ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36950—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 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　缩略语 …… 2
5　测试环境 …… 2
6　测试设备 …… 3
7　测试方法 …… 4
8　测试报告 …… 15
附录A（资料性附录）测试报告模板 …… 16

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（SAC/TC 260）提出并归口。

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。

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

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 evalua

3.2

评估机构　evaluation org

3.3

初次评估　first-time e

3.4

期间评估　continuo

的评估、检查活动。

3.5

能力复评　capabili

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[illegible]

[illegible]

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[illegible]

[illegible]

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：

[illegible]

4.3.2 组织管理能力

[illegible]

[illegible]

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，档案供阅，但管[illegible]

a) 人员管理制度

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。

[illegible]

b) 由于[illegible]

[illegible]

4.3.3 测评实施能力

4.3.3.1 人员能力

4.3.3.1.1 测评机构从事第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[illegible]

[illegible]

4.3.3.1.2 [illegible]

[illegible]

4.3.3.1.3 [illegible]

[illegible]

4.3.3.1.4 [illegible]

[illegible]

4.3.3.2 测评能力

4.3.3.2.1 测评[illegible]

[illegible]

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，[illegible]

[illegible]

准、规范及测评方案、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获得认可。

关于测评结论的产生方式，应注意以下几个方面的要求：

a) 给出测评结论的产生方法，应是通过综合分析多个测评对象和测评实施过程后给出的；

b) 应给出每个测评对象的测评结果；

c) 应给出针对每个测评对象的测评证据；

d) 应对测评证据和测评结果进行充分描述，证明其正确性、客观性和可重复性；

e) 应给出对单项测评结果的判定，以及基于这些单项测评结果的总体测评结论；

f) 应对测评过程中发现的问题进行总结，并给出相应的改进建议。

4.3.3 测评指导

测评机构应遵循测评方案的总体要求生成测评指导书，以指导测评人员有效实施测评活动。

测评指导书的内容应包括但不限于：

a) 测评实施的时间、资源要求；

b) 测评实施的详细过程；

c) 测评过程中的安全事故应急处置措施；

d) 测评过程中发现问题的处理流程。

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、设施原则上应当符合国家有关规定，满足测评工作需要。

4.3.4.2 测评机构应具备必要的测评设备，包括但不限于：

a) 漏洞扫描设备；

b) 渗透测试设备；

c) 协议分析设备；

d) 代码审计设备；

e) 移动终端测试设备；

f) 物联网测试设备；

g) 工控测试设备；

h) 大数据测试设备；

i) 云计算测试设备；

j) 其他测评设备。

4.3.4.3 测评机构应具备必要的测评工具，包括但不限于：

a) 漏洞扫描工具；

b) 渗透测试工具；

c) 协议分析工具；

d) 代码审计工具；

e) 移动终端测试工具；

f) 物联网测试工具；

g) 工控测试工具；

h) 大数据测试工具；

i) 云计算测试工具；

j) 其他测评工具。

4.3.4.4 测评机构应具备必要的测评设施，包括但不限于：

a) 电磁屏蔽室；

b) 信号发射接收装置；

c) 其他测评设施。

4.3.4.5 测评机构应具备必要的测评场地，包括但不限于：

a) 用于开展现场测评活动的办公场地；

b) 用于开展非现场测评活动的办公场地；

c) 用于开展测评设备接入测试的场地；

d) 用于开展测评人员培训的场地；

e) 用于开展保密测评活动的场地。

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，并确保测评机构各级人员能够理解和执行。

4.3.5.1.2 测评机构应建立并维护与测评相关的质量管理方面的记录，包括但不限于：

a) 测评合同；

b) 测评方案；

c) 测评指导书；

d) 测评结果记录；

e) 测评报告；

f) 测评项目总结；

g) 测评人员培训记录；

h) 测评设备和工具维护记录；

i) 测评场地和环境维护记录；

j) 保密协议；

k) 其他。

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，确保其有效性。

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[illegible]

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

[illegible]民共和国境内的中国公民，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[illegible]记录。

[illegible]

4.3.6.2.3 测评机构应建立并保[illegible]

[illegible]

