ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35280—2017

信息安全技术　信息技术产品安全检测机构条件和行为准则

Information security technology—Requirement and code of conduct for security testing bodies of information technology products

2017-12-29 发布　　2018-07-01 实施

中华人民共和国国家质量监督检验检疫总局
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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国电子技术标准化研究院、中国信息安全测评中心、中国信息安全研究院有限公司、北京信息安全测评中心、国家信息技术安全研究中心、公安部第三研究所、国家保密科技测评中心、国家应用软件产品质量监督检验中心、中国信息安全认证中心、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、中国科学院软件研究所、陕西省网络与信息安全测评中心、西安电子科技大学、重庆邮电大学、华东师范大学、国网江苏省电力公司电力科学研究院。

本标准主要起草人:范科峰、王惠莅、龚洁中、李琳、任泽君、王春佳、杨晨、顾健、杨宏宁、王坤、董晶晶、李凤娟、张宝峰、时志伟、魏方方、甘杰夫、刘玉岭、贺海、马文平、杨帆、裴庆琪、杨力、黄永洪、何道敬、刘虹、黄伟。

引　言

为保障关键信息基础设施网络安全，消减因为大量使用的信息技术产品可能给设施引入的安全缺陷、漏洞、恶意程序等潜在的安全风险，需要通过对信息技术产品安全检测，提高信息技术产品供应方产品的安全保障能力。

同时为加强信息技术产品安全检测机构管理，规范信息技术产品安全检测机构行为，保障检测活动的公正可信性以及安全检测机构的能力水平，促使信息技术产品供应方提高产品的安全保障能力，保障国家关键信息基础设施安全，制定本标准。

信息安全技术　信息技术产品安全检测机构条件和行为准则

1　范围

本标准规定了信息技术产品安全检测机构应具备的条件以及应遵守的行为准则。

本标准适用于从事信息技术产品安全性检测的第三方机构，可为相关主管部门、信息技术产品供应方和用户选择第三方检测机构提供参考。

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。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。

GB/T 25069—2010　信息安全技术　术语

GB/T 27000—2006　合格评定　词汇和通用原则

GB/T 27025　检测和校准实验室能力的通用要求

GB/T 32921—2016　信息安全技术　信息技术产品供应方行为安全准则

3　术语和定义

GB/T 25069—2010、GB/T 27000—2006 和 GB/T 32921—2016 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 32921—2016 中的一些术语和定义。

3.1

信息技术产品　information technology product

具有采集、存储、处理、传输、控制、交换、显示数据或信息功能的硬件、软件、系统和服务。

注：信息技术产品包括计算机及其辅助设备、通信设备、网络设备、自动控制设备、操作系统、数据库、应用软件与服务等。

[GB/T 32921—2016，定义 3.1]

3.2

信息技术产品供应方　information technology product supplier

提供信息技术产品的组织。

注：信息技术产品供应方包括生产商、销售商、代理商、集成商、服务商等。

[GB/T 32921—2016，定义 3.2]

3.3

信息技术产品安全检测机构　security testing bodies of information technology products

从事信息技术产品安全检测活动的第三方机构。

注 1：信息技术产品安全检测机构可以是一个组织，或是一个组织的一部分。

注 2：本标准中信息技术产品安全检测机构简称“检测机构”。

4 基本要求

4.1 行政管理要求

4.1.1 检测机构应是在中华人民共和国境内注册成立的法律实体，或者为某个法律实体的明确部分，该实体应对其全部检测活动承担法律责任。

4.1.2 检测机构应获得认证认可监督管理部门的检验检测机构资质认定。

4.1.3 检测机构在实施信息技术产品安全检测活动中，应满足本标准、国家认证认可监督管理部门及网络安全主管部门的要求。

4.1.4 检测机构应对在其固定场所、临时场所或者可移动的场所，以及客户场所中实施的活动负责。

4.2 能力要求

4.2.1 检测机构应明确其组织和管理结构，如检测机构属于某个实体的一部分，而该实体还从事检测以外的其他信息技术产品安全相关活动，则该实体的检测活动和其他活动之间的关系应予界定。

