CTS

中标通国际认证（深圳）有限公司技术规范

CTS ZBTMS037-2026

网络空间信息安全管理体系 要求

Information Security in Cybersecurity Management System-Requirements

编制：王天鹏

审核：张道金

批准：黄　云

2026 年 05 月 09 日发布　　2026 年 05 月 09 日实施

目录

前　言

本技术规范规定了网络空间信息安全管理体系建立、实施、维持和持续改进等内容。

本技术规范由中标通国际认证（深圳）有限公司技术部提出。本技术规范主要起草人：王天鹏。本技术规范中标通国际认证（深圳）有限公司解释。

本认证技术规范的详细内容已与认证认可业务信息统一上报平台保持同步，鉴于其中包含知识产权相关信息，若需知晓本认证技术规范的具体条文内容，可按以下方式联系，经中标通国际认证（深圳）有限公司确认后，会向您提供本认证技术规范的文本信息。

通讯地址：深圳市光明区马田街道禾湾社区松白路 4545 号宏发天汇城二期 A 栋 408A

联系电话：0755-23696561；17520455475

电子邮箱：3300703251@qq.com

网络空间信息安全管理体系 要求

1 范围

本规范规定了网络空间信息安全管理体系要求的术语和定义、组织所处的环境、领导作用、策划、支持、运行、绩效评价和持续改进。

本规范适用于组织网络空间信息安全管理体系的建立、实施、监督和绩效考核。也适用于本公司对网络空间信息安全管理体系实施第三合格评定。

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/T29246-2023 IDT ISO/IEC 27000：2018《信息安全技术 信息安全管理体系 概述和词汇》

GB/T22080-2025 IDT ISO/IEC 27001：2022《网络安全技术 信息安全管理体系 要求》

GB/T22081-2024 IDT ISO/IEC 27002：2022《网络安全技术 信息安全控制》

ISO/IEC27032：2023《网络空间互联网安全指南》

3 术语和定义

GB/T29246-2023、GB/T22080-2025、GB/T22081-2024 和 ISO/IEC27032：2023 中的术语，以及下列术语和定义均适用于本文件。

3.1 攻击矢量

攻击者可以访问计算机和网络服务器以传递恶意结果的路径和手段。

示例 1：物联网设备。

示例 2：智能手机。

3.2 攻击者

故意利用技术和非技术安全控制中的脆弱性，窃取和破坏信息系统和网络，损害信息系统和信息

网络资源合法用户的可用性的人。

3.3 混合攻击

通过组合多种攻击媒介，寻求最大限度地提高损害的严重性和传染速度的攻击。

3.4 机器人程序

用于执行特定任务的自动化软件程序。

注 1：该词通常用于描述在服务器上运行的程序，该程序可以自动执行转发和排序电子邮件等任务。

注 2：机器人程序也被描述为作为用户、其他程序的代理和模拟人类活动的程序。在互联网上，最普遍的机器人程序是一种程序，也被称为蜘蛛、爬行器，它们访问网站并收集内容用于搜索引擎索引。

3.5 僵尸网络

在受损计算机上自主或自动运行的远程控制恶意机器人的集合。

示例：分布式拒绝服务（DDoS）节点，其中僵尸网络控制器可以引导用户计算机生成到第三方站点的流量，作为协调 DDoS 攻击的一部分。

3.6 网络空间安全

保护人民、社会、组织和国家免受网络空间风险。

注 1：保护意味着将网络风险保持在可容忍的水平。

3.7 暗网

互联网中只能使用特定软件访问的秘密网站网络。

注 1：暗网也被称为暗网站。

3.8 欺骗性软件

在用户的计算机上执行活动的软件，而不首先通知用户该软件将在计算机上执行的确切操作，或要求用户同意该操作。

示例 1：劫持用户配置的程序。

示例 2：一种程序，它会导致用户无法轻易停止那些无休止的弹出广告。

示例 3：广告软件和间谍软件。

3.9 黑客攻击

未经用户或所有者授权、故意访问其计算机系统。

3.10 黑客行动主义

出于政治或社会动机的黑客攻击。

3.11 互联网

公共领域的全球互联网络系统。

3.12 互联网安全

保护互联网信息的机密性、完整性和可用性。

注 1：此外，还可能涉及其他属性，如真实性、可问责性、不可否认性和可靠性等。

注 2：请参考 ISO/IEC27000：2018 第 3 条中关于保密性、完整性、可用性、真实性、责任性、不可否认性和可靠性的定义。

3.13 互联网服务提供商 ISP

为用户提供互联网服务并使其客户能够访问互联网的组织。

注 1：有时也称为互联网接入提供商（IAP）。

3.15 恶意软件/病毒软件

恶意设计的软件，包含可能直接或间接、对用户或用户的计算机系统造成伤害的特征和功能。

示例：病毒、蠕虫和特洛伊木马。

3.16 组织

具有自身职能、职责、权限和关系以实现其目标的个人或群体。

注 1：在本文件中，个人与组织是不同的。

注 2：一般来说，政府也是一个组织。在本文件中，为了清楚起见，可以将政府与其他组织分开考虑。

3.17 网络钓鱼

在电子通信中伪装成可信赖的实体，试图获取私人和机密信息的欺诈过程。

注 1：网络钓鱼可以通过使用社会工程和技术来实现。

3.18 可能多余的软件

欺骗性软件，包括具有欺骗性软件特征的恶意软件和非恶意软件。

3.19 垃圾邮件

可能携带恶意内容和诈骗信息的、未经请求的电子邮件

注 1：虽然最广泛认可的垃圾邮件形式是电子垃圾邮件，但该术语也适用于其他媒体中的类似滥用：即时消息垃圾邮件、网络新闻组垃圾邮件、网络搜索引擎垃圾邮件、博客垃圾邮件、维基作弊垃圾邮件、手机短信垃圾邮件、互联网论坛垃圾邮件和垃圾传真传输。

