ICS 35.030
CCS L 80

团　　体　　标　　准

T/CIQA 39—2022

检验检测机构网络安全工作指南

Guidelines on cyber security of inspection and testing institutions

2022-07-08 发布　　2022-09-01 实施

中国出入境检验检疫协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由中国出入境检验检疫协会检验鉴定标准化技术委员会(CIQA/TC 1)提出并归口。

本文件起草单位：北京时代新威信息技术有限公司、华测检测认证集团股份有限公司、中理检验有限公司、青岛海检集团有限公司、力鸿检验集团有限公司、嘉德信(大连)检验测试科技有限公司、中国检验认证集团上海有限公司、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)、中国出入境检验检疫协会进出口商品检验鉴定机构分会。

本文件主要起草人：王新杰、王连强、杨玉忠、俞政臣、杜云浩、王亚涛、谭新星、王勋龙、费杨洁、童连松、杨毅、刘健、张琳。

引　言

网络安全风险是检验检测机构在开展检验、检测、认证等业务过程中的重大风险之一。如果不能有效地管理和控制网络安全风险，将导致检验检测机构的数据泄露、业务中断、客户投诉等重大损失，甚至还会带来法律责任，受到民事或刑事处罚。

选择正确的网络安全工作方法，是检验检测机构做好网络安全工作的基础。本文件第5章提出了检验检测机构网络安全工作方法的建议，为检验检测机构提供参考。这个方法包括建立网络安全工作的目标，识别和确定网络安全要保护的对象，开展网络安全风险评估，以及根据风险评估结果选择和建设网络安全控制措施。

履行网络安全的法律责任和法定义务，是检验检测机构网络安全工作的重要内容。截至目前，我国已经颁布实施的网络安全法律法规包括《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络安全审查办法》和《关键信息基础设施安全保护条例》等。

本文件第6章从检验检测机构应承担的网络安全法律责任入手，提出了检验检测机构应该开展的具体网络安全工作，如网络安全等级保护、商用密码应用安全性评估、数据安全保护、个人信息保护、网络安全审查和关键信息基础设施保护等，并提出了开展这些工作内容的具体方法和步骤，为检验检测机构提供参考。

网络安全是一项专业性很强的工作，并非所有的组织都具有满足其网络安全工作要求的网络安全能力。具有一定网络安全专业能力的检验检测机构，可以通过自身力量开展和落实上述具体网络安全工作。网络安全专业能力不足的检验检测机构，可以通过采购专业网络安全服务的方式来实现其网络安全目标，履行其网络安全责任。

检验检测机构网络安全工作指南

1 范围

本文件提供了检验检测机构开展网络安全工作的指南，描述了检验检测机构开展网络安全工作的方法，规定了检验检测机构必须开展和选择开展的网络安全工作任务。

本文件适用于任何类型、任何规模的检验检测机构的网络安全工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 20984 信息安全技术 信息安全风险评估规范

GB/T 22080 信息技术 安全技术 信息安全管理体系 要求

GB/T 22081 信息技术 安全技术 信息安全控制实践指南

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

GB/T 30146 公共安全 业务连续性管理体系 要求

GB/T 31595 公共安全 业务连续性管理体系 指南

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 39786 信息安全技术 信息系统密码应用基本要求

ISO/IEC 27701:2019 Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全 cyber security

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：《中华人民共和国网络安全法》，第七十六条(二)]

3.2

网络安全风险评估 cyber security risk assessment

识别网络安全风险、分析网络安全风险、评价网络安全风险的全过程。

3.3

网络安全控制措施 cyber security controls

保持和/或改变网络安全风险的手段。

注 1：包括但不限于制度、流程、设备设施、资源条件、活动等。