4.2.2 检测机构应制定和维护实施信息技术产品安全检测活动的策略和规程，以维持其检测活动的独立性和公正性以及检测活动中涉及信息的保密性和完整性。

4.2.3 检测机构应制定文件，明确其有能力实施的检测活动，并从组织和管理上确保其具备能够持续开展检测业务所需的能力。在进行信息技术产品安全检测时，应最少具备 4.2.4～4.2.7 所描述的能力。

4.2.4 检测机构应具备发现并分析被测产品中是否存在恶意程序、安全缺陷、漏洞等的检测技术能力。

4.2.5 检测机构应具备产品供应链安全的检测能力，包括产品供应链组件关系分析和安全检测能力。

4.2.6 检测机构应具备验证信息技术产品供应方是否仅依照所声称的方式进行数据交互和收集用户相关信息的检测能力。

4.2.7 检测机构应具备分析检测工作安全风险的能力，并能够通过采取人员培训、签署委托检测协议、保密协议、制定安全操作规程等方法，消减或缓解检测工作安全风险。

4.2.8 检测机构应明确涉及检测活动的每个岗位/人员的职责及相互关系。

4.2.9 检测机构应至少具有 5 名满足 5.1 中相关要求的人员，包括技术负责人、质量负责人、检测人员、监督人员等。

4.2.10 检测机构应具有有效运行的管理体系，并考虑管理体系的有效性和满足客户和其他要求的重要性，并及时沟通。

4.2.11 检测机构应建立信息安全管理制度，包括信息安全策略、资产管理、人员管理、物理和环境安全、保密制度等，并有效执行。

5 资源要求

5.1 人员

5.1.1 检测机构应建立和维护确定人员能力要求、人员选择、人员培训、人员监管、人员授权和人员能力监控的管理制度，明确人员的责任、义务和权利，并保存相关记录。

5.1.2 检测机构应维护从事信息技术产品安全检测的人员名单，包括最高管理者、技术负责人、质量负责人、授权签字人、检测人员、监督人员等。

5.1.3 检测机构的检测人员应了解检测活动中涉及的信息安全相关法律法规、政策文件、标准、信息技术产品安全检测工具、编程测试方法、测试指标和实施指南等，具备信息技术产品安全检测能力，能够满足检测机构开展信息技术产品安全检测业务的需求。

5.1.4 应由熟悉检验检测目的、制度、方法和结果评价的人员，对检验检测人员包括实习员工进行监督，监督内容包括信息安全检测方案、检测过程、检测结果以及信息安全检测质量评价等。

5.1.5 检测人员应具有信息安全、计算机软硬件、通信或网络等相关专业本科或以上学历，或至少1年信息技术产品安全检测经历。技术负责人、授权签字人应具备信息技术产品安全检测人员的专业背景，具有中级及以上相关专业技术职称或同等能力，至少3年信息技术产品安全检测经历。质量负责人应在上岗前接受GB/T 27025中质量管理体系的相关知识培训，熟悉本机构质量管理体系，具备保持机构质量管理体系正常运转的能力。

5.1.6 检测机构中从事检测的专业技术人员不应在两个或以上检测机构同时从业。技术人员在从事特定领域或产品的检测时，应具备相应的专业技术能力及相关检测经验。

5.1.7 检测机构的人员，不应提供影响检测结果公正性的咨询服务。

5.1.8 检测机构应至少每年对本机构和检测技术人员的检测技术能力进行评价，对检测技术手段进行更新等，以维持持续开展检测活动的技术能力。

5.2 设施和环境

5.2.1 检测机构应规定检测活动所需的设施和环境，并形成文档。设施和环境应满足检测活动的要求，不应影响检测结果的正确性。检测机构应监测、控制和记录相关说明书、方法和规程所要求的环境。如果存在影响结果正确性的情况，应根据需要监测、控制和详细记录环境。