3.20 间谍软件

欺骗性软件，从计算机用户那里收集私人和机密信息。

注 1：信息可能包括最常访问的网站和密码等更敏感的信息。

3.21 威胁

意外事件的潜在原因，可能对系统、个人和组织造成伤害。

3.22 特洛伊木马

恶意软件，看似为用户执行所需功能，但误导用户并掩盖其真实意图。

3.23 话钓诈骗

伪装成可信赖的实体获取私人和机密信息的语音网络钓鱼。

注 1：可以通过语音电子邮件、VoIP（IP 语音）、固定电话和蜂窝电话进行浏览。

3.24 水坑攻击

煽动人们访问专门包含（大量）恶意软件的网站的技术。

注 1：水坑也称为挖坑。

3.25 万维网

网络可访问信息和服务的世界。

4 组织环境

4.1 理解组织及其环境

4.1.1 组织应确定与其意图相关的，且影响其达到网络空间信息安全管理体系预期结果能力的外部和内部事项。

组织应确定气候变化是否是一个相关事项。

4.1.2 网络空间安全内外部事项，例如：

－互联网安全、网站安全、网络安全和网络空间安全之间关系；

－互联网用户的个人身份信息（PII）被互联网上提供的许多网站和服务捕获；

－互联网的许多应用涉及信息交换和提供与人和个人信息无关的服务，个人信息 PII 因司法管辖区而异；

－虽然有些人在管理自己的在线身份时很谨慎，但大多数人会上传个人资料的详细信息与他人分享；

－互联网上的安全攻击已经从为个人名誉而进行的黑客攻击演变为有组织犯罪和网络犯罪；

－许多攻击工具也可在公共软件存储库和其他公共资源中获得；

－由于互联网是一个全球性的公共网络，交易可以来自世界任何地方，攻击也一样可以；

－所有相关方，即使不是恶意的，也对其需求、要求和威胁有不同的看法，因此他们有不同的风险和控制措施来应对；

－交易和协议的达成规范取决于司法管辖区的特定法律和监管环境；

－信息在互联网上即时传播，这意味着攻击也可能即时发生。

4.2 理解相关方的需求和期望

4.2.1 组织应确定：

a）网络空间信息安全管理体系的相关方；

b）这些相关方的有关要求；

c）哪些要求将通过网络空间信息安全管理体系予以解决。

注 1：相关方的要求包括法律、法规和合同义务。

注 2：相关方可能提出与气候变化相关的要求。

1）有关气候变化的更多信息，见 ISO 和国际认可论坛（IAF）关于管理体系标准中增加气候变化因索的联合公报。

4.2.2 相关方包括：

－使用互联网上的服务；

－利用互联网提供服务；

－提供互联网的基础设施和通信能力；

－全球协调互联网的运行；

－制定和执行法律法规。

4.3 确定网络空间信息安全管理体系范围

4.3.1 组织应确定网络空间信息安全管理体系的边界及其适用性，包括 PII 的处理，以建立其范围。

组织应根据以下内容确定网络空间信息安全管理体系范围：

a）4.1 中提到的外部和内部事项；

b）4.2 中提到的要求。

范围应形成文件化信息并可用。

4.4 网络空间信息安全管理体系

组织应按本文件的要求，建立、实现、维护和持续改进网络空间信息安全管理体系，包括所需的过程及其相互作用，防范网络空间特有信息安全风险。

5 领导

5.1 领导和承诺

最高管理层应通过以下活动，证实其对网络空间信息安全管理体系的领导和承诺：

a）确保建立网络空间信息安全方针和网络空间信息安全日标并与组织战略方向一致；

b）确保将网络空间信息安全管理体系要求整合到组织的业务过程中；

c）确保网络空间信息安全管理体系所需资源可用；

d）沟通有效网络空间信息安全管理的重要性和符合网络空间信息安全管理体系要求的重要性；

e）确保网络空间信息安全管理体系达到预期结果；

f）指导并支持相关人员为网络空间信息安全管理体系的有效性作出贡献。

g）促进持续改进；

h）支持其他相关管理角色在职责范围内证实其领导作用。

注：本文件中提到的“业务”能广义地解释为对组组存在目的核心意义的活动。

5.2 方针

最高管理层应建立网络空间信息安全方针，该方针应：

a）与组织的意图相适宜；

b）包括网络空间信息安全目标（见 6.2）或为设定网络空间信息安全目标提供框架；

c）包括对满足适用的网络空间信息安全相关要求的承诺：

d）包括对持续改进网络空间信息安全管理体系的承诺。

网络空间信息安全方针应：

a）形成文件化信息并可用；

b）在组织内得到沟通；

c）适当时，对相关方可用。

5.3 组织的角色、责任和权限

最高管理层应确保与网络空间信息安全相关角色的责任和权限在组织内得到分配和沟通。

最高管理层应分配责任和权限，以便：

a）确保网络空间信息安全管理体系符合本文件的要求；

b）向其报告网络空间信息安全管理体系绩效。

注：最高管理层也能在组织内分配报告网络空间信息安全管理体系绩效的责任和权限。

6 规划

6.1 应对风险和机会的措施

6.1.1 通则

当规划网络空间信息安全管理体系时，组织应明确 4.1 中提到的事项和 4.2 中提到的要求，并确定需要应对的风险和机会，以便：

a）确保网络空间信息安全管理体系能达到预期结果；

b）预防或减少不良影响；

c）达到持续改进。

组织应规划：

e）应对这些风险和机会的措施；

b）如何：

1）将这些措施整合到网络空间信息安全管理体系过程中，并予以实现；

2）评价这些措施的有效性。

6.1.2 网络空间信息安全风险评估

组织应定义并应用网络空间信息安全风险评估过程，以：

a）建立并维护网络空间信息安全风险准则，包括：

1）风险接受准则；

2）网络空间信息安全风险评估实施准则。

b）确保重复实施的网络空间信息安全风险评估能产生一致的、有效的和可比较的结果。

c）识别网络空间信息安全风险：

1）应用网络空间信息安全风险评估过程，以识别网络空间信息安全管理体系范围内与信息保密性、完整性和可用性损失有关的风险；

2）识别风险责任人。

d）分析网络空间信息安全风险：

1）评估 6.1.2 c）1）中所识别的风险发生后，可能导致的潜在后果；

2）评估 6.1.2 c）1）中所识别的风险实际发生的可能性；

3）确定风险级别。

e）评价网络空间信息安全风险：

1）将风险分析结果与 6.1.2 a）中建立的风险准则进行比较；

2）对已分析的风险进行风险处置优先级排序。

组织应保留有关网络空间信息安全风险评估过程的文件化信息。

6.1.3 网络空间信息安全风险处置

组织应定义并应用网络空间信息安全风险处置过程，以：

a）在考虑风险评估结果的基础上，选择适合的网络空间信息安全风险处置选项；

b）确定实现已选的网络空间信息安全风险处置选项所必需的所有控制；

注 1：组织能按需设计控制，或识别来自任何来源的控制。

c）将 6.1.3 b）确定的控制与附录 A 中的控制进行比较，并验证没有遗漏必要的控制；

注 2：附录 A 包含了可能的网络空间信息安全控制清单。本文件的用户在附录 A 的指引下，确保没有忽略必要的信息控制；

注 3：附录 A 所列的网络空间信息安全控制并不是完备的，且如有必要，组织能引入额外的网络空间信息安全控制。

d）制定适用性声明，其包含：

－必要的控制[见 6.1.3 b）和 c）]；

－选择这些控制的合理性说明；

－必要的控制是否已实现；

－删减附录 A 中控制的合理性说明；

e）制定正式的网络空间信息安全风险处置计划；

f）获得风险责任人对网络空间信息安全风险处置计划的批准和对网络空间信息安全残余风险的接受。

组织应保留有关网络空间信息安全风险处置过程的文件化信息。

6.1.4 威胁

－威胁者是指在执行和支持攻击中发挥任何作用的个人和个人团体。全面了解他们的动机（宗教、政治、经济等）、能力（知识、资金、规模等）和意图（乐趣、犯罪、间谍活动等）对于评估脆弱性、风险以及制定和部署控制措施至关重要；

－恶意软件、病毒、蠕虫、特洛伊木马等；

－互联网用户的个人身份信息（PII）面临的网络安全威胁主要围绕着个人信息泄露、盗窃带来的身份问题；

－端点设备（可能包括个人设备），设备（BYOD）将破坏变成僵尸和机器人；

－支持互联网的基础设施也可以成为目标；

－在国家和国际层面上，互联网是特定管辖区内非法行为猖獗的领域；

－犯罪分子可以合法购买为其犯罪提供便利的应用程序、服务和资源，也可以采取非法手段保护该资源以避免被发现和跟踪；

－威胁涉及故意修改公开和专有信息，制造虚假信息和恶作剧。

6.1.5 脆弱性

－脆弱性是指资产和控制的弱点、漏洞，可被威胁利用；

－一旦发现并解决了该弱点、漏洞，制造商、软件开发商和其他技术开发商就会制作安全更新和补丁来修复该弱点、漏洞。当系统接收到修补程序时，会添加更新和新元素。随着系统变得过时或不受供应商支持，或者没有修补到最新版本，可能会引入新的脆弱性；

