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 practices 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 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 2
5　网络安全工作方法 2
5.1　概述 2
5.2　网络安全工作方法在检验检测机构的应用 3
6　网络安全工作任务 5
6.1　总则 5
6.2　网络安全等级保护 5
6.3　商用密码应用安全性评估 6
6.4　个人信息合规审计 7
6.5　网络安全审查 7
6.6　关键信息基础设施安全风险评估 7
6.7　业务连续性管理体系（BCM）认证 8
6.8　信息安全管理体系（ISMS）认证 8
6.9　隐私管理体系（PIMS）认证 8
6.10　数据安全管理认证 9
附录 A（资料性）　网络安全法定义务识别指南 10
参考文献 12

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这些专利的责任。

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/TC1）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、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。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，遭受民事或刑事处罚。

选择一个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4章提出了一个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。截止目前，我国已经颁布实施的网络安全法律法规包括网络安全法、密码法、数据安全法、个人信息保护法、网络安全审查办法和关键信息基础设施保护条例等。

本文件第5章从检验检测机构应负的网络安全法律责任入手，提出了一个检验检测机构应该开展的具体网络安全工作内容，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内容。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

本文件为检验检测机构开展网络安全工作提供了指南，描述了检验检测机构开展网络安全工作的方法，列出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 19000 质量管理体系 基础和术语

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 信息安全、网络安全和隐私保护 信息安全控制

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 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

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

是指通过采取必要措施，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：中华人民共和国数据安全法，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。

注2：网络安全控制措施不一定总能发挥出其预期或假设的风险保持和/改变作用。

3.4

业务连续性管理体系（BCMS） business continuity management system

建立方针和目标，以保持和持续改进组织的业务连续性水平和能力的一组相互关联、相互作用的要素。

注：管理体系（MS）的定义，请参照GB/T 19000 3.5.3。

3.5

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

［来源：中华人共和国数据安全法，第三条］

3.6

信息安全管理体系（ISMS） information security management system

建立方针和目标，以保持和持续改进组织的信息安全保护水平和能力的一组相互关联、相互作用的要素。

注：本术语中的信息安全，等同于本文件中的网络安全（3.1）。

3.7

网络安全等级保护 cyber security classified protection

对信息系统进行定级、备案、建设整改、测评，以及公安机关对上述活动进行监督、检查的全过程。是国家网络安全工作的一项基本制度。

3.8

商业密码应用安全性评估 security assessment for application of commercial cryptography

识别、分析和评价组织商用密码应用安全风险的全过程。是国家商用密码管理工作的一项基本制度。

3.9

隐私管理体系（PIMS）privacy information management system

建立方针和目标，以保持和持续改进组织的隐私保护水平和能力的一组相互关联、相互作用的要素。

3.10

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。

注：不包括匿名化处理后的信息。

［来源：中华人共和国个人信息保护法安全法，第四条］

3.11

网络安全审查 cyber security audit and inspection

由网络安全主管部门实施的，对我国境内组织采购网络产品和服务中，影响或可能影响国家安全的，进行的审核和监督检查活动。

3.12

关键信息基础设施 critical information infrastructure

指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失公共或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

注：关键信息基础设施安全保护工作部门负责认定关键信息基础设施。

［来源：关键信息基础设施保护条例，第二条］

4 缩略语

下列缩略语适用于本文件。

GDSP：数据标准管理平台（Good Data Standard Practice）

LIMS：实验室信息管理系统（Laboratory Information Management System）

OA：办公自动化（Office Automation）

5 网络安全工作方法

5.1 概述

一个组织开展网络安全工作，本文件建议的方法是第一从建立网络安全目标出发，第二确定网络安全的保护对象，第三针对网络安全保护对象和组织环境开展网络安全风险评估，第四根据风险评估的结果，选择、建设和实施网络安全控制措施，最终通过控制措施的实施来实现已经建立的网络安全目标。图1描述了这一方法中各要素之间的逻辑关系。

