|  |  |
| --- | --- |
| ICS | 35.040 |
| CCS | L 80 |

团体标准

P/CIQA-86-2021

检验检测机构网络安全工作指南

Guidelines for cyber security of inspection and testing institutions

（征求意见稿）

XXXX - XX - XX发布

XXXX - XX - XX实施

中国出入境检验检疫协会  发布

目次

[前言 III](#_Toc88579722)

[引言 IV](#_Toc88579723)

[1 范围 1](#_Toc88579724)

[2 规范性引用文件 1](#_Toc88579725)

[3 术语和定义 1](#_Toc88579726)

[4 网络安全工作概述 1](#_Toc88579727)

[5 网络安全工作方法 2](#_Toc88579728)

[5.1 网络安全目标 2](#_Toc88579729)

[5.2 网络安全保护对象 2](#_Toc88579730)

[5.3 网络安全风险评估 2](#_Toc88579731)

[5.4 网络安全控制措施 3](#_Toc88579732)

[6 网络安全工作任务 3](#_Toc88579733)

[6.1 网络安全等级保护 3](#_Toc88579734)

[6.2 数据保护 5](#_Toc88579735)

[6.3 个人信息保护 5](#_Toc88579736)

[6.4 开展网络安全教育培训 6](#_Toc88579737)

[参考文献 7](#_Toc88579738)

1. 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提出并归口。

本文件起草单位：

本文件主要起草人：

1. 引言

我国检验检测机构涉及健康、安全、卫生、环保和国计民生等多方面的数据和隐私信息资料，当前网络安全威胁日益严峻，恶意者或敌对者不断利用网络攻击窃取实验室数据，网络安全是检验检测机构信息化建设发展的“底线”，一旦发生网络安全事件，可能会给机构带来很大的负面影响。

网络安全不仅仅是安全设备和技术的堆砌，必须要依托科学的方法全面加强管理，目前网络安全已成为检验检测机构信息化发展的关键要素，需要我们对检验检测机构网络安全的建设和实施开展研究，明确检验检测机构开展网络安全工作需要遵循的方法和步骤。

《网络安全法》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。” 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，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。”

《数据安全法》第三条：“数据安全，是指通过采取必要措施，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。”

《密码法》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。”

《个人信息保护法》第四十条：“关键信息基础设施运营者和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，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。”

《关键信息基础设施保护条例》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。”

当前检验检测机构在网络安全治理中面临着管理制度不落地、部门职责不明确、资源底数不清晰、安全防护不到位、教育培训不充分等诸多问题，需要科学的网络安全工作方法指导，本文件为检验检测机构提供一条清晰的网络安全防护解决途径，从而有效的指导检验检测机构做好网络安全防护工作。

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规划建设、安全管理的方法，也为相关管理部门开展监督检查提供了指导。

本文件适用于任何类型、任何规模的检验检测机构（以下简称机构）。

* 1. 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—2007　信息安全技术　信息安全风险评估规范

GB/T 25069　信息安全技术　术语

* 1. 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

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：GB/T 22239—2019，3.1]

风险评估　risk assessment

依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

[来源：GB/T 20984—2007，3.7，有修改]