－通过互联网访问的 Web 应用程序很容易受到各种脆弱性的影响，该脆弱性是由缺陷的设计、缺陷的代码编写、缺陷的应用数据库和可执行文件等引起的。

6.1.6 攻击矢量

－攻击矢量是攻击者可以访问计算机、网络服务器以实现恶意结果的路径和手段；

－端口扫描仪是攻击者使用的最古老且仍然非常有效的工具之一；

－最初的攻击总是针对面向公众的系统（例如路由器、服务器、防火墙、网站等），但攻击者也可以试图利用连接到该面向公众系统的专用网络内的资产；

－窃听沟通渠道是一种简单易用的攻击矢量；

－互联网上的许多攻击都是使用恶意软件进行的，例如间谍软件、蠕虫和病毒等；

随着用于共享数字音乐、视频、照片等文件的对等应用程序的激增，攻击者在如何将自己和其恶意代码伪装成特洛伊木马进行攻击方面变得越来越复杂；

－IP 欺骗，即攻击者操纵与其消息相关的 IP 地址，试图将其伪装成已知的可信来源，从而获得对系统的未经授权的访问。

－攻击者并不总是使用相同的攻击矢量，他会使用多个矢量并经常变更；

－物联网设备、智能手机等可以连接到互联网；

－高级持续威胁（APT）是一种攻击方法，其目标是在很长一段时间内窃取信息；

－另一种古老的攻击方法是使用暴力。

6.2 网络空间信息安全目标及其实现规划

组织应在相关职能和层级上建立网络空间信息安全目标。

网络空间信息安全目标应：

a）与网络空间信息安全方针一致；

b）可测量（如可行）；

c）考虑适用的网络空间信息安全要求，以及风险评估和风险处置的结果；

d）得到监视；

e）得到沟通；

f）适当时予以更新；

g）形成文件化信息且可用。

组织应保留有关网络空间信息安全目标的文件化信息。

在规划如何达到网络空间信息安全目标时，组织应确定：

a）要做什么；

b）需要什么资源；

c）由谁负责；

d）何时完成；

e）如何评价结果。

6.3 针对变更的规划

当组织确定需要变更网络空间信息安全管理体系时，应对这些变更的实施进行规划。

7 支持

7.1 资源

组织应确定并提供建立、实现、维护和持续改进网络空间信息安全管理体系所需的资源。

7.2 能力

组织应：

a）确定在其控制下工作且影响其网络空间信息安全绩效的人员的必要能力；

b）确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；

c）适用时，采取措施以获得必要的能力，并评估所采取措施的有效性；

d）保留适当的文件化信息作为能力的证据。

注：适用的措施可能包括，例如针对现有员提供培训、指导或重新分配工作；雇佣或签约有能力的人员。

7.3 意识

在组织控制下工作的人员应了解：

a）网络空间信息安全方针；

b）其对网络空间信息安全管理体系有效性的贡献，包括改进网络空间信息安全绩效带来的益处；

c）不符合网络空间信息安全管理体系要求带来的影响。

7.4 沟通

组织应确定与网络空间信息安全管理体系相关的内部和外部的沟通需求，包括：

a）沟通什么；

b）何时沟通；

c）与谁沟通；

d）如何沟通。

7.5 文件化信息

7.5.1 通则

组织的网络空间信息安全管理体系应包括：

a）本文件要求的文件化信息；

b）组织所确定的、对于网络空间信息安全管理体系有效性所必需的文件化信息。

注：不同组织有关网络空间信息安全管理体系文件化信息的详略程度可能是不同的，这是由于：

1）组织的规模及其活动、过程、产品和服务的类型；

2）过程及其相互作用的复杂性；

3）人员的能力。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的：

a）标识和描述（例如标题、日期、作者或引用编号）；

b）格式（例如语言、软件版本、图表）和介质（例如纸质的、电子的）；

c）对适宜性和充分性的评审和批准。

7.5.3 文件化信息的控制

网络空间信息安全管理体系及本文件所要求的文件化信息应得到控制，以确保其：

a）在需要的地点和时间，是可用的和适宜使用的；

b）得到充分的保护（例如避免保密性损失、不恰当使用、完整性损失）。

为控制文件化信息，适用时，组织应开展以下活动：

c）分发、访问、检索和使用；

注：访问可能隐含着仅允许浏览文件化信息，或允许并授权浏览和更改文件化信息等的决定。

d）存储和保护，包括保持可读性；

e）对变更的控制（例如版本控制）；

f）保留和处理。

组织确定的、为规划和运行网络空间信息安全管理体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。

8 运行

8.1 运行规划和控制

为了满足要求并实现第 6 章中确定的措施，组织应通过以下方式来规划、实现和控制所需的过程：

－建立过程的准则；

－根据准则实现对过程的控制。

文件化信息应可用，其程度足以确信这些过程按计划得到执行。

组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

