CNAS-CI01-A018

检验机构能力认可准则在网络安全等级测评领域的应用说明

Guidance on the Application of Inspection Body Competence Accreditation Criteria in the Field of Classified Cybersecurity Protection

中国合格评定国家认可委员会

2022 年 6 月 30 日 发布　　2022 年 7 月 1 日 实施

目 次

前 言

本文件由中国合格评定国家认可委员会（CNAS）制定，是CNAS根据网络安全等级测评领域的特殊性而对CNAS-CI01:2012《检验机构能力认可准则》所作的进一步说明，并不增加或减少该准则的要求。因此，本文件依照CNAS-CI01:2012《检验机构能力认可准则》的具体条款提出应用说明的编排方式，故章节号不连续。

本文件中网络安全等级测评的定义应符合《中华人民共和国网络安全法》及相关管理部门的要求。

本文需与CNAS-CI01:2012《检验机构能力认可准则》及CNAS-CI01-G001:2021《检验机构能力认可准则的应用说明》同时使用。

本文件为初次制订。

检验机构认可准则在网络安全等级测评领域的应用说明

1 范围

本文件适用于对从事网络安全等级测评活动的检验机构认可，该类机构统称为网络安全等级测评机构。

2 规范性引用文件

下列参考文件对于本文件的应用不可缺少。对注明日期的参考文件，只采用所引用的版本；对没有注明日期的参考文件，采用最新的版本(包括任何的修订)。

中华人民共和国网络安全法

CNAS-CI01 检验机构能力认可准则

CNAS-CI01-G001 检验机构能力认可准则的应用说明

GB/T 25069 《信息安全技术 术语》

GB/T 28449 《信息安全技术 网络安全等级保护测评过程指南》

GB/T 36959 《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 28448 《信息安全技术 网络安全等级保护测评要求》

GB/T 22239 《信息安全技术 网络安全等级保护基本要求》

GB/T 22240 《信息安全技术 网络安全等级保护定级指南》

3 术语和定义

3.1

等级测评师 Evaluation professional of classified protection of cybersecurity

经过行业公认的机构考核，依据国家网络安全等级保护制度，按照有关管理规范和技术标准，对已定级备案的非涉及国家秘密的网络（含信息系统、数据资源等）的安全保护状况进行检验评估的专业人员。

注：GB/T 25069、GB/T 28448、GB/T 28449、GB/T 22239、GB/T 22240中的术语适用于本文件。

4 通用要求

4.1 公正性和独立性

4.1.6 网络安全等级测评机构及其人员应严格执行有关管理规范和技术标准开展客观、公正的测评活动，不得从事网络安全产品开发、销售或信息系统安全集成等可能影响测评结果公正性的活动（自用除外）。

4.2 保密性

4.2.1 网络安全等级测评机构应建立数据和信息保密程序，并与全体人员签订保密责任书，规定其应当履行的对机构自身和委托方的安全保密义务和承担的法律责任。检验机构应指派保密管理工作责任人，负责采取管理和技术措施保护测评活动中相关数据和信息在整个数据生命周期中的安全、保密和可控，不得泄露在测评活动中知悉的国家秘密、工作秘密、商业秘密、重要敏感信息和个人隐私信息；未经监管部门同意，不得发布、披露在测评活动中收集掌握的相关的数据和信息。

注：测评活动中相关的数据和信息包括但不限于：被测单位提供的资料、等级测评活动生成的数据和记录、网络拓扑信息、系统漏洞、网络攻击事件以及依据上述信息做出的分析与专业判断。

5 结构要求

5.1 行政管理要求

5.1.1 网络安全等级测评机构的基本条件应符合监管部门的要求。

5.1.4 网络安全等级测评机构应充分识别测评活动中可能产生的风险，并通过多种措施对可能面临的风险加以规避和控制，保留风险识别和对应措施的评审记录，风险包括但不限于以下方面：

a) 由于自身能力或资源不足造成的风险；

b) 测评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) 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。

5.2 组织和管理

5.2.2 网络安全等级测评机构应参加获得认可的能力验证提供者（PTP）组织的测评机构能力验证计划。初次申请认可的检验机构，应至少参加过1次能力验证并获得满意结果。对于已获认可的检验机构，应至少满足CNAS该领域能力验证频次的要求，监管部门有要求时也应满足。

5.2.5 网络安全等级测评机构应指定至少一名技术主管，技术主管应具备高级测评师资格，全面负责网络安全等级测评方面的技术工作。

6 资源要求

6.1 人员

6.1.1 网络安全等级测评机构应具有胜任等级测评活动的测评人员和管理人员，大学本科及以上学历所占比例不低于70%。检验机构应设置满足等级测评活动需要的岗位，包括测评项目组长、测评项目组员、渗透测试工程师、保密安全员等，岗位职责明确。