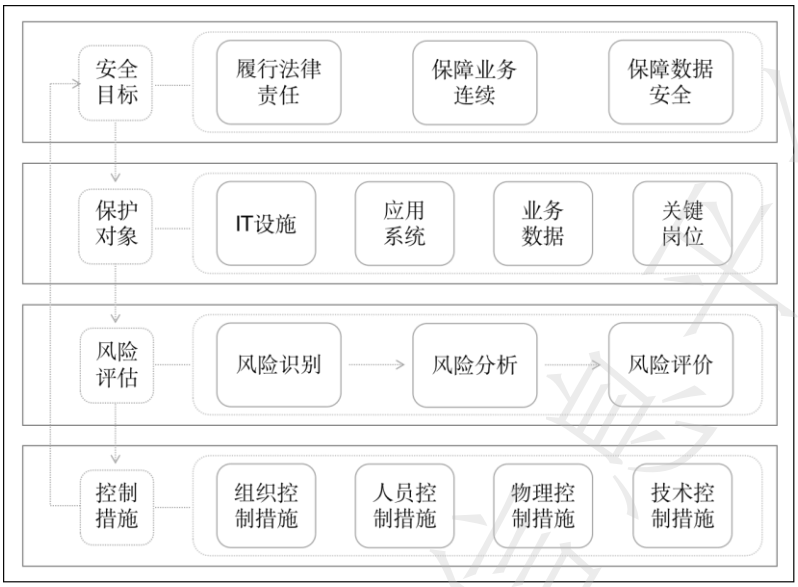

图1　网络安全工作方法逻辑示意图

实现网络安全目标是一个持续的过程，持续改进是应用这个方法需要遵循的基本原则。因为网络安全是一个动态的、持续的过程，没有任何一项或一组网络安全控制措施能够一劳永逸的消除所有的网络安全风险，网络安全风险总是随着时间的的变化而不断变化，且无法被彻底消除。所以，一个组织实现网络安全目标的工作是一个持续不断的过程。

5.2　网络安全工作方法在检验检测机构的应用

5.2.1　检验检测机构的典型网络环境

检验检测机构因其自身的网络环境使得其网络安全工作有其自身的特点。下面从一个检验检测机构本地化部署的典型网络环境入手，来说明检验检测机构如何应用上述网络安全方法开展网络安全工作。图2描述了一个检验检测机构本地化部署的典型网络环境。

图2　检验检测机构典型网络环境逻辑示意图

随着云计算的广泛普及，也有很多检验检测机构将本地化部署的网络系统部署在了公有云上，通过采购云服务商的云计算服务来实现自己的信息化和数字化应用。这种情况下，IT基础设施设备、操作系统和中间件等有关的网络安全工作就会转移给云计算服务商负责，检验检测机构应选择合格的云计算服务商，如要求云计算服务商提供等保测评报告、数据安全管理认证等。

5.2.2 建立网络安全目标

检验检测机构开展网络安全工作，首先要考虑网络安全目标，如图1所示。根据检验检测机构的业务特点，建立网络安全目标宜从以下三个方面考虑。

a) 履行法律责任。

检验检测机构作为一个法人组织，第一要考虑的就是要履行网络安全相关法律法规中规定的相关法定义务，目前我国已经颁布实施的相关法规包括网络安全法、密码法、数据安全法、个人信息保护法、关键信息基础设施保护条例和网络安全审查办法等，附录A提供了识别这些法规的网络安全法定义务的指南。此外，检验检测机构宜建立和维护识别法规要求的程序，以定期识别法规中网络安全要求。

b) 保障业务连续。

检验检测业务依赖于IT基础设施和应用系统的支持，如实验室业务依赖LIMS系统，营销业务依赖销售管理系统等。这些系统的稳定、可靠运行是检验检测机构实验室业务、营销业务等各类业务连续运行的基础。检验检测机构宜根据GB/T 30146业务连续性管理体系要求和GB/T 31595业务连续性管理体系指南建立和运行业务连续性管理体系来保障业务连续。

c) 保障数据安全。

数据已经成为检验检测机构重要的生产要素之一，数据也是检验检测机构的重要资产之一。保障数据安全，防止数据泄露、损坏、篡改或丢失，是检验检测机构的重要网络安全目标。

5.2.3 识别网络安全保护对象

检验检测机构宜建立和维护程序，以持续识别网络安全保护对象，并形成清单，定期对这个清单进行评审和维护，以确保保护对象清单的适宜性和完整性。检验检测机构识别网络安全保护对象，宜考虑以下四个方面。

a) IT 设施。

IT设施是检验检测机构信息化和数字化的物质基础，从图2中我们看到，一个检验检测机构的IT设施通常会包括数据中心、云计算、网络设备、服务器、存储设备、安全设备、个人终端设备等；通常操作系统、中间件、数据库系统等也会包含在这一部分中。

