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

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 [illegible]

[illegible] 构的能力建设，规范等级保护工作要求，特制定本标准。

网络安全等级保护测评机构能力要求参考国际、国内测评与检验检测机构能力建设与评定的相关 [illegible]

[illegible]

网络安全等级保护测评机构能力 [illegible] 理、评估准备、文件审核、现场评估、整改验收、到评估报告提交等整个评估过程提出了规范性要求。

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。

本标准适用于测评业务要求为[illegible]

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[illegible]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。

[illegible]

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。

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Ⅰ级、Ⅱ级和Ⅲ级，级差是通过增加新的能力要求条款或在原条款基础上提出增强要求来实现。各级能力增强要求的总结情况见附录A中表A.1。

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：

[illegible]

4.3.2 组织管理能力

4.3.2.1 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。

[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、保管直至销毁的各项

[illegible]

a) 人员管理制度

应包括人员录用、考核、离职管理以及各职位人员安全管理

b) 培训教育制度

应包括培训计划的制定、培训工作的实施、培训的考核与日常职责及岗位培训档案建立等内容和

要求。

c) [illegible]

应明确在测评活动中相关单位人员在电话、技术、现场

访到如下各项要求等内容的完整指南。

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

[illegible]

4.3.3.1.2 测评人员应通过相关网络安全等级测评与检测评估机构能力要求

4.3.3.1.3 测评技术负责人应具有[illegible]

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[illegible]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[illegible]

4.3.3.2.2 测评机构应保证其能力范围内从事[illegible]

体现在以下方面:

a) 安全技术测评能力:有场地和环境安全、网络和通信安全、设备和计算安全、应用和数据

[illegible]

4.3.3.2.3 测评机构应具备[illegible]

[illegible]

b) 测评准备阶段:熟悉被测系统的相关资

[illegible]

c) [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。

[illegible]

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以下条件：

a) 产品研制、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) 产品研制、生产单位及其主要业务、技术人员无犯罪记录；

[illegible]

e) [illegible]对国家安全、社会秩序、公共利益不构成危害；

f) [illegible]检测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。

4.3.4.2 测评机构应配备满足等级测评工作需要的测试设备和工具，如WEB安全检测工具、[illegible]

4.3.4.3 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，用于满足网络安全保障、技术培训和模拟测试的需要。

4.3.4.4 测评机构应确保测试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的测试数据。

4.3.4.5 测评[illegible]设备和工具均应有正确的标识。

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 [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，确保其有效性。

4.3.5.2.2 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。

4.3.6 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，开展客观、公正、安全的测评服务。

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(500 万元)。

4.3.6.2.3 测评机构应建立并保存工作人员的人员档案，包括人员基本信息、社会背景、工作经历、培训记录 [illegible]

4.3.6.2.4 测评机构使用的测试设备和工具 [illegible] 能外泄之类的隐患。

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 [illegible]

4.3.6.2.8 [illegible]

a) [illegible]

b) [illegible]

c) [illegible]

4.3.6.2.9 [illegible]

4.3.6.3 测评方法与程序的规范性

测评机构应保证与等级测评工作有关的所有工作程序、指导书、标准规范、工作表格、核查记录表等 [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) 测评记录应当清晰规范，并获得被测评方的书面确认；

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要的所有信息，以上信息均应正确、准确、清晰地表述；

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的持续建设和发展。

4.3.8.2 测评机构应制定并实施对管理体系运行进行监督和改进的要求，不断完善管理要求，通过目标设定、内部审核、管理评审等活动，持续改进管理体系的有效性，通过标准实施，逐步提升质量管理能力。

4.3.8.3 测评机构应根据培训制度做好管理工作，并保存培训和考核记录。

4.3.8.4 测评机构应及时了解并分析本领域相关技术发展动态和应用需求，积极开展或参与相关技术交流和研讨活动，保持与领域技术发展的同步性。

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全资事业单位；

b) 从事网络安全等级测评活动两年以上，无违法记录；

c) 法定代表人、主要负责人、技术负责人、财务负责人具有相应的网络安全等级测评从业经历；

d) 具有开展网络安全等级测评活动的场所，具有满足开展等级测评活动需要的办公环境；

e) 具有满足开展等级测评活动的软硬件环境；

f) 具有完善的网络安全管理制度和保密管理制度，具有独立的网络安全技术管理和质量管理能力；

g) 其他条件。

4.4.2 组织管理能力

4.4.2.1 测评机构应遵守国家有关法律法规和相关的标准规范，

4.4.2.2 测评机构应建立并实施完善的管理制度，包括但不限于

a) 人员安全录用和保密管理制度；

b) 项目风险控制管理制度；

c) 过程记录管理制度；

d) 文档管理制度；

e) 设备和工具管理制度；

f) 测评质量管理制度；

g) 申诉、投诉和争议处理制度；

h) 培训制度；

i) 保密制度；

j) 其他管理制度。

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

[redacted]