网络安全等级保护　cybersecurity classified protection

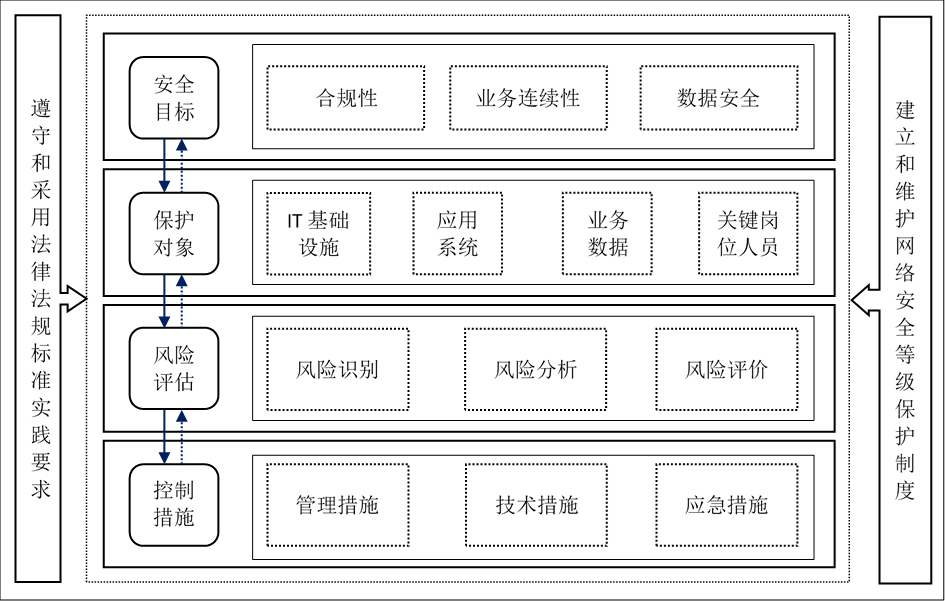
根据信息系统的重要程度，遭到破坏后造成的系统损失程度以及社会影响危害程度，对信息系统划分等级进行安全保护。

网络安全控制措施　cybersecurity control measures

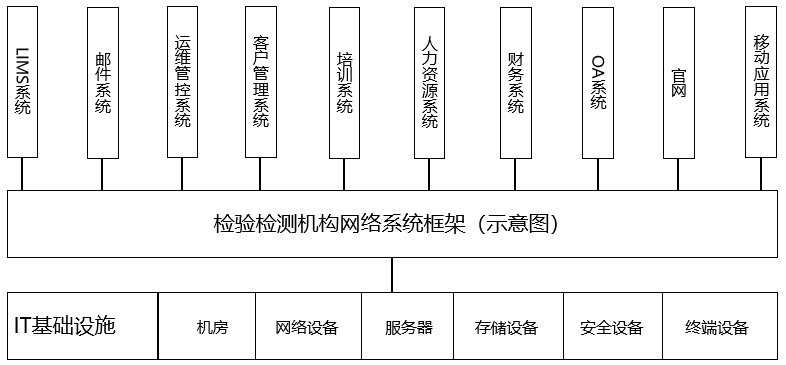
管控网络安全风险的方法，满足一组已定义的安全要求所需的任何过程、策略、设备、实践或其他行为。

* 1. 网络安全工作概述

机构的网络安全工作应基于以目标为导向的“组织网络安全”全局观，建立网络安全建设全景图，如图1所示。从组织的网络安全目标出发，结合组织实际情况，分析识别组织有效的保护对象，评估组织所面临的网络安全风险，选取适当的网络安全控制措施，最终达到机构网络安全建设和实施的目标。网络安全目标包含合规性、业务连续性和数据安全等三个目标；网络安全保护对象包含IT基础设施、应用系统、业务数据 、关键岗位人员等四个部分；网络安全风险评估包括风险识别、风险分析和风险评价的全过程；网络安全控制措施包含管理、技术和应急等三个部分控制措施。图2我们给出了检验检测机构网络系统框架图。



1. 网络安全建设全景图



1. 检验检测机构网络系统框架图
   1. 网络安全工作方法
      1. 网络安全目标

机构的网络安全目标包括：

1. 合规性：落实国家有关网络安全的法律、法规、政策和行业部门相关规定；
2. 业务连续性：根据业务连续性策略，制定应急响应计划和灾难恢复计划；
3. 数据安全：采取数据分类分级、数据分级保护等措施保障数据安全。
   * 1. 网络安全保护对象

