信 息 安 全 等 级 测 评 机 构
能 力 要 求

（ 试 行 ）

Competence for operation of bodies performing testing and evaluation of classified protection of information system security

200×-××-×× 发布　　200×-××-×× 实施

公安部信息安全等级保护评估中心

目　录

前　言

公安部颁布《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号），决定加快等级保护测评体系建设工作。信息安全等级测评机构的建设是测评体系建设的重要内容，为确保有效指导测评机构的能力建设，规范其测评活动，满足信息安全等级保护工作要求，特制定本规范。

《信息安全等级测评机构能力要求》（以下简称《能力要求》）是等级保护测评体系建设指导性文件之一。本规范吸取国际、国内测评与检查机构能力评定的相关内容，结合信息安全等级测评工作的特点，对测评机构的组织管理能力、测评实施能力、设施和设备安全与保障能力、质量管理能力、规范性保证能力、风险控制能力、可持续性发展能力等提出基本能力要求，为规范等级测评机构的建设和管理，及其能力评估工作的开展提供依据。

信息安全等级测评机构能力要求

1 范围

本规范规定了测评机构的能力要求。

本规范适用于测评机构的建设和管理以及对测评机构能力进行评估等活动。

2 名词解释

2.1 等级测评

等级测评是指测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密信息系统安全等级保护状况进行检测评估的活动。

2.2 等级测评机构

等级测评机构，是指具备测评机构基本条件，经能力评估和审核，由省级以上信息安全等级保护工作协调（领导）小组办公室推荐，从事等级测评工作的机构。

3 基本条件

依据《信息安全等级保护测评工作管理规范》（试行），信息安全等级测评机构（以下简称测评机构）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（港澳台地区除外）；

b) 由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

c) 产权关系明晰，注册资金 100 万元以上；

d) 从事信息系统检测评估相关工作两年以上，无违法记录；

e) 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；

f) 具有满足等级测评工作的专业技术人员和管理人员，测评技术人员不少于 10 人；

g) 具备必要的办公环境、设备、设施，使用的技术装备、设施应当符合《信息安全等级保护管理办法》对信息安全产品的要求；

h) 具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

i) 对国家安全、社会秩序、公共利益不构成威胁；

j) 应当具备的其他条件。

4 组织管理能力

4.1 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。

4.2 测评机构应按一定方式组织并设立相关部门，明确其职责、权限和相互关系，保证各项工作的有序开展。

4.3 测评机构应具有胜任等级测评工作的专业技术人员和管理人员，大学本科（含）以上学历所占比例不低于 60%。其中测评技术人员不少于 10 人。

4.4 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、质量主管、保密安全员和档案管理员等（不论称谓如何），并配备足够的、相对稳定并具备相应能力的工作人员。

4.5 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

测评机构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、各项保密措施与要求，以及违反保密制度的罚则等内容。

b) 项目管理制度

测评机构应依据《信息安全技术 信息系统安全等级保护测评过程指南》等技术标准制定完备的、符合自身特点的测评项目管理程序，主要应包括测评工作的组织形式、工作职责，测评各阶段的工作内容和管理要求等。

c) 质量管理制度（包含设备管理和文件档案管理等）

应以保证质量为前提对测评机构的设备、文件档案等提出各项要求。设备管理制度应包括对于仪器设备的购置、使用和维护的质量管理要求。文件档案管理制度应包括机构人员在文件档案管理中的相关职责、文件档案借阅、保管直至销毁的各项规定等。

d) 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。

e) 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训档案建立等的内容和要求。

f) 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、投诉和争议处理活动中相应的职责，建立从受理、确认到处置、答复等环节的完整程序。

5 测评实施能力

5.1 人员能力

5.1.1 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。

5.1.2 测评人员应参加由公安部信息安全等级保护评估中心举办的专门培训、考试并取得中心颁发的《等级测评师证书》（等级测评师分为初级、中级和高级）。等级测评人员需持证上岗。

5.1.3 初级、中级和高级等级测评师具体能力要求如下：

a) 初级等级测评师

- 了解信息安全等级保护的相关政策、标准；
- 熟悉信息安全基础知识；
- 熟悉信息安全产品分类，了解其功能、特点和操作方法；
- 掌握等级测评方法，能够根据测评指导书客观、准确、完整地获取各项测评证据；
- 掌握测评工具的操作方法，能够合理设计测试用例获取所需测试数据；
- 能够按照报告编制要求整理测评数据。

b) 中级等级测评师

- 熟悉信息安全等级保护相关政策、法规；
- 正确理解信息安全等级保护标准体系和主要标准内容，能够跟踪国内、国际信息安全相关标准的发展；
- 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；
- 具有较丰富的项目管理经验，熟悉测评项目的工作流程和质量管理的方法，具有较强的组织协调和沟通能力；
- 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；
- 能够根据信息系统的特点，编制测评方案，确定测评对象、测评指标和测评方法；

- 具有综合分析和判断的能力，能够依据测评报告模板要求编制测评报告，能够整体把握测评报告结论的客观性和准确性。具备较强的文字表达能力；
- 了解等级保护各个工作环节的相关要求。能够针对测评中发现的问题，提出合理化的整改建议。

c) 高级等级测评师

- 熟悉和跟踪国内、外信息安全的相关政策、法规及标准的发展；
- 对信息安全等级保护标准体系及主要标准有较为深入的理解；
- 具有信息安全理论研究的基础、实践经验和研究创新能力；
- 具有丰富的质量体系管理和项目管理经验,具有较强的组织协调和管理能力；
- 熟悉等级保护工作的全过程，熟悉定级、等级测评、建设整改各个工作环节的要求。