注：测评人员包括测评项目组员、测评项目组长、渗透测试工程师和技术主管等岗位人员。

6.1.2 网络安全等级测评机构中测评项目组员、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，数量不应少于15人，渗透测试工程师应取得行业认可的技术能力证明，渗透测试工程师数量不应少于2人。

6.1.3 网络安全等级测评机构测评人员应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，应取得等级测评师资格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，授权签字人应取得高级测评师资格。

6.1.5 网络安全等级测评机构应保留测评人员能力考核、授权记录，等级测评师证书应作为测评人员授权上岗的必要条件之一，未取得等级测评师证书的测评人员，不得授权上岗承担等级测评项目。

6.1.7 测评人员上岗前，网络安全等级测评机构应组织岗前培训。同时检验机构应组织测评人员参加多种形式的测评业务和技术培训，根据每个测评人员的测评活动领域制订培训计划，测评人员每年培训时长累计不少于40学时，或按照监管部门的要求进行培训。

6.1.10 网络安全等级测评机构应建立并保存测评人员的人员技术档案，包括人员基本信息、工作经历、培训记录、项目经历、监督记录、专业资格等。

6.1.13 网络安全等级测评机构中的测评人员离职前，检验机构应与其签订离职保密承诺书。检验机构应加强对测评人员的监督管理，每年至少一次组织开展安全保密教育培训。

6.2 设施与设备

6.2.1 网络安全等级测评机构应具有固定的办公场所和机房，配备满足测评业务需要的网络协议分析、漏洞扫描（至少包括Web漏洞、主机漏洞）、渗透测试等必要的软硬件安全测评工具，商业化工具需要得到正版授权，所有检验活动涉及到的工具应纳入设备管理。

注：如果软硬件安全测评工具是租赁（相关软硬件安全测评工具不允许从最终用户租赁）或由其他机构（如设备的制造者或安装者）提供的，所用设备的自身安全性、持续适用性应由检验机构独立承担。

6.2.13 网络安全等级测评机构应在安全测评工具投入使用前进行核验，且在每次项目使用前检查确认测评工具升级到最新版本（包括漏洞库、规则库等），以保证安全

测评工具自身的安全性、持续适用性。当安全测评工具有重大版本变更时，要重新进行验证。机构自行研发的工具需要经过功能性、安全性和结果准确性验证，并保留验证材料。

6.3 分包

6.3.1 网络安全等级测评机构不应将网络安全等级测评业务分包。

7 过程要求

7.1 检验方法和程序

7.1.1 网络安全等级测评机构应制定符合等级测评活动方面标准要求的测评过程管理程序。

7.1.2 网络安全等级测评活动的检验对象抽取原则需要符合GB/T 28449《信息安全技术 网络安全等级保护测评过程指南》附录B的要求。

7.1.9 如果检验机构的检验活动现场涉及安全作业要求，如能源、化工、工业生产控制等涉及生产安全的环境，应制订安全实施测评的文件化指导书。

7.2 检验项目和样品的处置

7.2.2 网络安全等级测评机构应通过调研系统构成情况、制订测评方案、取得被测评方书面授权、告知被测评方测评产生的风险、与被测评方确认被测系统数据已备份等方式确认检验项目已做好了准备，上述内容应经过被测评方书面确认。

7.2.4 网络安全等级测评机构应在避免被测系统由于测评损坏的控制措施中包括安全事件应急处置机制和纠纷处理机制，防范测评风险，妥善处理纠纷。应采取措施避免被测系统在测评期间出现数据和服务破坏，离场时应与被测评方一起对被测系统的运行状态进行确认，并保存系统状态确认记录和文档交接记录。

7.3 检验记录

7.3.1 网络安全等级测评机构应提供漏洞扫描工具的升级和扫描记录，至少应包括工具名称、工具版本、升级后的最新漏洞库版本、升级日期和升级人员等。

7.4 检验报告和检验证书

7.4.2 网络安全等级测评机构应按照行业统一规范的网络安全等级测评报告模板格式出具测评报告。

7.4.4 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。

7.5 投诉和申诉

7.6 投诉和申诉过程

8 管理体系要求

8.1 方式

8.2 管理体系文件（方式 A）

8.3 文件控制（方式 A）

8.4 记录控制（方式 A）

8.5 管理评审（方式 A）

8.5.2 网络安全等级测评机构的管理评审输入除了应满足基本认可准则的要求，还应包括以下相关信息：

a）测评机构基本条件符合情况；

b）测评机构管理制度执行情况；

c）测评机构相关事项变更报告、审查情况；

d）测评师管理、行为规范情况；

e）测评项目实施情况；

f）测评报告及相关数据文档管理情况；

g）行政主管部门监督检查的结果等。

8.6 内部审核（方式 A）

8.7 纠正措施（方式 A）

8.8 预防措施（方式 A）