b) 应用系统。

应用系统是检验检测机构的日常工作的工具和平台，应根据应用系统所支持的业务类型的不同进行划分。通常检验检测机构常用的应用系统包括LIMS系统、GDSP系统、移动应用系统、官网和商城系统、签章加密系统、邮件和OA系统、销售管理系统、人事和财务系统、运维管控系统等。值得注意的是，这些应用系统，有些可能是检验检测机构自主研发的，有些可能是采购的商业软件，不同来源的应用系统，网络安全的需求也会不同。

c) 业务数据。

根据数据安全法的要求，检验检测机构宜对数据进行分类分级。如图2所示，一个检验检测机构典型的数据类型通常包括：检验检测数据、对象物数据、设备数据、检验检测过程中的原始记录数据、出具报告的数据、检验检测标准和方法的元数据、经营管理数据、财务数据、IT运维数据等。对于不同类型的数据，应根据数据的重要程度不同再进行分级，如一般数据、重要数据、核心数据等。涉密数据的相关工作遵守国家法律和行政法规的要求，不在本文件的范围之内。

d) 关键岗位人员。

IT相关岗位的人员，既是网络安全工作的主体，也是网络安全工作的客体，即保护对象。如图2所示，如系统管理员、应用管理员、数据库管理员、IT运维和安全专员，还可以包括网络管理员、设备管理员、IT审计人员等。对于这些关键岗位人员，应通过背景调查、能力验证等方式来降低人员安全风险。

5.2.4 开展网络安全风险评估

网络安全风险评估的目的是了解和掌握网络安全保护对象（5.2.3）所处的风险环境。执行风险评估应从识别保护对象自身存在的脆弱性和来自外部的威胁，以及这些威胁和脆弱性共同作用所产生风险

的可能性和严重程度，根据检验检测机构建立的风险评价准则和风险可接受准则形成风险评估报告。风险评估报告的核心内容是风险的列表和风险的排序，以及确定可接受的风险和必须采取措施处置的风险。

检验检测机构宜根据GB/T 20984信息安全风险评估规范开展风险评估。风险评估的主要方法和步骤是：

a） 风险识别。

检验检测机构宜选择一个适合的风险识别方法，从网络安全保护对象、保护对象的脆弱性和保护对象面临的威胁等方面，形成一个网络安全风险列表。

b） 风险分析。

确定一个适合的风险分析方法，无论是定性的，还是定量的，还是二者结合的，对所识别的风险进行分析，目的是判断一个风险发生的可能性和后果。

c） 风险评价。

检验检测机构应根据自身的业务特点和风险偏好，建立风险评价准则和风险可接受准则。根据风险评价准则，可以对风险按照严重程度进行排序；根据风险可接受准则，确定可以接受的风险和不能接受且必须采取控制措施处置的风险。最后，经过综合分析和汇总形成风险评估报告。

5.2.5 建设和实施网络安全控制措施

对风险评估报告中的不可接受的所有风险，检验检测机构应选择、建设和实施网络安全控制措施来减少、转移或规避风险，这就是风险处置。检验检测机构可以从GB/T 22081信息安全控制中选择控制措施，然后建设和实施。这些控制措施包括以下四类：组织类控制措施、人员类控制措施、物理类控制措施和技术类控制措施。

此外，为了更有效的建设和实施网络安全控制措施，检验检测机构可以按照GB/T 22080信息安全管理体系要求，建立和实施可持续改进的信息安全管理体系（ISMS），来实现其网络安全目标，保障网络安全。

注：GB/T 22080和GB/T 22081中的“信息安全”等同于本文件中的“网络安全”。

6 网络安全工作任务

6.1 总则

在检验检测机构的工作实践中，网络安全工作通常体现为若干项具体工作任务。这些工作任务应该从检验检测机构建立的网络安全目标中来。根据4.2.2建立的网络安全目标，检验检测机构的网络安全工作任务通常包括：

a） 网络安全等级保护；
b） 商用密码应用安全性评估；
c） 个人信息合规审计；
d） 网络安全审查；
e） 关键信息基础设施安全风险评估；
f） 业务连续性管理体系（BCMS）认证；
g） 信息安全管理体系（ISMS）认证；
h） 隐私管理体系（PIMS）认证；
i） 数据安全管理认证。