b) 项目管理制度

[redacted]

c) 设备管理制度

[redacted]

d) 档案管理制度

[redacted]

e) 人员管理制度

[redacted]

f) 培训教育制度

[redacted]

g) 测评工作控制制度

[redacted]

4.4.3 测评能力

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）应具有把握国家政策，理解和掌握相关技术标准，熟悉等级测评的方法、流程和工作规范，以及风险分析、漏洞发现、渗透测试等方面的知识及能力，并有依据测评结果做出专业判断以及出具等级测评报告等任务的能力。

4.4.3.1.2 测评人员应参加由指定评估机构举办的专门培训、考试并取得等级测评师证书。等级测评人员需持证上岗。

[redacted]

4.4.3.2 测评能力

[redacted]

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[illegible]

c) 安全测试与分析能力：[illegible]

[illegible]

4.4.3.2.3 测评机构应[illegible]息技术在测评实施中的应用，借助自动化手段，规范测评流程，[illegible]配置，减少人为因素可能造成的差错，提高测评工作的效率。

4.4.3.2.4 测评机构应建立完善的测评方法研发、维护和更新机制，持续提高自身测评技术能力。

4.4.3.2.5 测评机构应结合被测系统的行业特点和业务类型，分析普遍存在的安全问题，并提出针对性的整改建议。

4.4.3.2.6 测评机构应依据测评工作流程，有计划、按步骤地开展测评工作，并保证测评活动的每个环节都得到有效的控制，具体要求如下：

a) 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[illegible]

b) 方案编制阶段：正确合理地确定测评对象、测评指标及测评内容等，并依据现行有效的技术标[illegible]编制测评方案，测评方案[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[illegible]设备、设施和管理系统[illegible]合以下条件：

a) 产品研制、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，[illegible]

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；

d) 产品研制、生产单位[illegible]

e) 对国家安全、社会秩序、公共利益不构成危害；

[illegible]

4.4.4.2 [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

评数据处理的计算机进行有效的运行维护，并保证计算

级测评工作需要的文件化的管理体系，并确保测评机构

效运行，发现问题及时反馈并采取纠正措施，确保其有效性。

诉及争议处理制度，并应记录采取的措施。

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

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

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

能影响其测评结果的来自于商业、财务和其他方面的压力

4.4.4.5 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

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

各级人员能够理解和执行。

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

4.4.5.2.2 测评机构应当严格遵守申诉、投

4.4.5.2.3 测评机构应建立并实施内部管

人员应独立于被审核部门。

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

4.4.6.1.1 测评机构及其测评人员应

评服务。

4.4.6.1.2 测评机构的人员应不受可

4.4.6.2 可靠与保密性保证

4.4.6.2.1 测评机构的单位

4.4.6.2.2 测评机构应通过提供单位基本情况、法人及股东基本信息的文件证明

4.4.6.2.3 测评机构应对工作人员的从业背景进行

4.4.6.2.4 测评机构应使用测试设备和工具或其组合全面的功能列表，证明在功能列表之

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 测评机构应[illegible]有效的技术手段，确保等级测评相关信息的[illegible]数据[illegible]安全[illegible]等。

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、核查记录表等现行有效并便于测评人员获得。

4.4.6.3.2 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[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：

a） [illegible]

b） [illegible]

c） 测评机构应具有安全保管记录的能力，所有的测评记录应保存三年以上。

4.4.6.5 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[illegible]

b） [illegible]

c） [illegible]

d） [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；

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。

[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

[illegible]

4.5 Ⅲ级测评机构能力要求

4.5.1 基本条件

[illegible]

4.5.2 组织管理能力

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

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

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、培训的考核与上岗以及人员培

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

4.5.3.1.2 测评人员应参加过指定单位组织的等级测评相关技术培训，并考试合格，获得等级测评

4.5.3.1.3 测评技术负责人应具有测评师证书和技术管理岗位人员应分别取得相应等级测评师证书

4.5.3.1.4 测评机构技术负责人应具有

4.5.3.1.5 测评初始指定一名技术负责人负责等级测评方面的技术工作，测

4.5.3.2 测评能力

a) 安全测评实施能力，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、安全运维管理等方面测评指导书的开发、使用，能开发获取相关结果的专业判断；

b) 安全测评与分析评估能力，根据安全测评要求开发测评指导书，指导测

c) 安全

e)

