ICS 35.040
L 80

中华人民共和国国家标准

GB/T 369

信息安全技术 网络安全等级保护

测评机构管理要求

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

Information security technology—Capability requirements and evaluation specification for assess

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 …… 2
4.4　Ⅱ级测评机构能力要求 …… 6
4.5　Ⅲ级测评机构能力要求 …… 11
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 …… 20
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别结情况一览表 …… 21
附录B（规范性附录）　等级测评人员能力要求 …… 24

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。

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申请网络安全等级保护测评机构能力认可和对测评机构能力进行评估。

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）其他规范对测评机构实施网络安全等级保护测评的能力和条件进行的评估。

3.2

评估机构　evaluation organization

由申请测评机构能力认可的组织。

3.3

初次评估　first-time evaluation

对测评机构首次进行的能力评估。

3.4

期间评估　continuous evaluation

为了保持测评机构能力满足要求而在证书有效期内实施的定期或不定期的评估、监督活动。

3.5

能力复评　capability review

测评机构在证书有效期结束时，为了延续证书有效期，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

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 测评机构的级别代表了网
级高依次是Ⅰ级、Ⅱ级和Ⅲ级，其中Ⅰ级是最低级别的能力要求条款在原 能力要求分为三级，级别由

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
级要求见附录B。

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 测评机构应当具有开展等级测评工作 满足相关的标准要求

4.3.2.2

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

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

4.3.5.2 管理体系维护

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有关管理规范和技术标准，及时客观、公正、安全地开展测评活动，出具测评报告。

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

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国境内的中国公民，且无犯罪记录。

4.3.6.2.2 测评机构应通过提供单位发函、股权结构证明资质申请法人及股东身份等信息的支撑材料证明其机构性质、经营范围等满足国家关系明晰、资金来源合规要求的情况。

4.3.6.2.3 测评机构应建立并保存工作人员的人员档案，包括但不限于本人及其相关直系亲属的身份证明、学历证明、工作经历、社会关系、无犯罪记录证明等。

4.3.6.2.4 测评机构应与每个工作人员签署保密协议，协议中应明确保密内容（包括但不限于测评对象、测评结果、被测评对象的相关数据等）、违约责任等。

4.3.6.2.5 测评机构应与每个工作人员签署岗位责任协议，协议中应明确岗位安全责任、违反岗位责任协议的惩罚措施等。

4.3.6.2.6 测评机构应对每个工作人员每次接触被测评对象的活动进行详细记录和管理，包括但不限于活动时间、地点、内容等，并形成记录表单，被测评对象应对记录表单内容进行确认。

4.3.6.2.7 测评机构应使用自己的测评设备、工具和测评结果记录表单，测评设备和工具应通过必要的测试验证，确保不会影响被测评对象的正常运行，不会对被测评对象的软硬件造成破坏，不会将测评数据泄露给未授权的第三方。

4.3.6.2.8 测评机构应对测评过程中获取的被测评对象的配置文件、用户鉴别信息、重要业务数据、系统漏洞扫描结果等敏感信息数据采取有效的保护措施，如签订保密协议、使用加密通道传输、在受控环境中处理、采用水印技术等，防止测评过程中发生数据泄露事件。

4.3.6.2.9 测评机构应建立数据使用和管理的内部控制制度，明确数据的保存环境、保存期限、使用权限、销毁要求和流程等内容，并严格执行。

4.3.6.3 测评方法与过程的规范性

测评机构应保证测评工作在实施过程中采用的测评方法、测评过程与已经备案的测评方案相一致；对测评过程中重大变更的，应依据相关管理规范重新备案或报告。测评机构应保证测评工作有序进行，保证在预定时间内完成预定的测评任务，并预留合理的时间用于问题复核和报告编制。

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) 测评机构应规范测评记录表单格式；

b) 测评机构应确保测评记录信息真实有效，测评记录包括但不限于录入测评数据的设备名称、测评项操作记录、测评结果记录、测评工具接入记录等；

c) 测评机构应规范测评记录的结果确认、归档和管理活动。

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板格式出具测评报告；

b) 测评机构应对每个测评报告的修改版本进行记录说明，并保留不同版本报告的测评记录。

4.3.7 风险控制能力

4.3.8 可持续性发展能力

4.4 Ⅱ级评价机构能力要求

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]

b) [illegible]

