a) 熟悉和跟踪国内、外信息安全的相关政策、法规及标准的发展；
- b) 对网络安全等级保护标准体系有深入的研究；
- c) 具有信息安全理论研究基础；
- d) 具有丰富的高级测评经验；
- e) 熟悉等级保护工作程序；



中华人民共和国  
国家标准  
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  
GB/T 36959—2018

\*

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)  
北京市西城区三里河北街16号(100045)

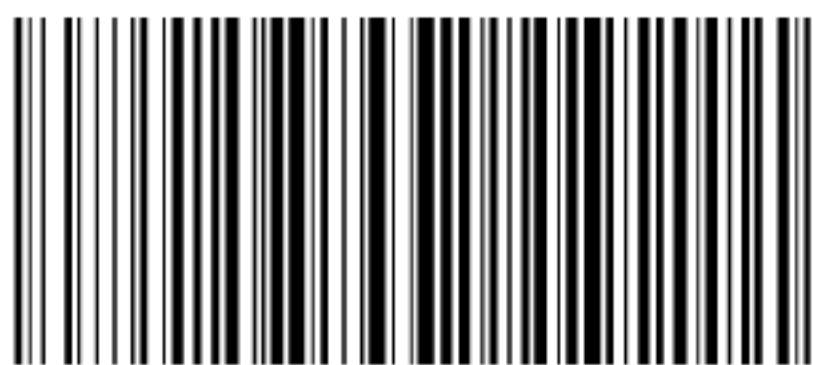
网址: [www.spc.org.cn](http://www.spc.org.cn)

服务热线: 400-168-0010

2018年12月第一版

\*

书号: 155066 · 1-61702



版权方 倡知必空

0161 36959-2018