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

4.5.5.1.2

4.5.5.1.3

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

4.5.5.2.3

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

4.5.6.1.1 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，严格遵守职业道德规范，公正、客观地开展测评活动。

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、财务和其他方面的压力。

4.5.6.1.3 测评机构在从事与测评活动有关的咨询服务时，应证明其咨询服务不会对测评结果的公正性产生影响。

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，资金注册达到要求。

4.5.6.2.3 测评机构应建立保密管理制度，明确保密责任和奖惩措施，并与所有员工签订保密协议，要求员工不得泄露在测评活动中接触到的被测评单位的商业秘密和国家秘密，并定期对员工进行保密教育和考核。

4.5.6.2.4 测评机构使用的测试设备和工具应具备完整的功能说明，并对其中存在的功能列表之外的功能进行说明。

4.5.6.2.5 测评机构应对其参与测评活动的人员进行有效管理，监督和控制其工作过程，防止其泄露或扩散在测评活动中接触到的被测评单位的国家秘密、商业秘密和个人隐私等。

4.5.6.2.6 测评机构应建立完善的保密管理制度，采取有效的保密措施，对测评活动中获取的文档和数据进行安全保密管理，

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

资料；

的数据和记录；

的分析与专业判断。

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

存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。

4.5.6.2.10 测评机构应建立

与程序的规范性

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

4.5.6.3.1 测评机构

行有效并便于测评人员获得。

格、核查记录表等现

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：

b) 应对所有通过计算机记录或生成的数据的转移、复制和发送进行核查，以确保其准确性和完整性。

c) 测评机构应具有安全保管记录的能力，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。

b) 能为所有符合条件的测评机构出具规范的等级测评报告模版；

c) 应对测评报告进行审核，并对测评报告的真实性负责；

d) 能为符合条件的测评机构出具相应等级的测评报告；

e) 应对测评报告使用者的义务和责任进行约定。

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、实施和维护符合自身等级测评工作要求的

安全管理体系，

能力

4.5.7 风险控制

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) 测评机构工作人员带来的风险；

b) 测评工具带来的风险；

c) 测评活动带来的风险；

d) 测评机构安全管理风险；

e) 被测系统重要信息资料泄露风险；

f) 测评结束后，被测系统数据恢复、系统安全恢复等风险。

患和有关文档等)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

