ICS 35.040
L 80

中华人民共和国国家标准

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

Information security technology—Capability requirements and evaluation specification for assessment organization of classified protection of cybersecurity

2018-12-28 发布

2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

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 …… 16
5.2　初次评估 …… 18
5.3　期间评估 …… 19
5.4　能力复评 …… 19
附录A（规范性附录）　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 …… 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[illegible]

本标准起草单位：[illegible]

本标准主要起草人：[illegible]

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

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。

本标准适用于测评机构实施网络安全等级保护测评活动的能力评估和管理。

2　规范性引用文件

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 28448　信息安全技术　网络安全等级保护测评要求

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）其他规范的文件，对测评机构实施的符合性评估。

3.2

评估机构　evaluation organization

由获得测评机构资质认可的专业机构实施评估的机构。

3.3

初次评估　first-time evaluation

对申请测评机构资质认可的机构进行的首次评估。

3.4

期间评估　continuous evaluation

为了保持在证书有效期内获得测评机构资质认可的机构持续符合能力要求的评估、监督活动。

3.5

能力复评　capability review

测评机构获得证书有效期结束前，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。

3.6

评估员　evaluator

4 测评机构能力要求

4.1 测评机构的分级

测评机构的级别代表了网络安全等级保护测评机构技术水平和业务服务能力的差异。测评机构按能力要求分为三级，级别由低到高依次是初级、中级、高级，具体要求见表3。

4.2 等级测评人员的分级

测评机构从事等级测评工作的人员按能力要求分为三级，级别由低到高依次是初级、中级、高级，具体要求见表3。

4.3 Ⅰ级测评机构能力要求

4.3.1 基本条件

测评机构应当具备以下基本条件：

4.3.2 组织管理能力

4.3.2.1 测评机构管理体系的组织架构

4.3.2.2 测评机构管理体系的管理制度

4.3.2.3 测评机构管理体系的质量控制

4.3.2.4 测评机构管理体系的人员管理

4.3.2.5 测评机构管理体系的文档管理

4.3.3 测评实施能力

测评机构应能按GB/T 28448制定完备的、符合自身特点的测评项目管理制度，主要包括测评对象确定、测评指标确定、测评工具接入、测评指导书开发、测评方案编制、风险规避、保密管理、回避制度、文档管理、测评队伍培训计划等。

4.3.4 人员管理能力

4.3.3.2　测评能力

4.3.3　测评实施能力

准、规范开展测评方案、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。

4.3.4 设施和设备安全与保障能力

4.3.4.1 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

4.3.5 质量管理能力

4.3.5.1 管理体系建设

4.3.5.1.1 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

4.3.5.2 管理体系维护

4.3.5.2.1 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

4.3.6 保证能力

4.3.6.1 公正性保证能力

[illegible]

4.3.6.1.1 测评机构及其测评人员应当遵守相关法律法规的规定，开展客观、公正、安全的测[illegible]

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结果的来自于商业、财务和其他方面的压力。

4.3.6.2 可靠与保密性保证能力

国境内的中国公民，且无犯罪

4.3.6.2.1 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记录。

4.3.6.2.2 测评机构应通过提供单位发质、股权结构、出资情况、法人及

4.3.6.2.3 测评机构应建立并保持工作人

4.3.6.3 测评方法与程序的规范性

4.3.6.3.1 测评机构应保证其在作为有关的质量要求与准则实施测评前，应制定测评方案，方案应规定测评对象、测评指标、测评内容、测评实施过程、测评结果判定原则和单项测评结果汇总分析方法等内容，并应形成文档。

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，并应得到测评人员的签字确认；

b) 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三年以上；

4.3.6.5 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范性。

a) 测评机构应依据公安机关或主管部门统一制订的网络安全等

报告模板格式出具测评

b) 测评机构应保证测评报告的测评结论客观、准确，并应得到测评

4.3.7 风险控制能力

4.3.8 可持续性发展能力

4.4 Ⅱ级测评机构能力要求

4.4.1 基本条件

4.4.2 组织管理能力

专职人员，不得兼任。

4.4.2.5 测评机构应制定完善的保密制度，包括但不限于以下内容：

a) 保密管理制度

[illegible]

[illegible]

[illegible]

[redacted]

4.4 设施和设备安全与保障能力 4.4

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： 4.4

[redacted]

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

4.4.4.5 测评设备和工具应有正确的标记

4.4.5 质量管理能力

4.4.5.1 管理体系建设

本系，并确保测评机构

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
各级人员能够理解和执行。

4.4.5.2 管理体系维护

4.4.5.3 质量监督能力

对测评活动实施质量监督，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

4.4.6 保证能力

4.4.6.1 公正性保证能力

影响其测评结果的来自于商业、财务和其他方面的压力

4.4.6.2 可靠与保密性保证能力

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

4.4.6.2.1 测评机构的单位法人及主

4.4.6.2.2 测评机

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、教育

4.4.6.2.3 测评机构应当在

4.4.6.2.4 测评机构应

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 测评机构应与被测单位签署保密协议，要求其对测评过程中获悉的被测单位商业秘密、测评过程中产生的阶段性报告、记录和结果数据等承担保密义务。

4.4.6.2.7 测评机构应对测评人员开展安全保密教育与培训，与其签署保密责任书，规定其应当履行的安全保密义务和承担的法律责任，并负责检查与监督。

4.4.6.2.8 测评机构应采取有效措施保证在测评过程中对获取的被测单位相关资料、数据文档等进行安全存储，使其不被泄漏、破坏和篡改。

4.4.6.2.9 应对测评过程中所获取的被测单位重要数据以及在测评过程中产生的重要数据及时备份。

4.4.6.2.10 测评机构应建立文档的定期存储

4.4.6.3 测评方法与程序的保证能力

4.4.6.3.1 测评机构应制定规范的测评方案，经过审核批准后实施。测评方案至少应包括测评对象、测评指标、测评内容及其选择依据、测评工具接入点、测评指南、测评风险规避等内容。