组织应确保由外部提供的与网络空间信息安全管理体系有关的过程、产品或服务是受控的。

8.2 网络空间信息安全风险评估

组织应依据 6.1.2 a）所建立的准则，按计划的时间间隔，或当重大变更提出或发生时，执行网络空间信息安全风险评估。

组织应保留网络空间信息安全风险评估结果的文件化信息。

8.3 网络空间信息安全风险处置

8.3.1 总则

组织应实现网络空间信息安全风险处置计划。

组织应保留网络空间信息安全风险处置结果的文件化信息。

8.3.2 风险处置策略

应对互联网安全风险的有效方法包括多种策略的组合，并考虑到各利益相关方。

该策略包括：

－行业特定方法和工具，与所有相关方合作，以识别和解决互联网问题和风险；

－广泛的消费者和员工教育，为如何识别和解决组织内、互联网用户社区中的特定互联网风险提供可靠的资源；

－创新的技术解决方案，保护消费者免受已知的基于互联网的攻击，保持最新状态，并做好应对新攻击的准备；

－更新法律法规，使司法管辖区之间的正义得以伸张。

8.3.3 安全控制

组织应制定安全控制、程序和应对能力，以：

a）定义人员可接受使用互联网的规则；

b）定义哪些服务可以通过互联网公开；

c）识别威胁、脆弱性、攻击媒介及其相关风险；

d）界定互联网各用户的角色和责任；

e）让用户了解使用互联网的安全做法；

f）明确处理互联网安全问题的责任部门；

g）建立网络安全事件应对机制；

h）进行安全演习演练、测试，建立响应源自互联网攻击的机制。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a）需要被监视和的内容，包括网络空间信息安全过程和控制；

b）适用的监视、测量、分析和评价的方法，以确保得到有效的结果。所选的方法宜产生可比较和可再现的结果，才会被视为有效；

c）何时执行监视和测量；

d）谁监视和测量；

e）何时分析和评价监视和测量的结果；

f）谁分析和评价这些结果。

作为结果证据的文件化信息应可用。

组织应评价网络空间信息安全绩效和网络空间信息安全管理体系的有效性。

9.2 内部审核

9.2.1 通则

组织应按计划的时间间隔进行内部审核，以提供下列相关信息：

a）网络空间信息安全管理体系是否符合：

1）组织自身对网络空间信息安全管理体系的要求；

2）本文件的要求；

b）网络空间信息安全管理体系是否得到有效实现和维护。

9.2.2 内部审核方案

组织应规划、建立、实施和维护审核方案（一个或多个），包括审核频次、方法、责任、规划要求和报告。

组织应根据相关过程的重要性和以往审核的结果，建立审核方案。

组织应：

a）定义每次审核的审核准则和范围；

b）选择审核员并实施审核，确保审核过程的客观性和公正性；

c）确保将审核结果报告至相关管理层。

作为审核方案实施和审核结果证据的文件化信息应可用。

9.3 管理评审

9.3.1 通则

最高管理层应按计划的时间间隔评审组织的网络空间信息安全管理体系，以确保其持续的适宜性、充分性和有效性。

9.3.2 管理评审的输入

管理评审应包括下列相关信息：

a）以往管理评审提出的措施的状态。

b）与网络空间信息安全管理体系相关的外部和内部事项的变化。

c）网络空间信息安全管理体系相关方的需求和期望的变化。

d）有关网络空间信息安全绩效的反馈，包括以下方面的趋势：

1）不符合与纠正措施；

2）监视和测量结果；

3）审核结果；

4）网络空间信息安全目标完成情况。

e）相关方反馈。

f）风险评估结果及风险处置计划的状态。

g）持续改进的机会。

9.3.3 管理评审的结果

管理评审的结果应包括与持续改进机会相关的决定以及变更网络空间信息安全管理体系的任何需求。

作为管理评审结果证据的文件化信息应可用。

10 改进

10.1 持续改进

组织应持续改进网络空间信息安全管理体系的适宜性、充分性和有效性。

10.2 不符合与纠正措施

当发生不符合时，组织应：

a）对不符合做出反应，且适用时：

1）采取措施，对其予以控制和纠正；

2）处理其后果；

b）通过以下活动，评价采取消除不符合原因的措施的需求，以防止不符合再次发生或在其他地方发生：

1）评审不符合；

2）确定不符合的原因；

3）确定类似的不符合是否存在，或是否可能发生；

c）实现任何需要的措施；

d）评审任何所采取的纠正措施的有效性；

e）必要时，对网络空间信息安全管理体系进行变更。

纠正措施应与所发生的不符合的影响相适应。

作为以下证据的文件化信息应可用：

a）不符合的性质及所采取的任何后续措施；

b）任何纠正措施的结果。

附录 A

（规范性）

网络空间信息安全控制

本附录表 A.1 所列的网络空间信息安全控制，是直接源自 GB/T 22080-2025 之附录 A 信息安全控制、ISO/IEC27032-2023 第 7 章至第 9 章，并与之相一致，应与 6.1.3 一起使用。

