检测和校准实验室能力认可准则
在信息安全检测领域的应用说明

Guidance on the Application of Testing and Calibration Laboratories Competence Accreditation Criteria in the Field of Information Security Testing

|  |
| --- |
|  |
|  |

目  次

[前  言 II](#_Toc26874549)

[1 范围 1](#_Toc26874550)

[2 规范性引用文件 1](#_Toc26874551)

[3 术语和定义 1](#_Toc26874552)

[4 通用要求 1](#_Toc26874553)

[4.1 公正性 1](#_Toc26874554)

[5 结构要求 1](#_Toc26874555)

[6 资源要求 1](#_Toc26874556)

[6.2 人员 1](#_Toc26874557)

[6.3 设施和环境条件 2](#_Toc26874558)

[6.4 设备 2](#_Toc26874559)

[6.5 计量溯源性 2](#_Toc26874560)

[7 过程要求 3](#_Toc26874561)

[7.1 要求、标书和合同评审 3](#_Toc26874562)

[7.2 方法的选择、验证和确认 3](#_Toc26874563)

[7.4 检测或校准物品的处置 3](#_Toc26874564)

[7.5 技术记录 3](#_Toc26874565)

[7.6 测量不确定度的评定 3](#_Toc26874567)

[7.7 确保结果有效性 3](#_Toc26874568)

[8 管理体系要求 4](#_Toc26874569)

[8.2 管理体系文件（方式A） 4](#_Toc26874570)

[8.7 纠正措施（方式A） 4](#_Toc26874571)

[8.8 内部审核（方式A） 4](#_Toc26874572)

[8.9 管理评审（方式A） 4](#_Toc26874573)

前  言

本文件由中国合格评定国家认可委员会（CNAS）制定，是结合信息安全检测的特点对 CNAS-CL01:2018《检测和校准实验室能力认可准则》 中的部分条款的应用说明，并不增加或减少该认可准则的要求。
 本文件与 CNAS-CL01:2018《检测和校准实验室能力认可准则》同时使用。

在结构编排上，本文件章、节的条款号和条款名称均采用 CNAS-CL01:2018中章、节条款号和名称，对 CNAS-CL01:2018应用说明的具体内容在对应条款后给出。

本文件代替：CNAS-CL01-A020:2018《检测和校准实验室能力认可准则在信息安全检测领域的应用说明》。

检测和校准实验室能力认可准则在信息安全检测领域的应用说明

1. 范围

 本文件适用于所有从事信息安全检测的实验室。

1. 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。

CNAS-CL01:检测和校准实验室认可准则（idt ISO/IEC 17025）

1. 术语和定义

CNAS-CL01界定的术语和定义适用于本文件。

1. 通用要求
	1. 公正性

4.1.3 如果实验室所在的组织从事信息安全检测以外的活动（例如，涉及信息安全相关的开发），应承诺并采取措施确保不利用被检测信息安全相关方的知识产权牟取利益。

4.1.4 实验室应建立并保持从事信息安全检测公正性和诚实性的政策和程序，识别产品开发商、系统集成商、系统运维商等对信息安全检测活动公正性的影响。

4.1.5 如果实验室所在的组织从事信息安全检测以外的活动，应确保信息安全检测人员不参加被测对象的开发和咨询，信息安全检测人员与产品开发、系统集成、系统运维等可能存在影响公正性的利害关系的人员之间相互分离。

1. 结构要求

5.2 实验室应具有管理信息安全检测领域的质量和技术负责人，且除授权签字人以外，至少具有5名信息安全检测人员。

1. 资源要求
	1. 人员

6.2.2 信息安全检测实验室的技术人员应满足以下要求：

a) 从事信息安全检测活动的人员，应具有计算机相关专业专科及以上学历；非相关专业应具有本科及以上学历，且应经过信息安全检测技术专业培训，从事信息安全检测工作1年以上并至少参与过3个信息安全检测项目。此外，各类人员均应具备信息安全检测工作相适应的背景知识和检测技能。

b) 各类人员其他应满足的要求包括：

1）从事信息安全检测项目组织与实施的负责人员应熟悉项目管理、信息安全开发过程、信息安全检测技术及其标准、规程和规范；

2）从事信息安全检测过程、检测质量规范与符合性审核监督的人员应熟悉信息安全的检测过程、标准/规范/规程和信息安全检测质量评价。

3) 从事信息安全检测结果评价（评估）和方法确认的人员，以及授权签字人员和意见解释人员，应从事信息安全检测工作5年以上，并至少作为项目负责人实施过5个信息安全检测项目。

4) 从事信息安全检测执行的人员，应经过相关培训、考核通过后方能上岗。实验室对信息安全检测人员进行的培训，应包括与信息安全检测有关的法规、标准培训和检测技术类培训。实习人员须在实验室有经验和有能力的正式签约人员的指导下，从事检测活动。