5.2.2 检测机构应有受到保护(例如通过防火墙、入侵检测系统等保护)的检测网络，保护其免受外部实体的非授权访问，以及免受恶意软件、蠕虫、病毒及间谍软件等的攻击。

5.2.3 检测机构应有保护客户硬件、软件、检测数据、电子和纸质记录以及其他材料的系统，该系统应保护客户所有的材料和信息，避免检测机构的外部人员、检测机构的访客、与相应检测无关的检测机构其他人员和其他未授权人员接触这些材料和信息。

5.2.4 如果检测机构在多个地点进行检测活动，每个地点都应符合本标准的相关要求，并应建立多个地点之间的安全通信机制。

5.2.5 检测机构应对检测活动相关信息系统进行及时维护，以有效预防病毒和恶意软件攻击。

5.2.6 检测机构应建立有效的备份机制，避免数据和记录的丢失。

5.2.7 当检测机构同时进行多个检测活动时，不同客户或者不同检测产品的检测环境应有效分离。

5.2.8 当检测活动在检测机构外部进行时，检测机构应制定相应管理规程，用以指导检测技术人员开展检测活动。例如，在客户地点进行检测活动时，管理规程应规定如何在客户地点安全的进行检测、如何存储记录和文档以及如何控制对检测设备的访问等。

5.3 设备

5.3.1 检测机构应具有满足检测活动的设备，应建立设备使用、维护、废弃等管理制度。当检测机构使用非本机构的设备时，应确保其满足本标准及相关要求。

5.3.2 检测机构针对可能对检测结果准确性或有效性产生显著影响的设备，在投入使用前应验证其是否能够满足检测的需求。

5.3.3 检测机构应具有相应的安全检测工具等资源，检测工具包括但不限于安全漏洞扫描工具、源代码分析工具、安全配置核查工具等。

5.3.4 检测工具应遵从制造商的说明书进行维护(如适用)，并遵从检测机构内部管理制度。

5.3.5 当检测工具发生变更时，无论其变动大小，检测机构都应对变更后的检测工具进行验证，以确保其正确执行。如检测工具没有配套的验证程序，检测机构应定义验证程序，形成文档，并记录验证过程。

5.3.6 检测机构应维护可能影响到检测活动的设备的记录。记录应包括：设备标识(包括软件和固件

版本，若适用）、型号、设备校准信息、维护活动、配置信息以及对设备的任何损害、故障、修改或者维修的信息等。

5.3.7 任何非正常运行或者可能损坏的设备，应不再予以使用。在其修复并验证能够正确完成其功能前，应隔离放置，并进行标记。

5.3.8 检测项目结束时，应及时清除设备中存储的相关信息。

5.4 外部提供的产品和服务

检测机构应确保使用的外部提供的产品和服务安全可靠。若所使用的外部提供的产品和服务可能影响检测活动时，应制定相应的管理制度，明确外部产品和服务供应商的资质要求和外部提供的产品和服务的要求，分析外部提供的产品和服务的风险，并制定相应的应对措施。