表 A.1 网络空间信息安全控制

5	组织控制	
5.1	网络空间信息安全策略	控制： 应定义网络空间信息安全方针和特定主题策略，由管理层批准后发布，传达并让相关工作人员和相关方知悉，按计划的时间间隔以及在发生重大变更时对其进行评审
		网络空间特定控制： －组织应根据安全目标，制定并发布有关人员和其他相关方使用互联网的策略 －决定了使用哪些互联网服务、授权谁使用该服务以及安全目标是什么等 －此策略指导有关安全连接和使用互联网的所有其他控制措施 －互联网安全策略应由管理层定义、批准、发布并传达给相关人员、承包商和外部各方等，并得到其认可 －互联网安全策略应规定有权访问互联网的人员、他们可以查看的内容、禁止在互联网上进行的行为等。 －应将责任分配给与互联网有关的所有活动，以及适用于互联网安全的所有具体控制措施的设计、批准、实施、操作和监控
5.2	网络空间信息安全角色和责任	控制： 网络空间信息安全角色和责任应根据组织需求进行定义和分配
		网络空间特定控制： －用户是指使用互联网的个人、最终用户以及私营和公共组织 －用户角色可以包括但不限于以下内容： •一般互联网应用程序用户、实体用户，如网络游戏玩家、即时消息用户、网络冲浪者等 •买方/卖方，参与为感兴趣的买方在网上拍卖和市场网站上放置商品和服务，反之亦然 •博客作者和其他内容贡献者（例如维基上一篇文章的作者），其中文本和多媒体信息（例如视频剪辑）发布供公众和受限观众消费 •一个组织的成员（如公司的雇员、与公司的其他形式的协会等） •其他角色，用户可以在无意中或未经其同意的情况下被分配角色 －组织经常使用互联网来宣传公司和相关信息，以及与市场相关的产品和服务 －各组织还利用互联网作为其网络的一部分，收发电子信息（例如电子邮件）和其他文件（例如文件传输） －组织应积极确保其在互联网使用方面的做法和行动不会给互联网用户群体带来进一步的安全风险，从而将其企业责任扩展到互联网；应采取积极措施包括： •通过实施和操作有效的信息进行信息安全管理 •实施信息安全管理系统（ISMS） •执行基于 ISO/IEC27002 和其他相关标准的控制，但不运行 ISMS •安全监控和事件响应

		•将安全性作为软件开发生命周期（SDLC）的一部分，其中系统内置的安全级别应根据组织的数据关键性来确定； —通过持续的技术和流程更新以及跟踪最新技术发展，定期对组织内的用户进行安全教育 —了解并使用适当的渠道与供应商和服务提供商，就使用过程中发现的安全问题进行沟通
5.3	职责分离	控制： 应分离相互冲突的职责和责任范围
5.4	管理责任	控制： 管理层应要求所有工作人员根据组织已建立的网络空间信息安全方针、特定主题策略和规程，履行网络空间信息安全责任
5.5	与职能机构的联系	控制： 组织应建立并维护与相关职能机构的联系
		网络空间特定控制： —政府当局 •政府掌握着有关国家安全、战略、军事、情报问题以及与政府和国家有关的许多其他因素的信息，但也掌握着有关个人、组织和整个社会的大量信息 • 各国政府应保护本国的基础设施和信息不受未经授权的访问和利用 • 利用互联网提供电子政务服务的趋势越来越大 •政府当局在执法监管机构之间发挥着协调作用，在大规模网络攻击引发危机时，政府当局是在国家和企业层面传播信息和协调任何所需资源的主要协调人 •各国政府授权大学和高等学校实施网络安全教育方案，并确保组织适当的公私伙伴关系，建立必要的法律结构，组织执法监管机构并确定其任务 —执法监管机构：构执行法律法规，并要求所有相关方在其国家管辖范围内遵守相关法律法规
5.6	与特定相关方的联系	控制： 组织应建立并维护与特定相关方或其他专业安全论坛和专业协会的联系
		网络空间特定控制： —协调和标准化组织（ICANN、IETF、W3C 等）制定有关互联网使用和服务提供商提供的服务的技术标准 —在互联网上为组织提供角色和职责建议 —应在互联网安全的相关方之间进行高效和有效的信息共享、协调和事件处理 —该合作应以安全可靠的方式进行，同时保护相关个人的隐私 —许多相关方可能居住在不同的地理位置和时区，并可能受到不同监管要求的管辖 —信息共享和协作包括： • 建立相互信任的主要考虑因素 • 合作、信息交流和共享的必要过程 • 不同相关方之间的系统集成和可互操作性的技术要求
5.7	威胁情报	控制： 应收集并分析网络空间信息安全威胁相关的网络空间信息，以生成威胁情报
		网络空间特定控制： —威胁情报是关于威胁和威胁行为者的信息，有助于缓解网络空间中的有害事件 —信息安全人员应不断扫描威胁情报来源，例如社交媒体情报、人类情报、技术情报和来自暗网的情报等，收集信息，然后进行分析、评审 —应建立支持信息共享和协调的技术解决方案，以帮助准备和应对安全事件和网络事

		件。这是各组织作为其安全控制的一部分应该采取的重要步骤 －该解决方案应包括安全、有效、可靠和高效的信息共享和协调功能
5.8	项目管理中的网络空间信息安全	控制： 应将网络空间信息安全整合到项目管理中
5.9	网络空间信息及其他相关资产的清单	控制： 应编制和维护网络空间信息及其他相关资产（包括资产拥有者）的清单
		网络空间特定控制： －应确定包含关键信息和应用的信息和通信技术组成 －对于网络组件，组织应该了解敏感资产的位置，以及潜在攻击者的入口点 －各组织还应确定用于访问敏感信息和通信技术资产、在组织网络内传输敏感信息的关键路径；该路径不应被入侵者看到、访问和监控 －该清单应采用网络架构、功能位置和基础设施的形式，两者都清楚地表明与互联网的所有互连网络的入口和连接点 －应确定、记录和实施与互联网相关的资产和处理设施的可接受使用规则和处理程序 －组织应制定并使用程序来评估持有、转让信息和通信技术资产的关键性 －组织能够清楚地确定在通用策略和网络安全方面应该保护什么、在什么级别上保护等
5.10	网络空间信息及其他相关资产可接受使用	控制： 应识别、文件化并实施网络空间信息及其他相关资产的可接受使用规则和处理规程
5.11	资产归还	控制： 适宜时，工作人员和其他相关方在任用、合同或协议变更及终止时，应归还其拥有的所有组织资产
		网络空间特定控制：网络空间供应商的网络空间客户的资产应在网络空间协议终止后及时移除，并在必要时返还
5.12	网络空间信息分级	控制： 应根据组织基于保密性、完整性、可用性的网络空间信息安全需求以及相关方的要求，对网络空间信息进行分级
5.13	网络空间信息标记	控制： 应按组织采用的网络空间信息分级方案，制定并实施适当的网络空间信息标记规程
		网络空间特定控制：
5.14	网络空间信息传输	控制： 应为组织内部以及组织与其他各方之间所有类型的传输设施，制定网络空间信息传输规则、规程或协议
5.15	访问控制	控制： 应基于业务和网络空间信息安全要求，建立和实施网络空间信息及其他相关资产的物理和逻辑访问控制规则
		网络空间特定控制： －访问控制不仅包括用户的访问权限，还包括设备、应用程序和自动化编程等权限 －每个连接都应该经过身份验证，每个活动都应该根据根据业务和安全规则建立的角色和权限进行正式授权，每个实体都应该被分配最低特权的权限 －帐户应仅限于因其工作角色、功能而获得授权的用户 －每个用户都应该有单独的帐户，不应该共享该帐户，也不应该多个帐户使用相同的密码

