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 ………………………………………………… [illegible]

4.1　测评机构能力等级划分 …………………………………………… [illegible]

4.2　[illegible] ……………………………………………………… [illegible]

4.3　Ⅱ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 ………………………………………… 15

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　[illegible] ………………………………………………………… [illegible]

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

附录B（[illegible]）　[illegible]能力要求 ……… 24

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

[illegible] 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 [illegible]

[illegible]

[illegible]

[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[illegible]

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。

[illegible]等活动。

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。[illegible]

GB/T 28448 信息安全技术 [illegible]

GB/T 28449 信息安全技术 网络安全等级保护测评过程指南

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[illegible]审查、验证和评价的过程。

3.2

评估机构 evaluation organization

[illegible]

3.3

初次评估 first-time evaluation

[illegible]

3.4

期间评估 continuous evaluation

为了[illegible]推荐证书的测评机构是否持续地符合能力要求，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。

[illegible]

3.6

评估员 evaluator

[illegible]

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 [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分为三级，级别由低到高依次是初级、中级、高级，具 [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

4.3.2.1 [illegible]

4.3.2.4 [illegible]

4.3.2.5 [illegible]

[illegible]

[illegible]，但篇幅有限，[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，档案借阅[illegible]

d） 人员管理制度

[illegible]

4.3.3 测评实施能力

4.3.3.1 人员能力

4.3.3.1.1 测评机构从事等级测评工作的专业技术人员[illegible]

[illegible]

.2 测评能力

.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[illegible]年以上的[illegible]

[illegible]

4.3.3.2.2 [illegible]

[illegible]

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 [illegible]

[illegible]

4.3.4 设施和设备安全与保障能力

4.3.4.1 [illegible]

[illegible]

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 [illegible]

[illegible]

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 [illegible]

4.3.6 保证能力

4.3.6.1 公正性保证能力

4.3.6.1.1 [illegible] 测评活动。

4.3.6.1.2 测评机构及其测评人员 [illegible] 可能影响其测评结果和能力的 [illegible] 和其他方面的压力。

4.3.6.2 可靠性与保密性保证能力

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 [illegible]

4.3.6.2.3 测评机构 [illegible]

4.3.6.2.4 测评机构 [illegible]

重视安全保密工作，建立安全保密工作管理制度。

4.3.6.2.5 测评机构 [illegible]

a) 实现测评人员实名管理；

b) [illegible]

c) [illegible]

4.3.6.2.9 测评机构 [illegible]

4.3.6.3 测评方法与程序的规范性

[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。

a) 测评记录应当 [illegible]

b) [illegible]

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版格式出具测评报告。

b) 测评报告 [illegible]

[illegible]

4.3.7 风险控制能力

[illegible]

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的持续建设和发展。

4.3.8.2 [illegible]

4.3.8.3 [illegible]

4.4 Ⅱ级测评机构能力要求

4.4.1 基本条件

[illegible]

b) 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；

[illegible]

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 [illegible]

4.4.2.3 [illegible]

4.4.2.4 测评机构应设置满足等级测评工作需要的[illegible]

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：[illegible]

b) 项目管理制度：测评机构应依据 GB/T 28449 [illegible]

c) 设备管理制度：[illegible]

d) 文档管理制度：[illegible]

e) 人员管理制度：[illegible]

f) 培训教育制度：应包括培训计划的制定、[illegible]工作的实施、培训的考核等[illegible]要求。

g) 申诉、投诉及争议处理制度：[illegible]

4.4.3 测评技术能力

4.4.3.1 人员能力

4.4.3.1.1 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）[illegible]

4.4.3.1.2 测评人员应参加[illegible]

4.4.3.1.3 测评机构[illegible]

4.4.3.1.4 [illegible]

4.4.3.1.5 [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 个的实施能力。

a) 安全技术测评[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：

[illegible]

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 [illegible]

[illegible]

4.4.4.5 测评设备和工具均应有正确的标识。

[illegible]

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。

[illegible]

4.4.5.2 管理体系维护

4.4.5.2.1 测评机构应保证管理体系的有效运行，[illegible]

[illegible]

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 [illegible]

4.4.6 保证能力

4.4.6.1 公正性保证能力

4.4.6.1.1 [illegible]

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 [illegible]

[illegible]

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，且无犯罪记录。

4.4.6.2.2 测评机构 [illegible]

4.4.6.2.3 测评机构 [illegible]

4.4.6.2.4 [illegible] 攻击。

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 测评机构应根据保密管理制度，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责任，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与专业判断。

4.4.6.2.9 测评机构[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 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、工作表格、核查表等[illegible]

4.4.6.3.2 [illegible]

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。

[illegible]

4.4.6.5 测评报告的规范性

[illegible]

4.4.6.6 安全管理能力

[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；

[illegible]

[illegible]

4.4.7.2 [illegible]

4.4.8 [illegible]

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。

[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[illegible]

[illegible]

4.5 Ⅲ级测评机构能力要求

4.5.1 基本条件

网络安全等级保护测评机构[illegible]应具备以下基本条件：

a) [illegible]

b) [illegible]注册资金1 000万元以上，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]