4.5.8.2 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

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。

4.5.8.3 测评机构应实施完善的培训制度,以确保其人员在专业技术和管理方面持续满足等

4.5.8.4 测评机构应跟踪国内外新技术、新应用的发

5 测评机构能力评估

5.1 评估流程

如图 1 所示,初次评估流程包括委托受理阶段、评估准备阶段、审核阶段、现场评估阶段、整改阶段

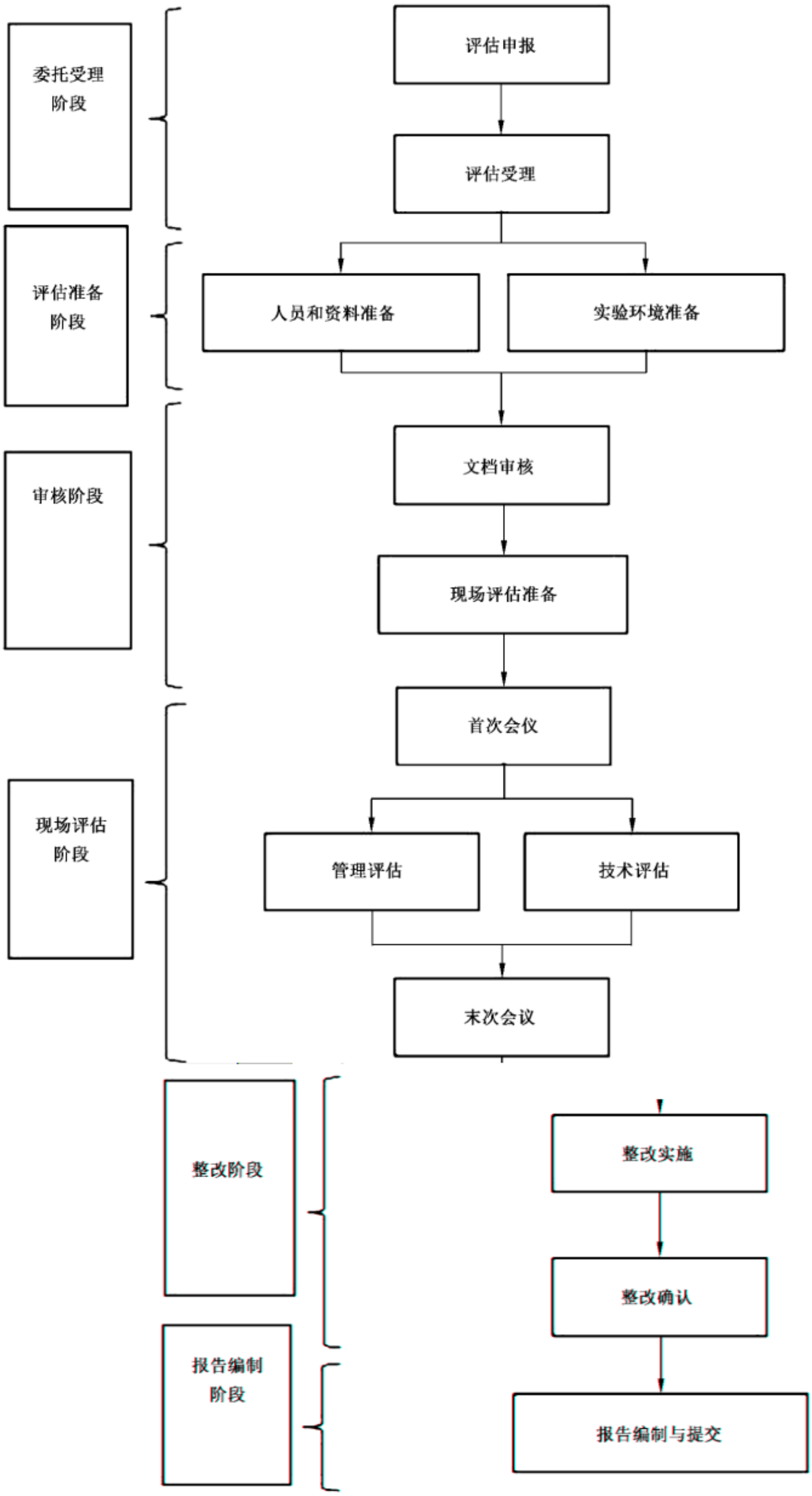
委托受理阶段
评估申报
评估受理
评估准备阶段
人员和资料准备
实验环境准备
审核阶段
文档审核
现场评估准备
首次会仪
现场评估阶段
管理评估
技术评估
末次会议
整改阶段
整改实施
整改确认
报告编制阶段
报告编制与提交

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
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
拟系统，并应制定等级测评
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

测评机构将管理体系、

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

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

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

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 证后监督

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监督。

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）

网络安全等级保护测评机构能力增强要求

各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
1	基本条件	4.3.1 b）产权关系明晰，注册资金 500 万元以上	4.4.1 b）产权关系明晰，注册资金 1 000 万元以上	4.5.1 b）同Ⅱ级机构
2		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 e）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
3		4.3.2.2 测评机构应按一定方式组织并设立相关部门，明确其机构职责、权限和相互关系	4.4.2.2 同Ⅰ级机构要求	4.5.2.2 同Ⅱ级机构要求
4		4.3.3.1 c）测评技术人员、测评项目组长和质量控制人员分别应至少有一名具备高级测评师资格	4.4.3.1 c）测评技术人员、测评项目组长和质量控制人员分别应至少有一名具备高级测评师资格	4.5.3.1 c）测评技术人员、测评项目组长和质量控制人员分别应至少有一名具备高级测评师资格
5		4.3.3.1 d）测评技术人员数量不少于 5 人	4.4.3.1 d）测评技术人员数量不少于 8 人	4.5.3.1 d）测评技术人员数量不少于 30 人
6		4.3.3.2 测评机构应每年对测评人员至少组织一次网络安全等级保护政策法规、技术标准和测评技术的培训，培训时间每人每年累计不少于 40 学时	4.4.3.2 测评机构应每年对测评人员至少组织一次网络安全等级保护政策法规、技术标准和测评技术的培训，培训时间每人每年累计不少于 40 学时	4.5.3.2 同Ⅱ级机构要求