		－应根据组织的访问控制策略和程序，提供、审查、调整、修改和删除对信息、系统、应用程序和服务的访问权限 －应限制和控制特权访问权的分配和使用 －应根据信息访问限制和相关访问控制规则实施安全的身份验证技术和程序 －应建立密码管理系统，以管理和支持密码创建过程及其保密质量 －直连到互联网的信息系统（例如防火墙基础设施、网络外围设备等）可以具有一个或多个特权实用程序，该程序可以覆盖系统和应用程序控制 －该程序应由组织充分控制，这样入侵者就不会访问该特权实用程序并越过系统和应用程序控制 －有效的访问管理应包括： •定期审查所有访问权限 •定期审查管理日志
5.16	身份管理	控制： 应管理身份的全生存周期
		网络空间特定控制：
5.17	鉴别网络空间信息	控制： 应通过管理过程控制鉴别网络空间信息的分配和管理，包括向工作人员提供鉴别网络空间信息的适当处理建议
		网络空间特定控制：
5.18	访问权限	控制： 应根据组织访问控制的特定主题策略和规则来提供、评审、修改和删除网络空间信息及其他相关资产的访问权限
		5.18.1 网络空间特定控制：
5.19	供应商关系中的网络空间信息安全	控制： 应定义并实施过程和规程，以管理供应商产品或服务使用相关的网络空间信息安全风险
		网络空间特定控制： －应确定并实施程序，以管理与供应商使用相关的互联网安全风险 －应根据供应商类型和相关风险，制定所有相关的信息安全要求，并与每个供应商达成一致 －与信息和通信技术供应商及其存储、利用和访问的信息相关的风险管理是制定合同的关键，以确保持续实现组织的信息安全目标 －应与互联网相关的供应商（例如互联网服务和云服务提供商等）签订协议并形成文件，以确保组织和供应商之间明确了解双方应履行相关信息安全要求的义务 －组织应与互联网服务提供商、电信服务提供商、云服务提供商和合作伙伴建立开放的合作伙伴关系，以通报、警告检测到的引入威胁 －应确定并定期监测互联网服务提供商以安全方式管理商定服务的能力。组织宜与服务提供商将就审计权达成一致 －对于可通过互联网访问并由组织采购的云服务，组织应审查并与云服务提供商协商云服务协议 －组织应进行相关风险评估，以确定与使用云服务相关的风险，并在协议期限内管理风险 －云服务协议宜将解决组织的机密性、完整性、可用性和 PII 处理等要求 －对于任何组织无法协商协议条款的云服务，组织宜在签订协议时应尽责勤勉，了解使用该服务的风险以及如何在协议期限内管理该风险 －组织必须对该基于云工具的使用建立安全控制

5.20	在供应商协议中强调网络空间信息安全	控制：应根据供应商关系的类型建立相关的网络空间信息安全要求，并与每个供应商达成一致
		网络空间特定控制： 为了满足已确定的互联网安全要求，应考虑将以下内容纳入协议： －法律法规要求，包括 ISP 端的信息保护要求，例如抵御 DDoS 和其他攻击等 －各合同方有义务实施一套商定的控制措施，包括访问控制、网络和系统监控、报告和审计等，以及供应商遵守组织安全要求的义务 －事件管理要求和程序（尤其是事件补救期间的通知和协作） －对供应商服务进行监测、审查和变更管理，以确保遵守协议的信息安全条款和条件，并允许对服务绩效水平进行监测，以验证对协议的遵守情况，监测供应商所做的产品和服务的变更
5.21	管理信息通信技术供应链中的网络空间信息安全	控制： 应定义并实施过程和规程，以管理与网络空间信息通信技术 ICT 产品和服务供应链相关的网络空间信息安全风险
		网络空间特定控制： －提供服务的组织可以包括两类： • 为员工和合作伙伴提供互联网接入服务； • 互联网消费者服务提供商。 －分销商和零售商应提供足够的安全和合法访问，支持服务通常默认返回给运营商和批发商。 －互联网服务提供商（ISP）应通过监督“流量”和提供替代路线和主机进行流量控制来提供支持。 －服务提供商应在互联网上寻找“危险”的交易，在必要的法律授权和用户的授权，过滤危险的内容 －服务提供商当他们发现威胁迹象时，服务提供商应警告他们的客户
5.22	供应商服务的监视、评审和变更管理	控制： 组织应定期监视、评审、评价和管理供应商网络空间信息安全实践和服务交付的变更
5.23	网络空间使用的网络空间信息安全	控制： 应根据组织的网络空间信息安全要求，建立网络空间的获取、使用、管理和退出过程
5.24	网络空间信息安全事件管理规划	控制：组织应通过定义、建立和传达网络空间信息安全事件管理过程、角色和责任，为管理网络空间信息安全事件做出规划和准备
		网络空间特定控制： －应建立一个事件管理小组（IMT）和一个支持事件响应小组（IRT），为组织提供评估、响应和从该事件中学习的能力 －事件响应程序应考虑通过人工或自动方式检测和报告安全事件的发生，例如潜在和实际事件 －组织实施的监控工具可以是检测和发送安全事件，以便响应之 －与互联网安全有关的事件应由指定的联系人、组织和相关方的其他相关人员作出回应 －在实施事件管理程序时，应考虑在规定时间内向相关利益方报告事件的任何外部要求（例如在规定时间内向监管机构报告事件通知的要求等）
5.25	网络空间信息安全事态	控制： 组织应评估网络空间信息安全事态，并决定是否将其归类为网络空间信息安全事件