注：外部提供的产品可能包括，例如：检测设备、辅助工具等。外部提供的服务可能包括，例如：校准服务、抽样服务、设施和设备维护服务等。

6 过程要求

6.1 要求、标书和合同的评审

6.1.1 通用要求

6.1.1.1 检测机构应与客户就检测工作签订保密协议，明确检测机构对用户资料和检测过程中产生信息的使用范围和方法。

6.1.1.2 检测机构应制定评审客户要求、标书和合同的管理制度，并形成文档。

6.1.1.3 当客户要求的方法不适当或者已不适用时，检测机构应告知客户。

6.1.1.4 应与客户及时沟通相关事宜，例如：合同执行情况、执行合同时发生的偏差、客户需要查看的检测活动等。

6.1.1.5 如果在执行合同期间，合同发生了变更，检测机构应对合同进行重新评审，并与受影响的相关方进行沟通。

6.1.1.6 应维护相关评审记录，包括任何重大变更的记录、与客户就客户要求的讨论记录、或者与客户进行的涉及检测活动结果的记录等。

6.1.1.7 对特殊行业或领域进行安全检测时，应对参与检测的人员背景进行审查。

6.1.2 外部提供的检测活动

6.1.2.1 检测机构评审客户申请、标书和合同的管理制度应包括对外部提供商的检测活动的管理。检测机构应告知客户有哪些检测活动由外部提供商执行，并获得客户的许可。

注：外部提供的检测活动可能发生在下列情况：

——当检测机构有资源和能力实施活动，但是由于意外原因不能够部分或者全部实施；

——当检测机构没有资源或者能力实施活动时。

6.1.2.2 检测机构应为外部提供的检测活动负责，除非是使用了客户或者主管部门指定的提供商。检测机构应确保外部提供的检测活动满足客户要求和本标准的相关要求。

6.2 方法选择和确认

6.2.1 基本要求

6.2.1.1 检测机构应对所有的检测活动制定适当的检测方法和管理程序，方法、程序及支撑文档，例如与检测活动相关的标准、规范、手册等都应为最新版本。

6.2.1.2 检测机构应使用满足客户要求的适用于检测活动的方法，当客户没有指定使用的方法时，检测机构应选择适当的方法，并告知客户。

注：推荐使用国际标准、区域标准或国家标准，或著名技术组织、相关科学文献或期刊已发布的方法、信息技术产品供应方推荐的方法，也可使用检测机构开发的或者修改的方法或者其他适合的方法。

6.2.1.3 当检测机构需要自行开发方法时，应具备相应的计划，并分配足够的资源。在开发方法的过程中，应定期评审其是否仍然满足客户的要求。检测机构应对任何需要修改开发计划的变更进行批准和授权。

6.2.1.4 检测机构在实施方法和程序前应验证其能正确实施。当检测活动的方法和程序在实施过程中发生偏离时，应记录该偏离情况，技术上有合理理由、经过授权且被客户接受。

6.2.2 方法的验证

检测机构应对非标准的方法、自行开发的方法等进行验证。当已经验证的方法发生变更时，应记录这些变更所造成的影响，必要时，应重新验证，并保存相关记录。

6.3 抽样

当客户要求通过抽样进行信息技术产品安全检测时，检测机构应制定抽样计划和抽样控制程序，并形成文档。文档中应详细描述抽样的策略(尽量根据适用的统计学方法)、决策过程、样品特性等，并记录抽样数据，当客户对抽样程序有偏离的要求时，应予以详细记录，同时告知相关人员。

6.4 检测样品的处置

6.4.1 检测机构应建立和保持样品管理程序，对样品的运输、接收、制备、处置、保护、存储、租借和归还进行管理。检测机构应有样品的标识系统，并在检验检测整个期间保留该标识。在接收样品时，应记录样品的异常情况或记录对检验检测方法的偏离。样品在运输、接收、制备、处置、存储过程中应予以控制和记录。当样品需要存放或养护时，应保持、监控和记录环境条件。

6.4.2 检测机构应采取措施保护检测和校准样品免受未授权的访问和使用，例如进行病毒检查。检测机构应对不同的检测项目的样品进行隔离，包括正在检测的样品、检测平台、外设以及文档等。

6.4.3 当受检样品包括软件组件时，检测机构应确保其保持正确的配置管理状态，以避免其在检测过程中对软件组件的无意更改。

6.5 技术记录

6.5.1 检测机构应具有记录维护体系，通过该体系可追溯每个信息技术产品安全评估的情况。该记录应易于获得，并包括了每个评估项目的所有信息。记录应包含记录生成日期、完成相关活动的人员、检测活动中生成的证据以及其他信息。应确保记录的完整性，并进行备份和归档。记录的保存期限应遵循国家相关规定、合同要求以及检测机构的相关策略等。