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：

[illegible]

4.3.6.5 测评报告的规范性

[illegible]规范性：

[illegible]的网络安全等级保护测评报告模版格式出具测评

测评机构应保证测评报告内容和出具过程管理的

a） 测评机构应按照公安行政主管部门统一制订[illegible]

[illegible]

[illegible]

4.3.7 风险控制能力

[illegible]

4.3.8 可持续性发展能力

[illegible]

4.4 Ⅱ级测评机构能力要求

4.4.1 基本条件

[illegible]

4.4.2 组织管理能力

[illegible]

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]

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：

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 测评设备和工具均应有正确的标识。

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

各级人员能够理解和执行。

5.2 管理体系维护

4.4.5

4.4.5.3 质量监督能力

测评机构应指定监督员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

4.4.6 保证能力

4.4.6.1 公正性保证能力

4.4.6.1.1

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、财务和其他方面的压力。

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民共和国境内的中国公民

4.4.6.2.2 测评机构应通过描述单位性质、股权结构、出资情况、法人及股东身份等信息

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。

[redacted]

[redacted]

[redacted]

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

[illegible]

e) 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、保管直至销毁的各项规定等。

[illegible]

f) 人员管理制度

[illegible]

g) 申诉、投诉及争议处理制度

应明确包括测评机构各岗位上是在[illegible]

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[illegible]

4.5.3.2 测评能力

[illegible]

4.5.4.5 测评设备和工具均应有正确的标识。

[illegible]

4.5.5 质量管理能力

4.5.5.1 管理体系建设

[illegible]

维护

4.5.5.2 管理体系

[illegible]

4.5.5.3 质量监督能力

[illegible]

4.5.6 规范性保证能力

4.5.6.1 公正性保证能力

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，正确客观、公正、安全的测

[illegible]

证能力

4.5.6.2 可靠与保密性保

[illegible]

4.5.6.2.1 测评机构的单

[illegible]

4.5.6.2.2 测评机构应通过提供单位性质、股权结构、正资情况、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。

[illegible]

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[illegible]

[illegible]

[illegible]的资料；

[illegible]成的数据和记录；

[illegible]

[illegible]

[illegible]

[illegible]

4.5.6.2.10 测评机构应建立专门的[illegible]存储场所和数据加密环境[illegible]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

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

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。

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

4.5.6.6 安全管理能力

[illegible]

[illegible]

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：

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]


委托受理
评估申报
评估准备
文档审核
审核阶段
首次会议
现场评估
技术评估
管理评估
整改阶段
整改实施

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

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

测评机构根据第4章的测评机构能力要求，逐项对照，准备资料，接受现场能力评估的相关管理人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

评估准备

5.2.3.2 现场

5.2.4 现场评估阶段

5.2.4.1 首次会议

5.2.4.2 管理评估

5.2.4.3 技术评估

5.2.4.4 末次会议

对发现的问题

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

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

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

效性的证据。

5.2.5.2 整改确认

5.2.6 报告编制阶段

记录、不符合项记录和整改报告。

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

5.3 复评

证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

5.4 能力复评

术能力始终符合测评机构能力要求。推

与初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

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

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

[illegible]

表 A.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

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
1	[illegible]	4.3.1 b) 产权关系明晰，注	4.4.1 b) 产权关系明晰，注册	4.5.1 b) 同Ⅱ级机构要求
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

表 A.1(续)

