ICS 35.020

团　体　标　准

T/TSIA 005-2019

网络安全第三方服务机构管理规范

Network Security Third Party Service Organization Management Specification

2019－4－8 发布　　2019－4－8 实施

天津市软件行业协会 发布

目　录

前　言

本规范按照GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本规范起草单位：天津市网络文化行业协会、天津市软件行业协会、天津市互联网协会、天津市青少年网络协会、天津市网络社会组织联合会、天津市市场信息中心、江西省计算技术研究所、中科锐眼（天津）科技有限公司、中国检验认证集团天津有限公司、天津烽火信息管理技术有限公司、恒银金融科技股份有限公司、天津卓易云科技有限公司、博雅创智（天津）科技有限公司、北京可信华泰信息技术有限公司、北京天腾信科技有限公司、天津恒生科技园投资发展有限公司、恒安嘉新（北京）科技股份公司、四川远鉴科技有限公司、万业（天津）科技有限公司、天津同力兴科网络科技有限公司、江西畅然科技发展有限公司、天津市兴先道科技有限公司、北京云盾科技有限公司、天津润成信息安全技术有限公司、内蒙古网智科技服务有限责任公司、江苏百傲网络科技有限公司、天津中泰力达科技有限公司。

本规范主要起草人：王小龙、王森、孙凯桐、周效铭、赵洪宇、刘玺、解万永、吕顺刚、刘永杰、谷思源、李兴、苑久川、李宇、刘贵臣、杨雪飞、陆浩、郭昕、付康、宋午阳、张荣林、吴伯喜、张云峰、崔小玉、宋瑞霞、刘鑫、孙瑜、王梅、李明山、张峰晓、闫崑、王秋明、王炳文、袁青霞、曾建锋、刘立民、万俊、赵亮、张秀成、黄河、张力。

引　言

为加强和规范网络安全威胁评估、检测监测、安全工程服务等网络安全第三方服务机构的管理，规范网络安全第三方服务机构的行为，提高网络安全综合保障能力和服务水平，根据《中华人民共和国网络安全法》和相关标准及行业规范的要求，制定本管理规范。

网络安全第三方服务机构管理规范

1 范围

本规范适用于从事网络安全行业的服务机构，包括网络安全威胁评估机构、网络安全检测监测机构以及提供网络安全工程的相关机构。

软件和信息技术服务业、互联网行业、企业、事业单位、社会团体等组织机构在进行网络安全活动时也可遵循本管理规范。

相关工作的开展在网络安全监管单位和行业组织的领导下进行。

2 规范性引用文件

下列文件对于本文件的适用是必不可少的。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《修正案》）适用于本文件。

GB/T 5271.8 信息技术 词汇 第8部分:安全

GB/T 25068.3 信息技术 安全技术 IT网络安全

GB/T 25069 信息安全技术 术语

GB/T 31495.2 信息安全技术 信息安全保障指标体系及评价方法

ISO/IEC 27005 信息技术 安全技术 信息安全风险管理

3 术语和定义

ISO/IEC 27005、GB/T 5271.8、GB/T 25069 和 GB/T 25068.3、GB/T 31495.2 界定的术语和定义适用于本文件。为了便于使用，以下更加明确了相关术语和定义。

3.1 网络安全评价认定机构

网络安全评价认定机构，是指对网络安全第三方服务机构的服务能力和工程实施结果进行评价认定，对上线运行的业务和应用系统进行安全评价认定的机构。评价认定机构可以选择国家或地方认可的相关行业管理认定机构，如中国检验认证集团、中国信息安全测评中心以及中国网络安全审查技术与认证中心等。

3.2 网络安全第三方服务机构

网络安全第三方服务机构，是指负责对上线运行的业务和应用系统进行网络安全威胁评估，以及从事相关的网络安全服务工作的企事业法人机构，例如：网络安全检测监测、网络安全应急响应、网络安全运维以及网络安全工程实施等工作。

4 要求

4.1 概述

网络安全第三方服务机构管理规范，是对从事网络安全服务机构的管理体系、技术实力和网络安全工程实施过程质量保证能力等方面的综合评价认定。

网络安全第三方服务机构能力和方向的认定，是依据“规范性引用文件”中的国家法律法规和国家标准具体要求进行能力认定，即在对申请组织的基本资格、技术实力、网络安全服务能力以及安全项目的组织管理水平等方面的评估结果进行综合评定后，由评价认定机构给予对应的能力资质认证，网络安全服务机构具体分为三个方向：网络安全咨询类、网络安全威胁评估类以及网络安全工程类。

4.2 资格要求

网络安全第三方服务机构须在中华人民共和国境内注册成立（港澳台地区除外），由中国公民、法人或地方和国家投资的企事业单位。

4.3 规模与业绩要求

网络安全第三方服务机构应具备完善的管理体系及管理、技术和项目实施团队，有充足的流动资金，有足够的人员从事网络安全服务及相关活动，近一个自然年内在网络安全活动中无违规记录。

4.4 人员能力要求

网络安全第三方服务机构应具备相对稳定的技术支撑队伍，团队所有成员应具备两年以上信息安全从业经历或具备信息安全从业资格证书，项目负责人或技术骨干应具备信息安全专业人员资质证书，并熟练掌握信息安全基础理论和核心技术，有足够的专业工作经验，安全服务团队架构合理人员结构清晰。