检验检测机构应适时维护其应开展的具体网络安全工作任务清单，如根据数据出境、个人信息保护认证等新政策的实施，适时开展个人信息保护认证、数据出境评估等相关工作任务。

6.2 网络安全等级保护

6.2.1 总则

网络安全等级保护是检验检测机构网络安全工作的必选项。实施网络安全等级保护的方法和步骤包括定级备案、建设整改、等保测评等。

6.2.2 定级备案

检验检测机构应根据GB/T 22240网络安全等级保护定级指南，对信息系统进行定级后向属地公安机关备案，取得备案证明。具体步骤如下：

a) 梳理和确定定级系统。可能是一个系统，也可能是多个系统；
b) 确定系统等级，一般为二级，或三级；
c) 准备定级备案材料；
d) 召开定级专家评审会；
e) 向检验检测机构所在地公安机关提交备案材料；
f) 取得备案号和备案证明。

6.2.3 建设整改

完成定级后，检验检测机构应根据GB/T 22239网络安全等级保护基本要求，开展相应等级的建设和整改，确保定级系统的安全保护措施满足和符合相应等级的要求。应从以下方面考虑安全措施的建设整改：

a) 安全物理环境；
b) 安全通信网络；
c) 安全区域边界；
d) 安全计算环境；
e) 安全管理中心；
f) 安全管理制度；
g) 安全管理机构；
h) 安全管理人员；
i) 安全建设管理；
j) 安全运维管理。

6.2.4 等保测评

完成建设整改后，检验检测机构应开展等保测评。三级系统每年测评一次，二级系统每两年测评一次。等保测评的步骤如下：

a) 选择适合的等保测评机构，签订测评合同；

注：中关村信息安全测评联盟定期发布的《全国网络安全等级测评与检测评估机构目录》，检验检测机构应从该目录中选择合格的测评机构。

b) 根据测评机构制定的测评实施方案，配合测评机构实施测评工作；
c) 对测评中发现的重大问题进行整改；
d) 完成重大问题整改后，通知测评机构进行复测；
e) 取得测评机构出具的测评报告；
f) 向备案的公安机关提交测评报告。

6.3 商用密码应用安全性评估

6.3.1 总则

对于具有等级保护三级系统、政务信息化系统和被关键信息基础设施安全保护工作部门认定为非涉密关键信息基础设施的检验检测机构，开展商用密码应用安全性评估是网络安全工作的必选项。开展商用密码应用安全性评估的方法和步骤包括：建设整改和开展评估。

6.3.2 建设整改

检验检测机构应根据GB/T 39786信息系统密码应用基本要求，开展相应等级的密码应用建设和整改，确保密码应用措施满足和符合相应等级的要求。应从以下方面考虑密码应用措施的建设整改：

a) 物理和环境安全；
b) 网络和通信安全；
c) 设备和计算安全；
d) 应用和数据安全；
e) 管理制度；

f） 人员管理；
g） 建设运行；
h） 应急处置。

6.3.3 开展评估

完成密码应用措施建设整改后，检验检测机构应开展评估。等级保护三级系统每年评估一次。评估的步骤如下：

a） 选择适合的密评机构，签订评估合同；

注：从国家密码管理局定期发布的《商用密码应用安全性评估机构目录》中选择合规的密评机构。

b） 根据密评机构制定的评估实施方案，配密评机构实施评估工作；
c） 对评估中发现的重大问题进行整改；
d） 完成重大问题整改后，通知密评机构进行复评；
e） 取得密评机构出具的评估报告；
f） 向系统备案的公安机关和/或商用密码管理部门提交评估报告。

6.4 个人信息合规审计

6.4.1 总则

个人信息合规审计是检验检测机构网络安全工作的必选项。开展个人信息合规审计的方法和步骤包括：个人信息保护建设和个人信息合规认证。

6.4.2 个人信息保护建设

检验检测机构按照个人信息保护法、GB/T 35273个人信息安全规范等法规和国家标准的要求，开展个人信息保护建设工作。建设内容应包括：

a） 制定个人信息保护管理制度和操作规程；
b） 实施个人信息实行分类管理；
c） 采取相应的技术措施，应包括加解密、去标识化、隐私计算、基于个人信息的自动化决策算法安全措施等；
d） 明确个人信息处理岗位和操作权限；
e） 定期开展个人信息保护安全教育和培训；
f） 制定并组织实施个人信息安全事件应急预案；
g） 当处理个人信息达到国家网信部门规定数量时，应指定个人信息保护负责人；
h） 必要时，应开展个人信息保护影响评估。