4.4.6.4 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：

4.4.6.5 测评报告的规范性

4.4.8.6 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

a) 测评机构由于自身能力或资

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[illegible]

d) [illegible]

4.4.7.2 测评机构应[illegible]

4.4.8 自我保持和发展能力

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 [illegible]

4.4.8.3 [illegible]

4.4.8.4 测评机构应投入专门的力量从事测评实践总结和测评技术研究工作，测评机构间应进行经验交流[illegible]

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Ⅲ级测评机构应具备以下基本条件：

a) 在中华人民共和国境内[illegible]

b) 产权关系明晰，注册资金1000万元以上，独立经营核算，无违法违规记录；

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) [illegible]

e) [illegible]岗位职责清晰，且人员相对稳定；

f) 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；

g) 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；

h) 不涉及网络安全产品开发、销售或信息系统安全集成等可能影响测评结果公正性的业务（自用除外）；

i) [illegible]

4.5.2 组织管理能力

4.5.2.1 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。

4.5.2.2 测评机构应明确设立开展等级测评业务的部门，确保测评活动的独立性[illegible]

4.5.2.3 [illegible]

4.5.2.4 测评机构应设置适于等级测评工作需要的技术岗位，如测评技术员、测评项目组长、技术主管、质量主管[illegible]

[illegible]

4.5.3 [illegible]

测评机构应[illegible]

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

c) 文档管理制度

应包括机构人员在测评文档（含电子文档）管理中的相关职责、档案借阅、保管直至销毁等各项

规定等。

d) 人员管理制度

应包括机构人员在测评人员的录用、考核、奖惩管理及素质和能力要求

e) 培训制度

应包括机构对测评人员的培训计划、培训内容、培训组织形式、培训记录

要求。

g) 申诉、投诉及争议处理制度

应明确规定测评机构各相关人员在申诉和争议处理

实施能力

4.5.3 测评

员能力

4.5.3.1 人

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）应具有相应国家政策、

力

4.5.3.2 测评能

4.5.4.5 测评设备和工具均应有正确的标识。

4.5.5 质量管理能力

4.5.5.1 管理体系建设

4.5.5.2 管理体系维护

4.5.5.3 质量监督能力

4.5.6 规范性保证能力

4.5.6.1 公正性保证能力

4.5.6.2 可靠与保

4.5.6.2.1 测评机

4.5.6.2.2 测评机构应通过提供单位性质、股权结构、出资情况、法人及股东身份等信息的文件材料，证明其机构合规、产权关系明晰，资金注册达到要求。

义务和承担的法律责任，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

[redacted]

保密。

4.5.6.2.10 测评机构应建立存储场所和数据加密措施，严格管理测评相关数据信息。

4.5.6.3 测评方法与程序的规范性

[redacted]

测评机构应保证测评记录内容和管理的规范性。

[redacted]

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范性：

a) 测评机构应按照公安行政主管部门统一制定的网络安全等级保护测评报告模版格式出具测评报告。

[redacted]

4.5.6.6 安全管理能力

[redacted]

4.5.7 风险控制能力

4.5.7.1 测评机构应系统分析测评活动可能给被测系统带来的风险，风险包括但不限于以下方面：

[redacted]

以规避和控制。

测评机构的持续建设和发展。

评机构行为规范性要求

测评机构不得从事下列活动：

构能力评估

流程



图 1 现场评估流程图

5.2 初次评估

5.2.1 委托受理阶段

5.2.1.1 评估申报

5.2.1.2 评估受理

求 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

5.2.2 评估准备阶段

5.2.2.1 人员和资料准备

能力要求，逐项对照，准备资料，接受现场能力评估前相关管理人

测评机构根据第4章的测评机构能
员和专业技术人员做好配合准备工作。

5.2.2.2 实验环境准备

5.2.3 审核阶段

5.2.3.1 文档审核

5.2.3.2 现场评估准备

5.2.4 现场评估阶段

5.2.4.1 首次会议

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

评估组到达现场后，应以首次会议开始

5.2.4.2 管理评估

5.2.4.3 技术评估

对发现的问题

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

提交整改报告及相应证明资料作为工作有

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

效性的证据。

5.2.5.2 整改确认

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

5.3 [illegible]

书有效期内安排的定期或不定期

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

5.4 能力复评

力始终符合测评机构能力要求。推

次评估的评估流程一致，评估内容应

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

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

附 录 A

（规范性附录）

[illegible]

[illegible]

[illegible]



表 A.1（续）

序号	机构条件和能力	1级机构要求	2级机构要求	3级机构要求
[illegible]	[illegible]	[illegible]	无要求	4.4.3.2.4 测评机构应建立完善的测评方法研发、维护和更
[illegible]	测评实施能力	4.4.3.2.5 测评机构应结合被	4.5.3.2.5 测评机构应针对被测系	无要求
[illegible]	[illegible]	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	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，	4.3.4.2 测评机构应配
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

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
			4.4.5.2 测评机构应指定监督	

附 录 B
（规范性附录）
网络安全等级保护测评机构能力要求

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) 具有[illegible]

d) 具有[illegible]

e) 具有[illegible]

f) 具有[illegible]

g) 具有[illegible]

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
北京市朝阳区惠新东街甲4号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2018年12月第一版
*
书号:155066·1-61702

版权专有 侵权必究