[illegible]

f) [illegible]

g) [illegible]

h) [illegible]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 [illegible]

4.5.2.3 [illegible]

4.5.2.4 测评机构应设置满足等级测评工作需要的岗位，如测评技术员、测评项目组长、技术主管、质量主[illegible]

[illegible]

[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[illegible]

d) 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、销毁等各项规定等。

e) 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。

f) 培训教育制度

应包括培训计划的制定、培训工作的实施、培训考核、人员培训档案管理等内容和要求。

g) 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的职责，[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[illegible]

[illegible]

4.5.3.2 测评能力

4.5.3.2.1 测评机构[illegible]

[illegible]

[illegible]的具体结果的能力；

[illegible]的风险分析结论科学合理；

[illegible]

[illegible]分，从安全控制点间、层面间和区域间出发考虑，给出整体测评的[illegible]

[illegible]

4.5.3.2.5 测评机构应针对被测系统存在的[illegible]安全问题[illegible]分析，通过对安全问题的深入分析，提出全面的建设整改解决方案。

4.5.3.2.6 [illegible]

[illegible]具体要求如下：

a) [illegible]

b) 方案编制阶段，[illegible]

c) 现场测评阶段，严格执行测评方案和测评指导书，[illegible]测评设备和工具，规范、准确、完整地填写测评结果记录，获取足[illegible]

[illegible]证据，客观、真实、科学地反[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

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[illegible]

[illegible]

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。

4.5.5.2.2　[illegible]

4.5.5.3　质量监督能力

测评机构应指定监督员对全体测评技术人员开展监督，监督内容包括现场测评活动、测评过程规范[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，开展客观、公正、安全的测评服务。

[illegible]标准和规范。

4.5.6.2　可靠与保密性保证能力

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中国公民，且无犯罪记录。

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[illegible]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]

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与专业判断。

4.5.6.2.9 [illegible]

保密。

4.5.6.2.10 测评机构应建立专门的[illegible]存储场所和[illegible]，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

[illegible]

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的规范性：

[illegible]

c) 测评机构应具有[illegible]记录的能力，所有的测评记录应保存3年以上。

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

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]

息和有关文档等泄漏的风险等。

4.5.7.2 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。

4.5.8 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。

4.5.8.2 [illegible]

[illegible]

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) 影响被测评等级保护对象正常运行，危害被测评等级保护对象安全；
b) [illegible]
c) [illegible]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数据文件；
f) [illegible]
g) [illegible]
h) [illegible]

5 测评机构能力评估

5.1 评估流程

如图1所示，初次评估流程包括受理阶段、评估准备阶段、审核阶段、现场评估阶段、审批阶段。

[illegible]

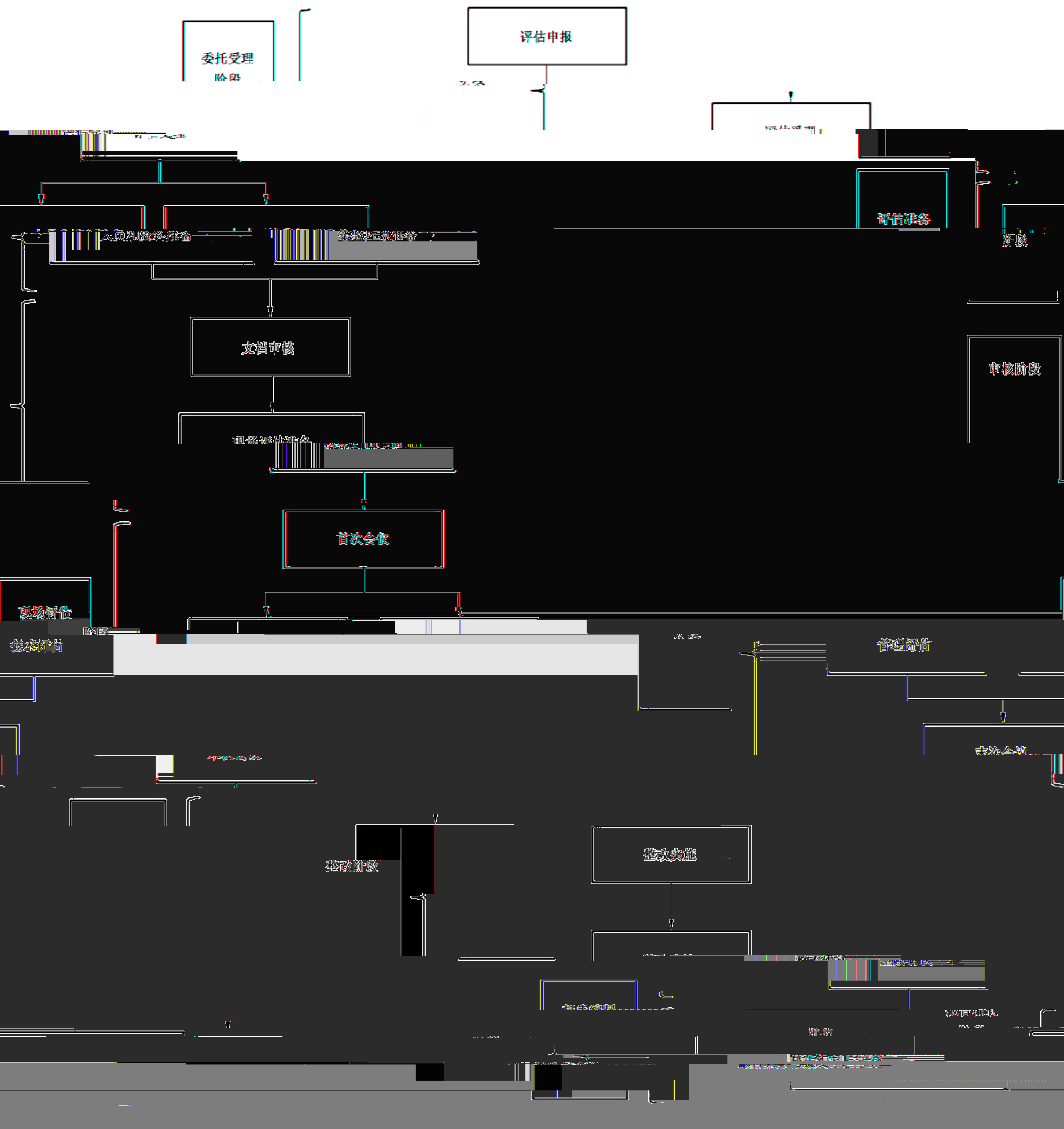
委托受理阶段
评估申报
评估受理
评估准备阶段
评估准备
文档审核
审核阶段
首次会议
现场评估阶段
技术评估
管理评估
末次会议
整改阶段
整改实施