	的评估和决策	
5.26	网络空间信息安全事件的响应	控制： 应按文件化的规程响应网络空间信息安全事件
5.27	从网络空间信息安全事件中学习	控制： 应使用从网络空间信息安全事件中得到的知识来加强和改进网络空间信息安全控制
		网络空间特定控制： －从评估面向互联网的系统的安全事件中获得的信息，应用于识别重复发生的、相关的事件，以便计划和实施更改，以减少未来类似事件的可能性和影响 －IPS 和 SIEM 等工具可以根据安全事件的评估进行重新配置，并可以启动相关的策略更新，以防止未来发生事件
5.28	证据收集	控制： 组织应建立并实施包括识别、收集、获取和保存网络空间信息安全事态相关证据的规程
		网络空间特定控制： －使用互联网的组织应确定适用的信息识别、收集、获取和保存程序，该程序可作为安全事件的证据 －根据监测日志和其他数字证据，如果事件被证明来自另一个国家，预估收集证据的方式是否被适当的国家法院和国际当局接受 －在发生安全事件时，数字证据可以超越组织和管辖范围 －应确保组织有权收集所需信息，作为未来行动的数字证据 －应正确设置计算机时钟对于确保审计日志的准确性非常重要，审计日志可用于在发生任何来自互联网的攻击时进行调查，也可作为可能的法律行动的证据
5.29	中断期间的网络空间信息安全	控制： 组织应制定在中断期间将网络空间信息安全维持在适当级别的计划
5.30	业务连续性的网络空间信息通信技术就绪	控制： 应根据业务连续性目标和网络空间信息通信技术 ICT 连续性要求，策划、实施、维护和测试 ICT 的就绪
		网络空间特定控制： －互联网基础设施的任何中断都会对组织构成连续性风险，应由组织解决 －组织应计划从不同的互联网服务提供商处采购互联网服务，以实现基本的连续性措施 －组织应部署安全措施以避免中断，例如针对网络设备连续性的防 DDoS 措施 －组织还可以要求相应的 ISP 在其网络内部署防 DDoS 措施 －无论连续性服务是否，在 ISP 业务连续性模式下，组织应持续考虑 ISP 解决方案中的信息安全
5.31	法律、法规、规章和合同要求	控制： 应识别与网络空间信息安全相关的法律、法规、规章和合同要求，以及组织满足这些要求的方法，并将其文件化且保持更新
		网络空间特定控制： －互联网被用作部署许多在线交易服务的平台，应符合可能涉及保护交易细节的机密性、完整性和可用性的数据安全、网络安全和隐私法律法规 －银行交易、支付渠道、基于移动应用程序的交易和其他电子商务活动通常因涉及数字形式的资金而应受到监管 －所有信息安全和网络安全相关的法律法规、监管和合同要求，和组织满足该要求的方

		法都应予以识别、记录并保持最新 －根据法律、法规、监管、合同和业务要求，通过互联网访问的在线系统上保存的记录应受到保护，确保不丢失、销毁、篡改、未经授权的访问和未经授权发布等 －可将记录作为组织符合法定和监管规则范围内运营的证据，以确保对潜在的民事和刑事诉讼进行辩护，或向相关方确认组织的财务状况
5.32	知识产权	控制： 组织应实施适当的规程来保护知识产权
5.33	记录的保护	控制： 应保护记录不被丢失、破坏、篡改和未经授权的访问和未经授权的发布
		网络空间特定控制：
5.34	隐私和个人可识别网络空间信息保护	控制： 组织应根据适用的法律、法规和合同要求，识别并满足有关隐私保护和个人可识别网络空间信息 PII 保护的要求
		网络空间特定控制： －服务要符合最佳实践标准，遵守覆盖用户隐私要求的最低协议条款 －除了确定面向互联网的网站、应用程序的数据保护和个人隐私规定外，服务提供商还应要求托管在其网络上的网站、应用软件在上线前，于应用程序层面实施整套最佳实践安全控制 －在互联网上提供注册、服务之前，组织应进行隐私影响评估（PIA），以确定可以使用、收集、处理、存储和传输的个人信息以及相关的隐私风险，以确定该信息安全风险是否为组织所接受，并进行相应的管理。这不仅包括收集客户数据以提供服务，还可以包括收集元数据，例如浏览网站的个人的 IP 地址、地理位置数据等 －组织应在其网站上发布隐私声明，明确告知所有用户与组织在线服务互动、沟通的要求 －应根据法律要求、组织的访问控制策略和业务要求使用数据屏蔽 －DLP 措施应适用于处理、存储和传输敏感信息的系统和网络 －某些互联网浏览器具有技术功能，允许用户更改隐私设置
5.35	网络空间信息安全的独立评审	控制： 组织管理网络空间信息安全的方法及其实现，包括人员、过程和技术，应在计划的时间间隔内或发生重大变化时进行独立评审
		网络空间特定控制：
5.36	符合网络空间信息安全的策略、规则和标准	控制： 组织应定期评审与组织网络空间信息安全方针、特定主题策略、规则和标准的符合性
5.37	文件化操作规程	控制： 网络空间信息处理设施的操作规程应形成文件，并对有需要的工作人员可用
6	人员控制	
6.1	审查	控制： 加入组织前，应对所有拟录用工作人员的候选人进行背景审查，并在入职后持续进行，同时考虑适用的法律、法规和道德规范，与业务要求、访问网络空间信息的级别和感知到的风险相适宜
6.2	任用条款和条件	控制： 应在任用合同协议中规定工作人员和组织对网络空间信息安全的责任
6.3	网络空间信	控制：

	息安全意识、教育和培训	组织工作人员和相关方应接受适宜的网络空间信息安全意识、教育和培训，并获得与其工作职能相关的组织网络空间信息安全方针、特定主题策略和规程的定期更新网络空间信息
		网络空间特定控制： 一组织的人员（包括最高管理层、系统管理员、IT 员工和特权用户等）应定期更新主要威胁（例如网络钓鱼和视频聊天等）以及预防威胁的措施，并在操作了不当措施时做出回应 一组织应使用各种形式，例如电子邮件通信、在线培训和通过内部网发送信息等，定期向人员提供意识和培训材料，以告知人员在线威胁、他们可接受的使用和报告事件的义务
6.4	违规处理过程	控制： 应正式制定违规处理过程并将之传达给工作人员和相关方，以便对违反网络空间信息安全策略的工作人员和其他相关方采取措施
6.5	任用终止或变更后的责任	控制： 应确定任用终止或变更后仍有效的网络空间信息安全责任及其义务，传达至相关工作人员和其他相关方并执行
6.6	保密或不泄露协议	控制： 应识别、文件化、定期评审反映组织网络空间信息保护需求的保密或不泄露协议，并与工作人员和其他相关方签署
6.7	远程工作	控制： 应在工作人员远程工作时实施安全措施，以保护在组织场所外所访问的、处理的或存储的网络空间信息
6.8	网络空间信息安全事态的报告	控制： 组织应提供机制，使工作人员通过适当渠道及时报告观察到的或可疑的网络空间信息安全事态
7	物理控制	
7.1	物理安全边界	控制： 应定义并使用安全边界来保护包含网络空间信息及其他相关资产的区域
		网络空间特定控制： 一确保内部网络与内部边界保护充分隔离，将关键、重要组件于入口点隔离，并易于进入内部传输通道
7.2	物理入口	控制： 安全区域应由适当的入口控制和访问点保护
7.3	办公室、房间和设施的安全保护	控制： 应对办公室、房间和设施的物理安全进行设计并予以实施，例如自然灾害和其他对基础设施有意或无意的物理威胁
7.4	物理安全监视	控制： 应持续监视场所，以防止发生未经授权的物理访问
7.5	物理和环境威胁防范	控制： 应对物理和环境威胁的防范进行设计并予以实施，例如自然灾害和其他对基础设施有意或无意的物理威胁
7.6	在安全区域工作	控制： 应设计并实施在安全区域工作的安全措施
7.7	清理桌面和屏幕	控制： 应定义并适当地执行纸质和可移动存储媒体的桌面清理规则和网络空间信息处理设施