6.4.3 个人信息合规审计

检验检测机构应根据国家相关部门制定和实施的个人信息合规审计管理办法和个人信息合规审计指南，落实和开展个人信息合规审计工作。

6.5 网络安全审查

被关键信息基础设施安全保护工作部门认定为关键信息基础设施的检验检测机构，在采购网络产品和服务的过程中，应当预判该产品和服务投入使用后可能带来的国家安全风险，影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。

6.6 关键信息基础设施安全风险评估

6.6.1 总则

对于被关键信息基础设施安全保护工作部门认定为关键信息基础设施的检验检测机构，开展关键信息基础设施安全风险评估是网络安全工作的必选项。开展关键信息基础设施安全风险评估的方法和步骤包括：建设和评估。

6.6.2 关键信息基础设施保护建设

检验检测机构应根据关键信息基础设施保护条例的规定以及相关国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。具体包括以下内容：

a) 设置专门安全管理部门，并对专门安全管理部门负责人和关键岗位的人员进行安全背景审查；
b) 建立网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；
c) 开展网络安全监测、检测和风险评估；
d) 制定网络安全事件应急预案并定期进行演练；
e) 认定网络安全关键岗位，定期组织网络安全教育培训；
f) 对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；
g) 按规定报告网络安全事件和重要事项。
h) 采购安全可信的网络产品和服务，与产品和服务提供者签订安全保密协议。

6.6.3 关键信息基础设施风险评估

检验检测机构可以自行组织，也可以委托网络安全服务机构对关键信息基础设施每年至少开展一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照关键信息基础设施安全保护工作部门要求报送评估报告。

6.7 业务连续性管理体系（BCM）认证

6.7.1 总则

业务连续性管理体系（BCM）认证是检验检测机构网络安全工作的可选项。开展业务连续性管理体系认证的方法和步骤包括：BCM建设运行和BCM认证。

6.7.2 BCM 建设运行

检验检测机构应根据GB/T 30146业务连续性管理体系要求，建设和实施、运行和维护、监视和评审、保持和改进一个文件化的业务连续性管理体系。

6.7.3 BCM 认证

建设完成的业务连续性管理体系运行至少3个月后，检验检测机构选择适合的认证机构开展BCM认证，取得并维护BCM认证证书。

6.8 信息安全管理体系（ISMS）认证

6.8.1 总则

信息安全管理体系（ISMS）认证是检验检测机构网络安全工作的可选项。开展信息安全管理体系认证的方法和步骤包括：ISMS建设运行和ISMS认证

6.8.2 ISMS 建设运行

检验检测机构应根据GB/T 22080信息安全管理体系要求，建设和实施、运行和维护、监视和评审、保持和改进一个文件化的信息安全管理体系。

6.8.3 ISMS 认证

建设完成的信息安全管理体系运行至少3个月后，检验检测机构选择适合的认证机构开展ISMS认证，取得并维护ISMS认证证书。

6.9 隐私管理体系（PIMS）认证

6.9.1 总则

隐私管理体系（PIMS）认证是检验检测机构网络安全工作的可选项。开展隐私管理体系认证的方法和步骤包括：PIMS建设运行和PIMS认证

6.9.2 PIMS建设运行

检验检测机构应根据ISO/IEC 27701隐私管理体系要求，建设和实施、运行和维护、监视和评审、保持和改进一个文件化的隐私管理体系。

6.9.3 PIMS认证

建设完成的隐私管理体系运行至少3个月后，检验检测机构选择适合的认证机构开展PIMS认证，取得并维护PIMS认证证书。

6.10 数据安全管理认证

6.10.1 总则

数据安全管理认证是检验检测机构网络安全工作的必选项。开展数据安全管理认证的方法和步骤包括：数据安全管理建设和DSM认证。

6.10.2 数据安全管理建设

检验检测机构应根据数据安全法、数据安全相关标准开展数据安全管理（DSM）建设，应覆盖数据的收集、存储、使用、加工、传输、提供、公开等整个生命周期，以确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。数据安全管理建设的主要内容应包括：

a) 建立数据安全管理制度；
b) 组织开展数据安全教育培训；
c) 采取相应的技术措施，应包括以下方面：数据安全存储、数据保密、客户信息保护、原始数据防篡改、数据防造假、数据脱敏、基于数据的自动决策算法的安全措施、隐私计算等；
d) 有重要数据的检验检测机构应当明确数据安全负责人和管理机构；
e) 开展数据安全风险监测；
f) 有重要数据的检验检测机构应当定期开展数据安全风险评估；
g) 开展数据进行分级分类管理。