5）实验室应确保所有人员接受安全保密和知识产权保护方面的培训，以确保客户利益和商业机密不被侵害与泄露。

* 1. 设施和环境条件

6.3.1 实验室应建立防静电、防范恶意代码的检测环境，以及防止实验室环境中部署的信息安全防护设备影响信息安全检测结果。

6.3.3 对结果有影响的因素，实验室应进行监控和记录环境条件，包括防止病毒木马等不良程序感染等。

6.3.4 c）实验室检测网络应与其他网络采取隔离措施。如果同时进行多个检测项目，实验室应保持检测环境的有效分离，防止拒绝服务攻击等影响检测结果。当检测活动在实验室以外场所进行时，其检测环境也应满足要求，并确保检测活动在受控环境下执行。当通过实验室以外的网络实施远程检测时，应确保网络正常运行的环境，并记录或确认影响性能指标的外部因素。

* 1. 设备

6.4.1 信息安全检测设备包括但不限于性能测试工具、安全性测试工具、仿真测试工具等。

6.4.2 实验室应在客户提供的检测设备投入使用前进行验证。

6.4.3 实验室应及时更新升级检测设备的版本和特征库，确保检测使用的检测样本集（如病毒样本库、网络攻击数据包、漏洞库等）为最新版本，并保存升级记录。

6.4.4 有指标要求的检测设备在投入使用前及发生变更时，均应对其进行验证。租赁的检测设备，应有可追溯的许可和/或授权协议。

6.4.12 正在进行检测的被测对象和检测用的硬件设备应张贴“检测中”的状态标识，并在运行被测对象和检测用的计算机设备屏保屏幕中设置标识，以避免错误调整检测环境影响检测工作的进行。

6.4.13 实验室应保存所有检测设备的档案。实验室的记录还应包括所有检测设备的配置信息，软件形态检测工具所需运行环境、相关组件的库版本信息以及其他需要特殊声明的信息等。信息安全检测设备的不同版本，均应有唯一性标识。

* 1. 计量溯源性

6.5.3 对于新的或发生了重大变化的无法进行外部溯源的方法和检测工具，实验室应采取措施检查检测方法和检测工具的有效性，检查措施可包括：
 a）适用时，对特定的信息安全产品样例进行检测，审查信息安全产品样例预埋问题的复现情况，确认其偏差。
 b）适用时，应溯源到权威的测试集规范或其它有关的权威标准或规范。

1. 过程要求
	1. 要求、标书和合同评审

7.1.1 a）实验室的要求、标书和合同评审程序，应确保：

1）对检测项目的保密性要求和知识产权保护要求，在合同中（或签订专门的协议）应予明确、充分规定。

2）对信息安全检测依据、为达到检测目的需要提供给实验室的检测输入项等应予以明确规定，检测输入项可包括被测对象相关技术材料、软/硬件等。

3）对检测项目结束后如何处置检测对象、检测报告的交付数量及方式等应予以明确规定。

* 1. 方法的选择、验证和确认

7.2.2方法的确认

7.2.2.1 针对非标准方法，应经过5名（含）以上的信息安全领域外部专家评审。

* 1. 检测或校准物品的处置

7.4.1 实验室应有措施保证检测工具或测试集不会将病毒或其他损坏因素引入到属于客户的硬件或软件中。特殊的渗透性测试或破坏性测试，应在向客户充分说明可能的后果并获得客户的允许后进行。检测工作完成后，实验室应按合同要求的检后处置方式处置被测对象，并保留记录。

7.4.3 在接收软件形态的检测样品时，实验室应对检测对象进行病毒检查并记录。

* 1. 技术记录

7.5.1 信息安全检测项目的技术记录应能够追溯到检测人员的操作和工作方法及检测环境，应详细记录检测环境配置（硬件和软件）、检测工具及参数配置等信息，确保该检测过程和检测结果在尽可能接近原条件的情况下能够进行重复和复现。

7.6 测量不确定度的评定

7.6.3 实验室应对信息安全检测中定量类检测项目评定测量不确定度。

注1：在测量不确定度的评定中，实验室需更多关注由检测方法、设备和人员带来的测量不确定度影响。

注2：对于信息安全检测领域无法评定测量不确定度的定性类检测项目，实验室需关注以下几点：

a） 检测环境满足要求；

b） 检测设备的状态满足要求；

c） 检测人员熟悉并严格按照操作流程和标准方法要求进行操作。

* 1. 确保结果有效性

7.7.1 实验室制定的质量监控方案还应包括：
a）由同一检测人员对被测对象进行重复检测；

b）由不同的检测人员使用相同方法对同一被测对象进行检测；
c）使用不同的检测方法（技术）对同一被测对象进行检测；

d）同一类型的不同仪器或工具对同一被测对象进行检测。

实验室应保存监控活动的记录，包括对比对检测结果的评价。

1. 管理体系要求

8.2 管理体系文件（方式A）

8.2.4 实验室应建立并实施与实验室信息安全检测活动范围相适应的管理体系。此外，应制定非固定场所信息安全检测活动的程序，对开展非固定场所信息安全检测活动的人员职责和任职条件、工作程序和质控方法等予以规定。

* 1. 纠正措施（方式A）

8.7.1b）信息安全检测活动产生问题的原因还可能是：恶意代码、检测操作顺序、软件版本、参数设置、 漏洞库、攻击特征库、检测环境中采取的信息安全防护技术或设备等。

* 1. 内部审核（方式A）

8.8.1 实验室开展内部审核至少为12个月一次。

* 1. 管理评审（方式A）

8.9.1 实验室开展管理体系评审至少为12个月一次。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_