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
		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	4.4.3.1.5 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	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
		具备安全专业相关的大学本科（或中级）及以上学历或同等专业水平，具有两年以上网络安全检测评估相关工作经历，或在本单位两年以上相关工作经验	具备安全专业相关的大学本科（或中级）及以上学历或同等专业水平，具有两年以上网络安全检测评估相关工作经历，或在本单位两年以上相关工作经验	具备安全专业相关的大学本科（或中级）及以上学历或同等专业水平，具有两年以上网络安全检测评估相关工作经历，或在本单位两年以上相关工作经验
		4.3.3.2.1 测评机构应通过培训或实践掌握至少 2 种以上被测对象的测评技术实施能力	4.4.3.2.1 测评机构应具备每年开展至少 2 个等级测评项目的能力，其测评技术实施能力应涵盖所测评信息系统涉及的全部技术类测评对象	4.5.3.2.1 测评机构应具备每年开展至少 3 个等级测评项目的能力，其测评技术实施能力应涵盖所测评信息系统涉及的全部技术类测评对象
		4.3.3.2.2 a）同 II 级机构要求	4.4.3.2.2 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、应用和数据安全等方面测评指导书的开发、使用、维护及获取相关结果的专业判断，测评指导书应覆盖目前流行产品和相关技术	4.5.3.2.2 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、应用和数据安全等方面测评指导书的开发、使用、维护及获取相关结果的专业判断，测评指导书应覆盖目前流行产品和相关技术
			4.4.3.2.2 b）安全测试与分析能力，包括测试工具的选择与使用能力，测试分析方法的设计与实施能力，测试结果的分析与总结能力，测试结果应与预期安全目标一致	4.5.3.2.2 b）安全测试与分析能力，包括测试工具的选择与使用能力，测试分析方法的设计与实施能力，测试结果的分析与总结能力，测试结果应与预期安全目标一致
			4.4.3.2.2 c）风险分析能力，包括依据风险分析方法对测评过程中发现的安全问题或风险进行分析和评价的能力，应对单个安全问题的风险进行综合分析并给出综合风险等级	4.5.3.2.2 c）风险分析能力，包括依据风险分析方法对测评过程中发现的安全问题或风险进行分析和评价的能力，应对单个安全问题的风险进行综合分析并给出综合风险等级
			4.4.3.2.2 d）安全设计与开发能力，包括依据测评结果进行安全设计和开发的能力，应能够根据测评发现的问题进行整改或者重新设计安全解决方案	4.5.3.2.2 d）安全设计与开发能力，包括依据测评结果进行安全设计和开发的能力，应能够根据测评发现的问题进行整改或者重新设计安全解决方案

表 A.1（续）

序号	机构条件和能力	一级机构要求	二级机构要求	三级机构要求
13	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评设备和工具，测评设备和工具应通过权威机构的检测并可提供检测报告	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，测评设备和工具应通过权威机构的检测并可提供检测报告	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，测评设备和工具应通过权威机构的检测并可提供检测报告
14	设备和设施安全管理能力	4.3.4.3 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、安全设备组成的网络环境，用于开展渗透测试等测评活动	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、安全设备组成的网络环境，用于开展渗透测试等测评活动	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、安全设备组成的网络环境，用于开展渗透测试等测评活动
15	质量管理能力	无要求	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	4.5.4.6 同Ⅱ级机构要求
16	质量管理能力	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，并确保测评机构的管理体系得到有效的运行和实施	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，并确保测评机构的管理体系得到有效的运行和实施	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，并确保测评机构的管理体系得到有效的运行和实施
17	质量管理能力	无要求	4.4.5.2.3 测评机构应建立并实施内部管理审核机制以验证管理体系的符合性及有效性	4.5.5.2.3 测评机构应建立并实施内部管理审核机制以验证管理体系的符合性及有效性

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。监督员应具备丰富的安全测	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	规范性保证能力	无要求	同Ⅱ级机构要求	4.1.6.2 2）测评机构
22	规范性保证能力	无要求	同Ⅲ级机构要求	4.1.6.2 3）测评机构
23	规范性保证能力	无要求	同Ⅱ级机构要求	4.1.6.3 2）上述文件
24	规范性保证能力	无要求	4.5.5.3 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	4.1.6.4 6）对所有通
25	规范性保证能力	无要求	4.5.5.3 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	4.1.6.6 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
26	规范性保证能力	无要求	4.5.5.3 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	4.1.8.3 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技术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
27	规范性保证能力	无要求	4.5.5.3 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	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；

[redacted]

B.2 [redacted]

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