机构的网络安全保护对象包括：

1. IT基础设施，例如：机房、网络、服务器、存储设备、安全设备、终端设备等；
2. 应用系统，例如：LIMS系统、邮件系统、运维管控系统、客户管理系统、培训系统、人力资源系统、财务系统、OA系统、官网、移动应用系统等；
3. 业务数据，例如：重要数据、过程数据、报告数据、跨境数据、隐私个人信息等；
4. 关键岗位人员，例如：管理部门的领导和管理人员、网络运维部门的系统管理员和工程师、数据库管理员等。
   * 1. 网络安全风险评估

机构的网络安全风险评估参见GB/T 20984-2007，包括：

1. 风险识别：按照机构网络的构成，开展资产识别、威胁识别、脆弱性识别等工作，最后汇总形成资产脆弱性列表；
2. 风险分析：完成风险识别以及对已有控制措施确认后，可采用适当的方法确定威胁利用脆弱性导致网络安全事件发生的可能性，判断网络安全事件造成的损失对机构的影响，即安全风险。

风险计算的方式如下：

风险值=脆弱性被利用的可能性等级×威胁利用脆弱性的影响程度等级×资产价值；

计算资产风险值，形成《资产风险值表》；

1. 风险评价：汇总上述分析报告和等级列表，从风险评估算法库中选择合适的风险评估算法，综合评价风险的等级，形成《风险评估报告》。
   * 1. 网络安全控制措施
   1. * 1. 安全管理措施

机构的安全管理措施包括：

1. 建立健全网络安全管理制度，明确网络安全负责人和管理部门，合理配备工作人员和信息联络员，明确各级岗位的工作职责，落实网络安全岗位责任和考核机制，从管理、技术、运营多维度保障数据安全；
2. 各信息资产或系统主管部门指定专人对接各项工作部署，配合、协调和处置网络安全工作；
3. 开展网络安全管理现状分析，查找网络安全管理建设整改需要解决的问题，明确网络安全管理建设整改的需求；
4. 确定网络安全管理目标和安全策略：

1) 网络安全建设管理涉及与网络建设活动相关的过程管理内容；

2) 网络安全运维管理涉及环境和资产安全管理、设备和介质安全管理、日常运行维护、集中安全管理、事件处置与应急响应、灾难备份、实时监测、其他安全管理等内容；

3) 网络安全人员安全管理，涉及人员录用、离岗、考核、教育培训等内容。

* + - 1. 安全技术措施

机构的安全技术措施包括：

1. 按照“同步规划、同步建设、同步使用”的原则，在网络系统设计、开发和使用的过程中，融入网络安全机制及策略；
2. 构建主动防御的安全防护体系，部署必要的网络安全产品；
3. 定制网络安全防护策略，建立认证、授权、访问控制等机制，例如，用户仅有分配的最小权限等；
4. 可购买第三方专业的网络安全服务，满足网络安全防护技术要求；
5. 定期开展风险评估工作，评估和改进已有防护体系的有效性。
   * + 1. 安全应急措施

机构的安全应急措施包括：

1. 按照国家有关要求，制定网络安全事件应急预案，组织网络安全应急力量，定期开展网络安全应急演练；
2. 发生网络安全事件时，启动应急预案，采取应急措施，控制和降低网络安全事件造成的危害和影响，消除安全隐患；
3. 发生重大网络安全事件时，按照网络安全应急预案要求，及时向上级监管部门报告，请求支持和帮助，联合开展应急响应处置。
   1. 网络安全工作任务
      1. 网络安全等级保护
4. 1. * 1. 识别确定定级对象

机构确定的等级保护定级对象包括：

1. 起支撑传输作用的基础信息网络（包括专网、内网、外网、网管系统等），从安全管理和安全责任的角度将基础信息网络划分成若干安全域或单元去定级；
2. 用于生产、调度、管理、作业、指挥、办公等目的的各类业务系统，按照不同业务类别单独确定为定级对象；
3. 单位网站、邮件系统作为独立的定级对象，如果网站的后台数据库管理系统安全级别较高，也可作为独立的定级对象；网站上运行的信息系统也可作为独立的定级对象；
4. 对于云平台、大数据、工业控制系统、物联网、移动互联网、卫星系统等，按照定级指南确定定级对象；
5. 确认负责定级的机构对所定级网络负有业务主管责任，业务部门主导对业务网络的定级，运维部门（例如信息中心、托管方）可以协助定级并按照业务部门的要求开展后续安全保护工作。
6. 具有网络的基本要素，作为定级对象的网络、信息系统是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的有形实体，避免将某个单一的系统组件（例如服务器、终端、网络设备等）作为定级对象。
   * + 1. 网络定级