6.5.2 当检测机构需对记录进行增补时，应确保对记录的增补可追溯到前一版本以及可追溯到原始观察资料。检测机构应保留原始数据和修改的数据，包括变更方面的指示以及变更负责人。

6.6 检测结果质量的保证

检测机构应建立和保持质量控制制度，定期参加能力验证或机构之间比对。通过分析质量控制的数据，当发现偏离预先判据时，应采取有计划的措施来纠正出现的问题，防止出现错误的结果。质量控制应有适当的方法和计划并加以评价。

6.7 结果报告

6.7.1 基本要求

6.7.1.1 检测机构应制定检测报告管理制度。所出具的检测报告应准确、清晰、客观且无歧义，应满足国家相关规定或客户要求。其内容应包括检测人员的分析、检测环境、检测步骤、检测结果以及其他所需信息。检测机构或者另外的检测机构可根据这些信息重复检测活动。

6.7.1.2 检测机构应对其出具的检测报告的所有信息负责，除非该信息由客户提供。如果数据是由客户提供，应在报告中明确标出。如果信息由客户提供，且能够影响检测或者校准结果正确性时，应在报告中具有声明。如果检测机构不负责抽样（例如，抽样由客户提供），应在报告中说明结果仅适用于接收的样品。

6.7.1.3 检测机构在向客户出具正式检测报告前，应对其进行技术和质量的评审，并保存评审记录。

6.7.1.4 当检测机构以电子方式传输检测报告时，应根据国家相关规定和客户要求采取相应安全通信方式进行传输，例如使用电子签名或者以加密方式传输。

6.7.2 报告符合性声明

当检测机构提供对于某标准或规范的检测符合性声明时，应清晰的陈述其采用的确定规定以及相关的风险级别（例如，错误的接受、错误的拒绝和统计假设）。

6.7.3 意见和解释

当需要对报告做出意见和解释时，检测机构应确保只有授权的人员进行意见和解释，并应将意见和解释的依据形成文件，在检测报告中对意见和解释进行清晰标注。

6.7.4 报告的修改

检测报告或证书签发后，若有更正或增补应予以记录，且应清晰的标出任何修改的信息或者重新签发的信息。修订的检验检测报告或证书应标明所代替的报告或证书，并注以唯一性标识。

6.8 投诉

检测机构应具有接收和处理投诉的管理程序，该程序应公开可用。检测机构应确认该投诉与检测机构负责的检测活动相关，必要时，在处理过程中与投诉人就投诉进展和处理结果进行沟通。对送达投诉人的决定，应由与投诉所涉及的检测活动无关的人员做出，或对其审查和批准。

6.9 不符合检测工作的控制

检测机构应制定不符合检测工作的管理制度。

注：在检测过程中出现不符合规程的情况时，检测人员该如何处理。

6.10 数据和信息的管理

6.10.1 检测机构应能够获得开展检测活动所需的数据和信息，应具有收集、处理、记录、报告、存储或者撤销数据的信息管理系统，对于管理系统的任何变更，都应授权后进行，并且记录变更情况，在使用前验证管理系统的正确性。

注：信息管理系统包括计算机环境和非计算机环境下对数据和信息的管理。

6.10.2 检测机构应管理和维护信息管理系统的安全性，确保数据和信息的完整性。当管理和维护非

检测机构的信息管理系统时，或通过外部提供商管理和维护检测机构的信息管理系统时，检测机构应确保其满足本标准的相关要求。

7 管理体系要求

检测机构应建立符合 GB/T 27025 中相关要求的管理体系。

8 行为准则

检测机构应遵守以下行为准则：

a） 遵守法律法规

检测机构应遵守国家法律法规和相关主管部门的要求，客观独立、公平公正、诚实信用地向社会各界开展检测服务，履行法律义务，承担法律责任和社会责任，接受相关主管部门的监督管理。