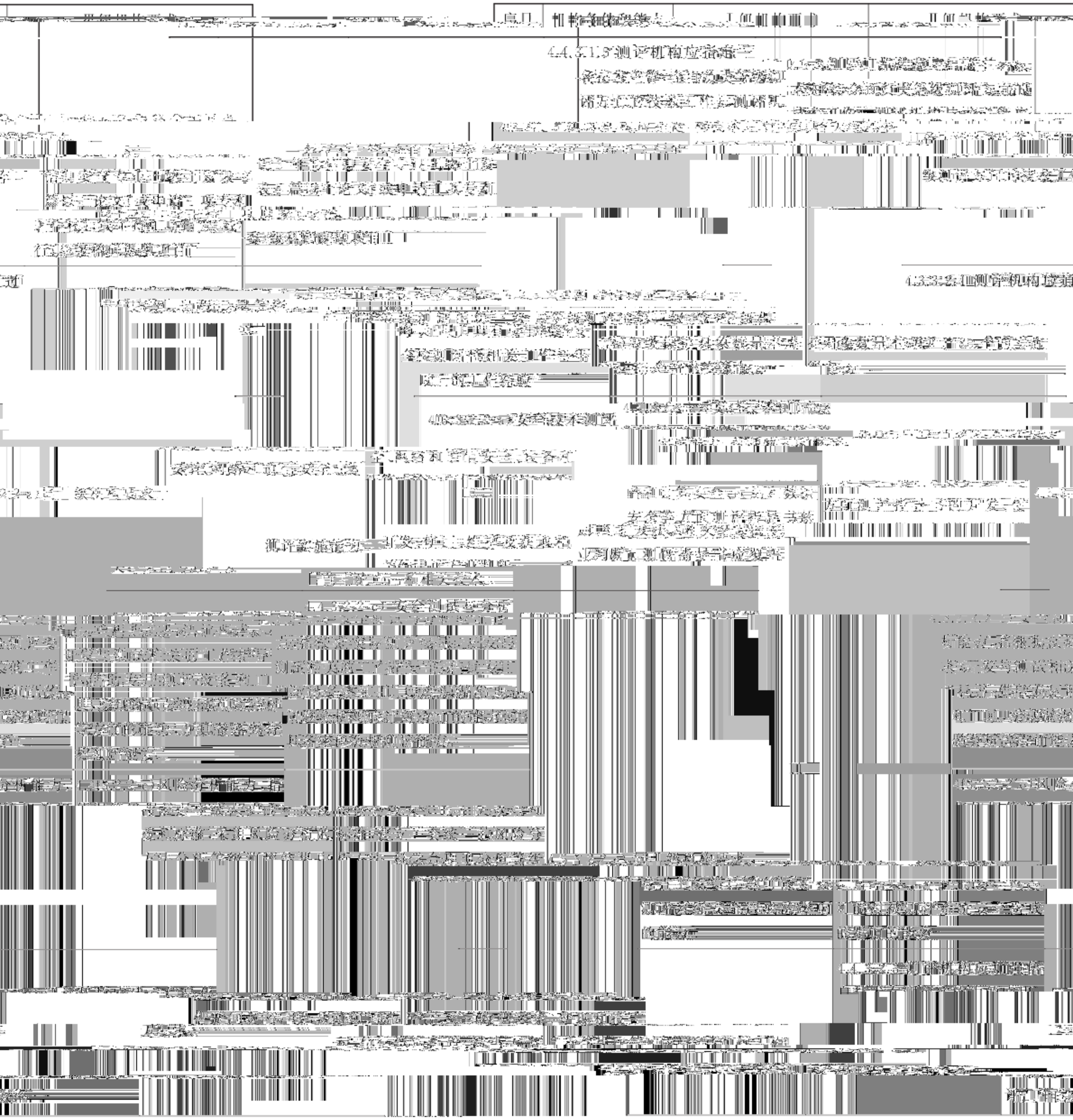

表 A.1（续）

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 测评机构应建立完善的测评方法研发、维护和更	4.5.3.2.4 同Ⅱ级机构要求	无要求
	测评实施能力			
		4.3.4.2 测评机构应配备满足等级测评工作需要的测	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，
		4.3.5.1.10 测评机构应建立、实施和维护符合等级测评	4.4.5.1.10 测评机构应建立、实施和维护符合等级测评	4.5.5.1.10 测评机构应建立并维护符合等级测评工作需
	质量管理能力		4.4.6.2.3 测评机构应建立并	4.5.6.2.3 测评机构应建立并

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

附 录 B
（规范性附录）

[illegible]

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[illegible]

b) 熟悉信息安全基础知识；

[illegible]

B.2 [illegible]

[illegible]

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[illegible]

[illegible]

e) 能够独立开发测评[illegible]

[illegible]

B.3 [illegible]

[illegible]

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

*

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

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