机构遵循以下流程确定网络安全保护等级：

1. 确定定级责任主体：机构和行业主管部门是网络定级的责任主体；
2. 明确定级要素：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度；
3. 对各类网络定级的处理方法：

1）机构自建的网络（与上级单位无关），由本机构定级；

2）跨省或全国统一联网运行的网络或信息系统，可以由行业主管部门统一定级；

1. 专家评审：拟定为第二级以上的网络由机构组织专家评审；
2. 主管部门核准：有行业主管部门的在评审后报请主管部门核准；
3. 新建网络的定级：新建网络的网络运营者在规划设计时确定网络的安全保护等级，按照确定的网络等级，同步设计、同步建设、同步实施安全保护技术措施和管理措施。
   * + 1. 公安机关备案

机构遵循以下备案审核流程：

1. 网络安全保护等级在第二级及以上的定级对象，在网络安全保护等级确定后10个工作日内，机构到所在地设区的地市级以上公安机关网络安全保卫部门办理备案手续，提交定级报告；
2. 向公安机关备案第三级及以上的网络时，机构需要提交测评报告、经专家评审通过的安全建设方案等其他有关材料；
   * + 1. 网络安全建设

定级对象的网络安全保护等级确定后，机构按照有关管理规范和技术标准，选择符合要求的网络安全产品，制定并落实网络安全管理制度，建设网络安全设施，落实网络安全技术措施。

* + - 1. 等级测评与检测评估

机构遵循以下流程开展等级测评：

1. 网络建设整改完成后，从《全国网络安全等级测评与检测评估机构目录》中选择等级测评与检测评估机构，对网络安全保护状况开展等级测评与检测评估；
2. 对等级测评与检测评估中发现的安全风险隐患，机构制定整改方案，落实整改措施，消除风险隐患；
3. 涉及关键信息基础设施的安全建设整改方案，通过专家评审后方可实施。
   * + 1. 变更管理

机构的网络功能、服务范围、服务对象和处理的数据等发生重大变化时，需要依法变更网络的安全保护等级。

因网络撤销或变更调整安全保护等级的，机构在10个工作日内向原受理备案公安机关办理备案撤销或变更手续。

* + - 1. 实施关键信息基础设施的保护

机构主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门，根据国家有关认定规则负责组织认定检验检测领域的关键信息基础设施，及时将认定结果通知相关机构，并通报国务院公安部门。

机构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，实行重点保护：

1. 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；
2. 建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；
3. 建立健全网络安全监测预警制度，开展网络安全监测、检测和风险评估；
4. 制定网络安全事件应急预案，并定期进行演练；
5. 定期对从业人员进行网络安全教育、技术培训和技能考核；
6. 对重要系统和数据库进行容灾备份；
7. 建立有效的漏洞管理闭环机制，对发现和存在的安全风险漏洞进行有效管控；
8. 优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。
   * 1. 数据保护
   1. * 1. 确定数据保护对象

按照国家有关规定，根据数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益等造成的危害程度，将检验检测认证数据分为一般数据、重要数据和核心数据三级。

机构根据检验检测认证领域数据分类分级、重要数据和核心数据识别认定及数据分级防护等制度规范，形成重要数据和核心数据具体目录，实施动态管理，并将重要数据和核心数据目录报送主管部门，并采取措施开展数据分级防护，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施严格保护。