6.10.3 DSM认证

数据安全管理建设完成后，检验检测机构可以向中国网络安全审查技术与认证中心提出数据安全管理认证申请，取得并维护DSM认证证书。

附 录 A
（资料性）
网络安全法定义务识别指南

表A.1组织的网络安全法定义务给出了一个检验检测机构识别网络安全法定义务的方法。其中法律法律法规包括网络安全法、密码法、数据安全法、个人信息保护法、关键信息基础设施保护条例和网络安全审查办法。组织的法定义务是对上述法律法规相关条款中对一个组织网络安全法定义务的总结。最后一列给出了一项法定义务所对应的法规的具体条款。

表A.1 组织的网络安全法定义务

序号	法律法规	组织的法定义务	对应法规条款
1	网络安全法	保障网络安全、稳定运行，维护网络数据的完整性、保密性和可用性。	第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。
		举报维护网络安全的行为	第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。
		落实网络安全等级保护	第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务
		制定网络安全事件应急预案	第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。
		个人信息和重要数据境内存储和出境安全评估	第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。
		每年一次关基检测评估	第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。
		建设网络信息安全投诉、举报制度	第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。
2	密码法	商用密码应用安全性评估	第二十七条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。
3	数据安全法	数据处理总要求	第八条 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。
		数据安全检测评估 数据安全认证	第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。
		a) 建立数据安全管理制度 b) 开展数据安全教育培训 c) 采取数据安全措施 d) 明确数据安全负责人和管理机构	第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。 重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。
		数据安全风险监测	第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

序号	法律法规	组织的法定义务	对应法规条款
		重要数据风险评估	第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。
4	个人信息保护法	采取个人信息保护措施	第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失： （一）制定内部管理制度和操作规程； （二）对个人信息实行分类管理； （三）采取相应的加密、去标识化等安全技术措施； （四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训； （五）制定并组织实施个人信息安全事件应急预案； （六）法律、行政法规规定的其他措施。
		指定个人信息保护负责人	第五十二条 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。
		个人信息合规审计	第五十四条 个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。
		个人信息保护影响评估	第五十五条 有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录： （一）处理敏感个人信息； （二）利用个人信息进行自动化决策； （三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息； （四）向境外提供个人信息； （五）其他对个人权益有重大影响的个人信息处理活动。
		个人信息泄露报告	第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项： （一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害； （二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施； （三）个人信息处理者的联系方式。
5	关键信息基础设施保护条例	保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性	第六条 运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。
		设置安全管理机构和开展人员背景审查	第十四条 运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。
		每年一次网络安全检测和风险评估	第十七条 运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。
		重大事件和威胁报告	第十八条 关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。
6	网络安全审查办法	关基运营者和网络评估运营者应进行网络安全审查	第二条 关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。
		国外上市的网络安全审查	第七条 掌握超过100万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。
		网络安全审查办公室认为需要开展的网络安全审查	第十一条 网络安全审查办公室认为需要开展网络安全审查的，应当自向当事人发出书面通知之日起30个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关部门征求意见；情况复杂的，可以延长15个工作日。

参 考 文 献

[1] GB/T 25058-2019 信息安全技术 信息系统安全等级保护实施指南
[2] GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求
[3] GB/T 29246-2017 信息安全管理体系 概述和词汇
[4] GB/T 19001-2016 质量管理体系 要求
[5] 中华人民共和国网络安全法（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）
[6] 国家网络安全事件应急预案 （2017年1月10日中央网信办以中网办发文[2017]4号印发）
[7] 中华人民共和国数据安全法（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）
[8] 关键信息基础设施安全保护条例（2021年7月30日中华人民共和国国务院令第745号）
[9] 中华人民共和国个人信息保护法（2021年8月20日十三届全国人大常委会第三十次会议表决通过）
[10] 网络安全审查办法（国家互联网信息办公室2021年11月16日第20次室务会议审议通过）