b） 服务客观公正

——坚持公开、平等的服务原则，对任何客户均不得附加任何歧视性的不合理要求，合理收费；

——不应与同行业机构结成经济联盟、垄断检测市场；

——不对相关主管部门和客户之外的组织和个人公开评价具体的被测产品和结果；

——不得将接收的被测产品、相关资料及检测过程中获取的被测产品相关信息用于检测之外的任何目的，特别是商业目的。

c） 检测活动守信

——检测人员资质信息真实可信；

——严禁出租资格证书、在报告上冒用他人签名；

——保障检测服务和报告质量，按规定格式如实出具检测报告，不故意隐瞒检测过程中发现的安全问题，或者在检测过程中弄虚作假；

——所出具的检测结果需要有充分的证据支持，并能够追溯到相应的过程记录。

d） 检测结果可追溯可复现

检测机构应保存检测原始记录和报告，保证检测结果的可追溯性。

必要时，检测机构应复现检测结果。例如：

——由同一检测人员对被测对象进行重复检测；

——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；

——使用不同的检测方法（技术）或同一类型的不同仪器或工具对同一被测对象进行检测。

e） 利益回避

——不接受客户及相关利益方的有可能影响检测结果的任何资金往来；

——不接受影响检测活动独立性、公正性的委托、代理和授权；

——不向有经济利害关系的客户投资参股，牟取经济利益；

——不向客户推荐产品，不要求其使用指定的产品或检测工具等；

——不介入客户之间的市场竞争；

——不从事信息技术产品（专用检测设备和工具以外）开发、销售和信息系统集成实施等活动。

f） 安全保密

检测机构应对检测活动中获得的或者生成的所有信息进行安全保密管理。

——可通过具有法律效力的承诺（例如合同、协议等）与客户约定双方的保密责任和义务、保密期限

等。应事先告知客户拟在公开场合发布的信息。除客户可公开的信息，或者检测机构与客户达成一致的信息外，所有其他信息都视为是客户专有信息，检测机构都应负有保密义务和责任。

注：所有其他信息包括客户及被测产品的相关信息（如产品未公开的通信协议和接口、加密方式、源代码、设计文档等）等。

——检测机构依照法律要求或者合同授权发布保密信息时，应通知相关客户，除非法律禁止；

——检测机构通过投诉者或者监管机构等途径获得的关于客户的信息不应告知客户，除非其同意；

——所有涉及检测活动的机构和人员（包括外部机构和人员），应对检测活动中获得或者生成的信息保密，除非法律要求；

——检测机构不应将检测活动中获得或者生成的客户专门信息，未经客户同意的情况下用于检测验证之外的其他用途；

——应将检测活动中的相关信息存储在我国境内。

g） 重大变更及时报告

检测机构发生下列事项变更时，应在变更后及时向相关部门报告。

——检测机构名称、地址、技术负责人、检测报告授权签字人发生变更的；

——检测机构或其所在组织的法人、股权结构发生变更的；

——其他重大事项发生变更的。

参 考 文 献

[1] GB/T 27021—2007 合格评定 管理体系审核认证机构的要求

[2] GB/T 30270—2013 信息技术 安全技术 信息技术安全性评估方法

[3] CNAS-CL46:2013 检测和校准检测机构能力认可准则在信息安全检测领域的应用说明

[4] 国家认监委关于印发《检验检测机构资质认定评审准则》及释义和《检验检测机构资质认定评审员管理要求》的通知(国认实〔2016〕33号)

[5] NIST Handbook 150-216 National Voluntary Laboratory Accreditation Program Procedures and General Requirements

[6] NISTHandbook 150-17 NVLAPCryptographicandSecurity Testing

[7] NISTHandbook 150-20 NVLAP Common Criteria Testing

[8] ISO-CASCO-WG44_N0100_DIS_ISOIEC_17025_with_WG_comments_in_track_changes