* + - 1. 建立数据安全管理制度

按照国家法律法规规定和制度要求，机构建立并落实数据安全管理制度：

1. 管理机制覆盖数据全生命周期的安全，保障机构重要数据和核心数据在收集、存储、使用、加工、传输、提供、公开、销毁等环节的安全；
2. 明确数据安全管理的责任部门和负责人，统筹负责数据处理活动的安全监督管理；
3. 确定数据处理活动的操作权限，严格实施人员权限管理；
4. 制定数据安全事件应急预案，并定期进行演练。
   * + 1. 采取数据安全保护措施

机构建立认证、授权、访问控制等机制，保障机构重要数据和核心数据的完整性、保密性和可用性。采取专门控制措施，管理跨境传输的数据。

* + - 1. 数据安全风险评估及整改

机构依据数据安全风险评估规范，加强风险监测，对发现的数据安全风险问题进行及时整改：

1. 对于一般数据，机构定期开展数据安全风险自评估；
2. 对于重要数据和核心数据，机构每年自行或者委托数据检测评估机构开展一次安全风险评估，并向主管部门报告。
   * 1. 个人信息保护
   1. * 1. 建立个人信息处理管理制度和操作规程

机构按照国家法律法规规定和制度要求，建立并落实个人信息处理管理制度。建立敏感个人信息保护机制，设置敏感个人信息使用限制或脱敏机制。

* + - 1. 制定个人信息安全事件应急预案

机构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，制定并组织实施个人信息安全事件应急预案。对可能损害用户合法权益的个人信息安全事件，应当及时告知用户，并提供减轻危害措施。

* 1. 1. 开展网络安全教育培训
        1. 网络安全意识宣贯

机构的网络安全意识宣贯包括以下内容：

* 1. 开展网络安全普及宣传教育，使机构全体人员，包括网络安全产品和服务提供商，了解他们的网络安全责任，提高网络安全防范意识；
  2. 按照机构的网络安全策略和相关规程建立网络安全意识宣贯方案，例如，组织宣传活动、发行宣传册或制作简报等；
  3. 定期安排宣贯方案中的活动，活动可以重复开展，并覆盖新进人员以及产品和服务提供商，宣贯方案根据机构的安全策略和管理规程定期更新，并汲取网络安全事件的经验教训；
  4. 每年组织一次全员网络安全宣贯培训。
     + 1. 网络安全人才教育和培训

机构网络安全人才教育和培训包括以下内容：

* 1. 建立网络安全知识学习平台，包含网络安全服务管理和防护技术等内容；
  2. 制定网络安全培训方案，培训可使用不同的媒介方式，包括现场教学、远程学习、网络教学、自学及其他。
     + 1. 应急演练培训

机构的应急演练培训包括以下内容：

1. 定期依照网络安全应急预案开展网络安全应急演练活动，使各相关部门和人员熟悉在发生安全事件时的工作职责和响应处置流程，积累工作经验；
2. 在定期演练的基础上，有针对性地拓展相关人员应急知识，例如，讲解常见网络安全事件的产生、应急流程制定原理、可能的后续处置方法等，提高相关人员检查、发现、处置常见网络安全事件的能力。

参考文献

1. GB/Z 20986—2007　信息安全技术　信息安全事件分类分级指南
2. GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求
3. GB/T 25058—2019　信息安全技术　信息系统安全等级保护实施指南
4. GB/T 28448—2019　信息安全技术　网络安全等级保护测评要求
5. GB/T 29246—2017 信息安全管理体系 概述和词汇
6. 国家突发公共事件总体应急预案（2005年1月26日国务院第79次常务会议通过）
7. 中华人民共和国突发事件应对法 （2007年8月30日第十届全国人民代表大会常务委员会第二十九次会议通过）
8. 突发事件应急预案管理办法 （2013年10月25日国务院办公厅以国办发[2013]101号印发）
9. 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）
10. 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）
11. 网络安全威胁信息发布管理办法（征求意见稿） （2019年11月20日国家互联网信息办公室发布征求意见稿）
12. 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）
13. 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）
14. 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）