测评机构应依据GB/T 28449—[illegible]制定完备的实施[illegible]

[illegible]

c) 文档管理制度

[illegible]

d) 人员管理制度

[illegible]

e) 培训交流制度

[illegible]

f) 申诉投诉及争议处理制度

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

4.4.3 测评人员能力及培训要求

4.4.3.1 人员能力

[illegible]

4.4.3.1.2 测评人员应具备信息安全等级保护及相关领域知识[illegible]

4.4.3.1.3 测评机构应[illegible]

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个的实施[illegible]

4.4.3.2.2 测评人员应具备[illegible]

a) 安全技术测评实施能力：包括但不限于物理安全、网络通信安全、设备和计算安全、应用和数据[illegible]

[illegible]

[redacted]

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：

[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

4.4.5 质量管理能力

4.4.5.1 管理体系建设

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

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实施质量监督，监

4.4.6 保证能力

4.4.6.1 公正性保证能力

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、财务和其他方面的

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，且无犯罪

4.4.6.2.2 测评机构应通过指定单位维护一般状态下的情况、法人及股东身份等信息

4.4.6.2.3 测评机构应指定并保存工作人员的个人安全背景审查记录，包括但不限于

4.4.6.2.4 测评机构应建立测试设备和工具管理制度，并保证测试设备

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 [illegible]

4.4.6.2.7 [illegible]

4.4.6.2.8 [illegible]

a) [illegible]

b) [illegible]

c) [illegible]

4.4.6.2.9 [illegible]

4.4.6.2.10 测评机构应建立专门的文档存储场所和数据加密环境，严格管理测评相关数据信息。

4.4.6.3 测评方法与程序的保证能力

4.4.6.3.1 [illegible]

4.4.6.4 测评记录的规范性

[illegible]

4.4.6.5 测评报告的规范性

[illegible]

4.4.6.6 [illegible]

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) 测试验证活动可能造成测试数据泄露的风险；

d) 测试验证活动可能造成测试数据丢失的风险。

4.7.2 测评机构应制定规范的保密管理制度，明确保密范围和各类人员的保密责任。

4.4.8 其他资质要求

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。

4.5 人员能力要求

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。

4.5.2.3 测评机构应设置项目负责人岗位等级测评工作相关岗位，如测评技术员、测评组长、技术主管、质量

4.5.2.4 测评机构应按照规定等级测评工作相关岗位，如测评技术员、测评组长、技术主管、质量

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

[illegible]管直至销毁的各项

规定等。

[illegible]

[illegible]

[illegible]

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

4.5.5.1.1 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

4.5.5.2 管理体系维护

4.5.5.2.1 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。

力

4.5.5.3 质量监督能力

测评机构应指定

能力

4.5.6 规范性保证能力

证能力

4.5.6.1 公正性保证能力

构及其测评人员应当严格执行有关管理规范和技术标准，开展客观、公正、安全的测

4.5.6.1.1 测评机构

4.5.6.2 可靠与保密性保证能力

仅限于中华人民共和国境内的中国公民，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

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完全、保密和可控。这些信息包

[illegible]

[illegible]

4.5.6.2.10 测评机构应建立存储测评数据和资料的安全管理制度，规定测评过程中产生的数据和资料

[illegible]

4.5.6.3 测评方法与程序的规范性

[illegible]

测评机构应保证测评记录内容和管理的规范性。

[illegible]

4.5.6.4 测评记录的规范性

[illegible]

测评机构应保证测评记录内容和管理的规范性。

[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]

4.5.6.6 安全管理能力

[illegible]

4.5.7 风险控制能力

[illegible]

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]

4.5.8 可持续性发展能力

4.5.8.1 测评机构应根据自身情况制定

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：

5 测评机构能力评估

5.1 评估流程


委托受理
评估申报
评估准备
现场评估
技术评估
管理评估
首次会议
文档审核
审核阶段
现场审核
末次会议
审核结论
认证决定
颁发证书

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

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

5.2.4.2 管理评估

5.2.4.3 技术评估

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

5.2.5 整改阶段

5.2.5.1 整改实施

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

测评机构根据不符合项记效性的证据。

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]

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

5.4 能力复评

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

附 录 A

（规范性附录）

[illegible]