图1 能力评估流程图

5.2 初次评估

5.2.1 委托受理阶段

5.2.1.1 评估申报

[illegible]

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[illegible]

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

[illegible]

5.2.3 审核阶段

5.2.3.1 文档审核

[illegible]

5.2.3.2 现场评估准备

[illegible]

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[illegible]

5.2.4.2 管理评估

[illegible]

5.2.4.3 技术评估

[illegible]

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，如对发现的问题有异议，测评机构可以在现场进行申诉或者补充证明材料，最终审核结果应得到双方确认。

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

[illegible]

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[illegible]

5.3 监督评估

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[illegible]

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[illegible]

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	基本条件	4.3.1 b) 产权关系明晰，注 [illegible] 4.3.1 e) 具有网络安全相关工作经历的技术和管理人员 [illegible]	4.4.1 b) 产权关系明晰，注册 [illegible] 4.4.1 e) 具有网络安全相关工作经历的技术和管理人员 [illegible]	4.5.1 b) 同Ⅱ级机构要求 4.5.1 e) 具有网络安全相关工作经 [illegible]
[illegible]	[illegible]	4.3.2.3 测评机构应具有 [illegible]	4.4.2.3 测评机构应具有 [illegible] 4.4.2.2 测评机构应明确设立 [illegible]	4.5.2.2 同 [illegible] 方式组织开设 [illegible] 部门 [illegible]
[illegible]	测评实施能力	4.3.3.1.1 [illegible] 测评项目数量不应少于 15 个 [illegible] 4.3.3.1.4 测评人员除具备等级测评 [illegible]	[illegible] 测评项目 [illegible] 少于 30 个 [illegible]	4.5.3.1 [illegible] 测评技术 [illegible] 等级测评师 [illegible] 测评师数量不应少于 50 人 [illegible] 4.5.3.1.4 测评人员除具备等级测 [illegible]

表 A.1（续）

[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
13.1	测评实施能力	无要求	4.4.3.2.4 测评机构应[illegible]善的测评方法研发；维[illegible]	4.5.3.2.4 同Ⅱ级机构要求
		无要求	4.4.3.2.5 测评机构应结合被[illegible]系，分析确定存在的安全问题，并提出针对性的整改建议	4.5.3.2.5 测评机构应针对被测系[illegible]通过对安全问题的深入分析，提出全面的建设整改解决方案
14	[illegible]	4.3.4.2 测评机构应配备满足等级测评工作需要的测[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[illegible]工具、[illegible]	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，[illegible]
[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
		4.4.6.4 b)对所有通过计算机记录或生成的数据的转移、复	4.4.5.2 测评机构应指定监督 无要求 无要求 无要求 无要求	4.4.6.3 上述文件的发布 4.4.6.6 安全管理能力

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) 熟悉信息安全产品分类，了解其功能、特点和操作方法；

d) [illegible]

e) [illegible]

f) [illegible]

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、标准；

b) [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究的基础和实践经验；

d) [illegible]

e) 能够独立开发测评指导书，熟悉测评指导书的开发、版本控制和评审流程；

f) [illegible]

g) [illegible]

B.3 高级等级测评师应具备以下条件或能力：

a) [illegible]

b) [illegible]

c) 具有信息安全理论研究基础和实践经验[illegible]

d) [illegible]管理能力；

e) 熟悉等级保护工作的[illegible]要求。

GB/T 36959—2018

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

版权专有 侵权必究