4.5 管理要求

网络安全第三方服务机构必须拥有完善的服务质量保障体系，为开展网络安全服务提供可靠保障，必须具有专业从事信息安全服务的队伍和相应的质量保证措施，所有开展网络安全服务相关的成员需签订保密协议并遵守有关法律法规。

a） 网络安全第三方服务机构应制定管理规范，出具评估或服务报告时应加盖服务机构公章或服务专用章，未加盖用章的报告视为无效。

b） 网络安全第三方服务机构的相关从业人员必须具备从业资格证书和相关能力认证证书，未取得相关资质和能力认证的，不得参与或开展网络安全服务工作。

c） 网络安全第三方服务机构和从业人员实行年度审核，服务机构应将本单位的从业人员情况和服务情况真实有效的上报至监管单位和行业组织，相关服务人员不得采用挂靠或聘用兼职等情况开展网络安全服务业务，对于一年内未参与或未开展网络安全服务业务的相关机构，应注销其相关资质证书。

d） 网络安全第三方服务机构应建立健全管理制度和技术保障措施对所服务单位的相关情况应严格保密，保证在服务过程中所获得的重要敏感信息和个人信息不外泄；未经监管单位许可，不得擅用、滥用、擅自发布、披露在网络安全服务中收集掌握的网络状态、系统隐患、恶意代码、网络威胁等信息。

e） 网络安全第三方服务机构应加强对相关人员的监督管理，定期组织开展安全保密教育，签订安全保密协议和行业自律责任书，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。

f） 网络安全第三方服务机构提供网络安全服务不受地域、行业、领域的限制，网络安全服务项目采取统一登记备案管理。服务机构在实施服务项目之前，须将服务的项目信息及时、准确进行申报。

g） 网络安全第三方服务机构名称、地址、重要服务人员、主要负责人和联系人发生变更的，应在变更后 5 个工作日内向发证机构报备，并提交变更材料。

h） 网络安全第三方服务机构应组织从业人员和服务人员参加多种形式的网络安全服务业务和技术培训，从业人员每年培训时长累计不少于 10 课时，服务人员每年培训不低于20课时。

i） 网络安全第三方服务机构应根据监管单位要求定期向监管单位报备业务开展情况和相关威胁数据，服务机构在业务开展过程中，发现重大网络安全事件、重大网络安全风险隐患、高危漏洞和重大网络安全威胁时，应及时上报监管单位。

4.6 技术服务能力要求

网络安全第三方服务机构应有能力跟踪、了解和掌握国际、国内的安全动态、行业标准，了解信息网络安全的最新动向，有能力掌握最新的技术，具有持续技术更新迭代的能力，并建立健全符合相关标准要求的服务方法和流程，能够对信息系统开展调研、分析和描述，能够对发现、发生的安全隐患进行检测监测、分析、识别，并对其产生的危害和影响进行评估并给出相关的建议和应对方案。具体服务能力参考以下要求：

a） 网络安全咨询服务能力；

b） 网络安全风险评估服务能力；

c） 网络安全应急响应处置能力；

d） 信息系统灾难备份与恢复能力；

e） 网络安全运维能力；

f） 网络安全工程（集成）实施能力；

g） 网络安全事件识别分析能力。

4.7 设备及环境要求

网络安全第三方服务机构应有固定的办公场地和开展相关安全服务工作对应的设备和工具。

5 监督审查

监管单位和行业组织每年开展对网络安全服务机构的监督审查指导工作，在监督审查过程中发现不符合相关规范的或严重违规的给与警告、限期整改、取消服务资格等处罚，重点监督审查以下内容：

a） 网络安全第三方服务机构基本条件符合情况；

b） 网络安全第三方服务机构管理制度与保密制度落实情况；

c） 网络安全第三方服务机构服务评价，及人员管理与培训情况；

d） 网络安全服务项目实施情况，相关文档和数据管理情况；

e） 法律法规要求的其他需要监督审查的事项。

6 参考文献

《中华人民共和国网络安全法》

GB/T 20984-2007 信息安全技术 信息安全风险评估规范

GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南

GB/T 25069-2010 信息安全技术 术语

GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范

GB/T 22081-2016 信息技术 安全技术 信息安全控制实践指南

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

GB/T 32924-2016 信息安全技术 网络安全预警指南

GB/T 30271-2013 信息安全技术 信息安全服务能力评估准则

GB/T 29246-2017 信息安全技术 信息安全管理体系 概述和词汇

GB/T 35273-2017 信息安全技术 个人信息安全规范

GB/T 22080-2016 信息安全技术 信息安全管理体系 要求

GB/T 35279-2017 信息安全技术 云计算安全参考架构

GB/T 34978-2017 信息安全技术 移动智能终端个人信息保护技术要求

GB/T 35281-2017 信息安全技术 移动互联网应用服务器安全技术要求

GB/T 35283-2017 信息安全技术 计算机终端核心配置基线结构规范

GB/T 35284-2017 信息安全技术 网站身份和系统安全要求与评估方法

GB/T 35287-2017 信息安全技术 网站可信标识技术指南

GB/T 20985.1-2017信息安全技术 信息安全事件管理

GB/T 25066-2010 信息安全技术 信息安全产品类别与代码

GB/T 35625-2017 公共安全 业务连续性管理体系 业务影响分析指南

GB/T 36643-2018 信息安全技术 网络安全威胁信息格式规范

《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》

《互联网新闻信息服务新技术新应用安全评估管理规定》(公安部令第151号)