[illegible]级能力增强要求的总结情况见表 A.1。

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]

表 A.1(续)

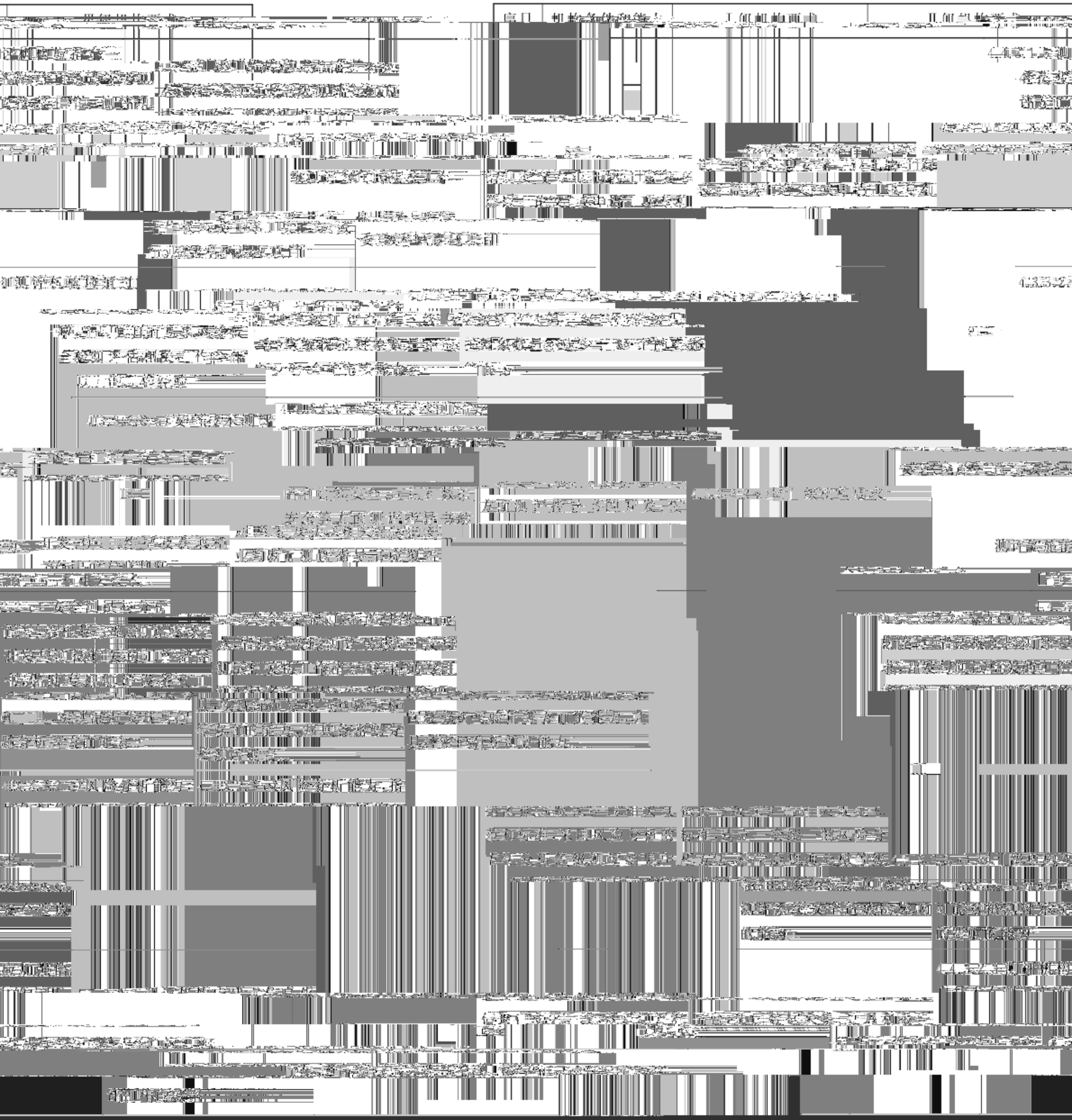


表 A.1（续）

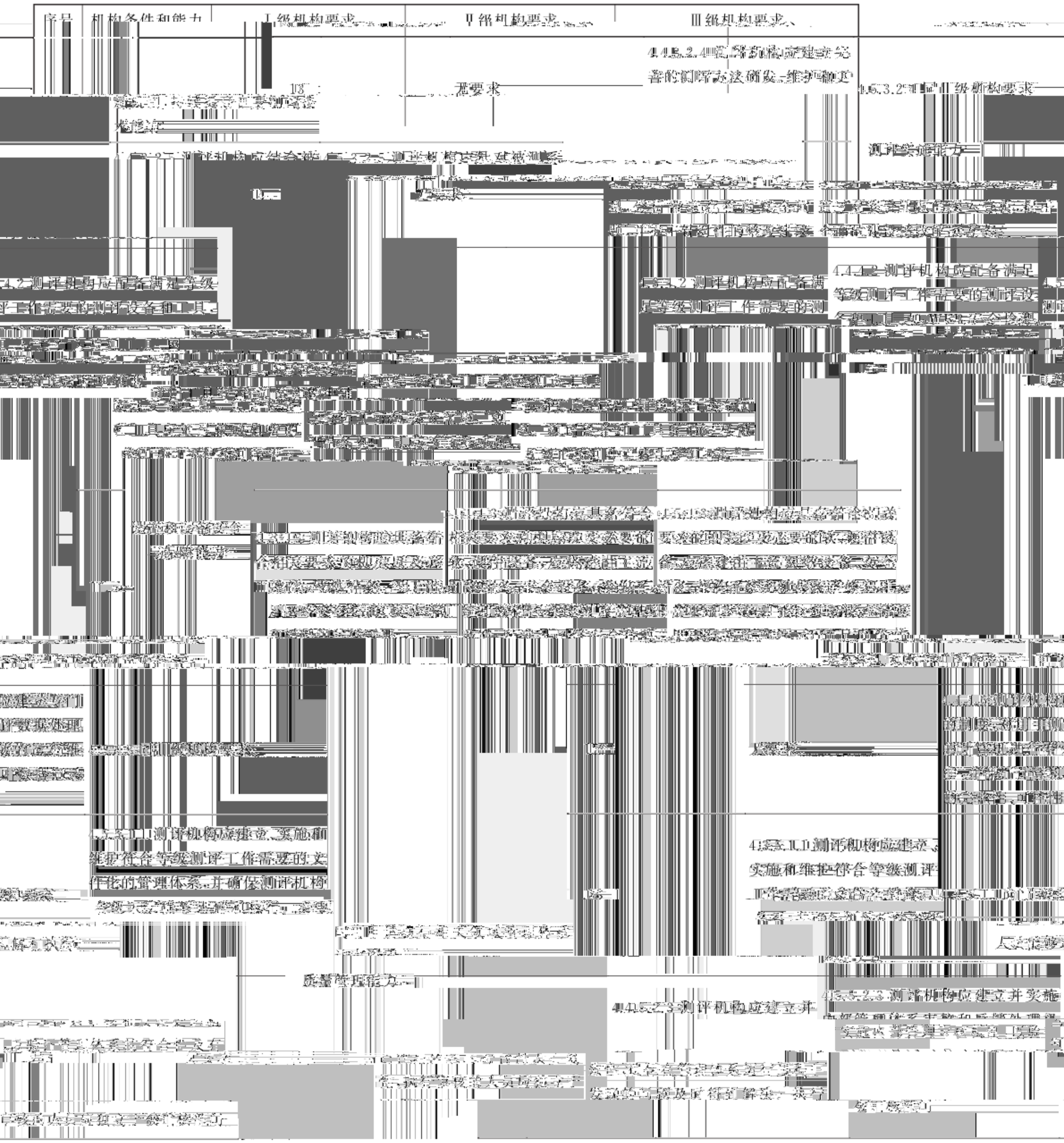


表 A.1（续）

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
			4.4.5.2 测评机构应指定监督	
			4.5.2.1 同Ⅱ级机构要求	无要求
			4.5.2.1 同Ⅱ级机构要求	无要求
			4.5.3.1 同Ⅱ级机构要求	无要求
			4.6.3.1 对所有通过计算机	
			4.6.6 安全管理能力	4.5.6.6 安全管理能力 测评机构应当制定安全方针和
			4.8.3.1 测评机构应制定并实	
				和有制度性安全计划，并进

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

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
服务热线:400-168-0010

2018年12月第一版

*

书号:155066·1-61702

GB/T 36959—2018