5.1.4 测评技术员、测评项目组长和技术主管岗位人员应分别取得初、中、高级等级测评师证书，其比例应满足等级测评工作需要。

5.1.5 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。

5.2 测评能力

5.2.1 测评机构应通过提供案例、过程记录等资料，证明其具有从事信息系统检测评估相关工作两年以上的工作经验。

5.2.2 测评机构应保证在其能力范围内从事测评工作，并有足够的资源来满足测评工作要求，具体体现在以下方面：

a) 安全技术测评实施能力，包括物理安全测评、网络安全测评、主机安全测评、应用安全测评、数据安全及备份恢复测评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；

b) 安全管理测评实施能力，包括安全管理制度测评、安全管理机构测评、人员安全管理测评、系统建设管理测评、系统运维管理测评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；

c) 安全测试与分析能力，指根据实际测评要求，开发与测试相关的工作指导书，借助专用测评设备和工具，实现主流协议分析、漏洞发现与验证等方面的能力；

d) 整体测评实施能力，指根据测评报告的单元测评的结果记录部分、结果汇总部分和问题分析部分，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

具体结果的能力。

e) 风险分析能力，指依据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测评系统安全造成的影响的能力；

5.2.3 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。

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，全面掌握被测评系统的详细情况，为测评工作的开展打下基础；

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：

- 符合相关的等级测评标准；
- 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。

c) 现场测评阶段，严格执行测评方案和测评指导书中的内容和要求，并依据操作规程熟练地使用测评设备和工具，规范、准确、完整的填写测评结果记录，获取足够证据，客观、真实、科学地反映出系统的安全保护状况，测评过程应予以监督并记录；

d) 报告编制阶段，找出整个信息系统安全保护现状与相应等级的保护要求之间的差距，分析差距可能导致被测评系统面临的风险，给出等级测评结论，形成测评报告，测评报告应依据公安部统一制订的《信息系统安全等级测评报告模版（试行）》的格式和内容要求编写，测评报告应通过评审并有相关记录。

6 设施和设备安全与保障能力

6.1 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；

d) 产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能；

e) 对国家安全、社会秩序、公共利益不构成危害；

f) 信息安全产品应获得公安部计算机信息安全产品销售许可证。

6.2 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，如漏洞扫描器、协议分析仪、渗透测试工具等。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（见附录《信息安全等级测评设备和工具指引》）。

6.3 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，用于满足信息系统仿真、技术培训和模拟测试的需要。

6.4 测评机构应确保测评设备和工具运行状态良好，并通过校准或比对等手段保证其提供准确的测评数据。

6.5 测评设备和工具均应有正确的标识。

7 质量管理能力

7.1 管理体系建设

7.1.1 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。

7.1.2 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。

7.1.3 测评机构应指定一名质量主管，明确其质量保证的职责。质量主管不应受可能有损工作质量的影响或利益冲突，并有权直接与测评机构最高管理层沟通。

7.2 管理体系维护

7.2.1 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。

7.2.2 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。

8 规范性保证能力

8.1 公正性保证能力

8.1.1 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。

8.1.2 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。

8.2 可信与保密性保证能力

8.2.1 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。

8.2.2 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（100 万元）。

8.2.3 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、专业资格、奖惩情况等，保障人员的稳定和可靠。

8.2.4 测评机构使用的测试设备和工具应具备全面的功能列表，且不存在功能列表之外的隐蔽功能。

8.2.5 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。

8.2.6 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、商业秘密、敏感信息和个人隐私等。

8.2.7 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。

8.2.8 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。

8.2.9 测评机构应借助有效的技术手段，确保等级测评相关信息的整个数据生命周期的安全和保密。

8.3 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、核查记录表等现行有效并便于测评人员获得。

8.4 测评记录的规范性

a) 测评记录应当清晰规范，并获得被测评方的书面确认；

b) 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。

8.5 测评报告的规范性

a) 测评机构应按照公安部统一制订的《信息系统安全等级测评报告模版（试行）》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依据《信息安全等级保护测评工作管理规范》第六条，对出具的等级测评报告统一加盖等级测评机构能力合格专用标识并登记归档。

9 风险控制能力

9.1 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。

9.2 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。

10 可持续性发展能力

10.1 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。

10.2 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资质认可），通过目标的实现，逐步提升质量管理能力。

10.3 测评机构应建立文件化的培训制度，以确保其工作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。

10.4 测评机构应投入专门的力量来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和技术研讨，保持与测评技术发展的同步性。

11 测评机构能力约束性要求

测评机构不得从事下列活动：

a) 影响被测评信息系统正常运行，危害被测评信息系统安全；

b) 泄露知悉的被测评单位及被测信息系统的国家秘密和工作秘密；

c) 故意隐瞒测评过程中发现的安全问题，或者在测评过程中弄虚作假，未如实出具等级测评报告；

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) 分包或转包等级测评项目；

g) 信息安全产品（专用测评设备和工具以外）开发、销售和信息系统安全集成；

h) 限定被测评单位购买、使用其指定的信息安全产品；

i) 其他危害国家安全、社会秩序、公共利益以及被测单位利益的活动。