		的屏幕清理规则
7.8	设备安置和保护	控制： 应安全地安置并保护设备
7.9	组织场所外的资产安全	控制： 应保护组织场所外的资产
7.10	存储媒体	控制： 存储媒体应在其获取、使用、运输和处置的整个生存周期内，按组织的分级方案和处理要求进行管理
7.11	支持性设施	控制： 应保护网络空间信息处理设施使其免于由支持性设施的故障而引起的电源故障和其他中断
7.12	布缆安全	控制： 应保护传输电力、数据或支持网络空间信息服务的电缆免受窃听、干扰或损坏
7.13	设备维护	控制： 设备应予以正确维护，以确保网络空间信息的可用性、完整性和保密性
7.14	设备的安全处置或重复使用	控制： 应对包含存储媒体的设备的所有部分进行核查，以确保在处置或重复使用之前，任何敏感数据和获得许可的软件已被删除或安全地覆写
8	技术控制	
8.1	用户终端设备	控制： 应保护用户终端设备所存储或处理的，或通过其访问的网络空间信息
		网络空间特定控制： －应保护存储在端点设备（例如物联网设备、USB 设备、BYOD 等）上、由端点设备处理和可通过端点设备访问的信息。应适当控制在安全区域携带和使用端点设备 －应制定并实施端点设备管理的安全策略。该策略应包括设备防火墙的管理、特定于电子邮件的过滤工具、互联网安全和过滤、移动设备管理和安全工具、加密和入侵检测工具等 －对端点的保护，应立即采取行动阻止攻击者并限制进一步的损害 －组织应在端点部署技术手段，也被称为端点检测和响应（EDR）技术，以检测来自未知来源和不良行为者的不良流量，并做出响应 －组织应具有一种机制，以确保始终适用于最终用户系统和设备的所有组织安全策略，该技术应确保最终用户无法禁用和绕过安装在其端点上的安全功能 －组织应部署技术，确保能够跟踪该设备，在设备发生任何丢失和损坏的情况下，最迟于数据被不良行为者窃取之前，他们应能够远程擦除设备的内容
8.2	特许访问权	控制： 应限制和管理特许访问权限的分配和使用
8.3	网络空间信息访问限制	控制： 应按已建立的访问控制特定主题策略，限制对网络空间信息及其他相关资产的访问
8.4	源代码的访问	控制： 应对源代码、开发工具和软件库的读写访问进行适当的管理
8.5	安全鉴别	控制： 应规定安全访问限制和访问控制的特定主题策略实施安全的鉴别技术和规程
8.6	容量管理	控制： 应根据当前和预期的容量需求，监视和调整资源的使用
8.7	恶意软件防	控制：

	范	应实施恶意软件防范，并通过适当的用户意识教育予以支持
		网络空间特定控制： －为了能够检测新的恶意代码，确保扫描软件始终保持最新，应每日更新扫描软件 －某些流行的操作系统具有嵌入式功能，可以抵御常见的恶意软件，但仍应为高风险环境补充反恶意软件技术 －应实施预防、检测、纠正和恢复措施，以防止恶意软件，并结合适当的用户教育和意识 －组织应考虑以下措施： •在通往互联网的网关上使用反恶意软件，用于扫描进出互联网的所有流量，包括授权使用的网络协议 • 在客户端系统上使用反恶意软件，尤其是员工用于互联网访问的系统 •扫描文件、电子邮件、即时消息附件、网页和外部链接上使用反恶意软件，查找病毒、勒索软件、木马和其他形式的恶意软件 •阻止可疑弹出窗口、网络广告、已知和疑似恶意网站，阻止列表用于未经授权的服务，例如聊天频道、网络邮件服务等 • 让用户意识到，通过外部链接与外部方接触时，恶意软件的风险相当大 •验证与恶意软件相关的准确信息是否合格且信誉良好的来源（例如可靠的互联网网站、反恶意软件供应商等） • 对允许向互联网传输数据的所有服务进行日志记录和监控 • 限制使用能够传输大量数据的未经授权的服务 • 实现非授权协议的过滤器，例如对等网络协议 •在基于脆弱性、关键性的时间框架内修补已知系统脆弱性，重点关注接收互联网流量的所有系统 • 配置通过互联网访问的系统和应用程序，以禁用不必要的功能（例如宏） •准备适宜的恶意软件攻击中恢复计划，包括所有必要的数据和软件备份（包括在线和离线备份等）以及恢复安排
8.8	技术脆弱性管理	控制： 应获取有关使用中的网络空间信息系统的技术脆弱性的网络空间信息，评价组织暴露于此类脆弱性的风险，并采取适当措施
		网络空间特定控制： －应及时获得有关正在使用的信息和通信技术系统脆弱性的信息 －应对组织暴露于该脆弱性的情况进行评估，并采取适当措施应对相关风险 －应建立、记录、实施配置，包括硬件、msoftware、服务和网络等安全配置，并进行监控和审查 －提供技术产品（防火墙、IDS、IPS 等）和服务（网络服务、VoIP 服务、托管安全服务等）的组织应统一、持续、有效地实施措施，以识别、处理和披露其提供的产品和服务的脆弱性 －根据产品和服务供应商披露的脆弱性，采取适当的保护措施来解决脆弱性 －确保检测到的任何新恶意软件、间谍软件都可以被有效删除、禁用 －应与安全供应商建立联系，并向供应商提交相关报告和恶意软件样本以供后续行动，特别是在病毒流行似乎激增的情况下 －组织都有一个电子邮件列表，用于接收该报告和样本进行分析和跟进 －组织应定义并实施严格的策略，规定用户可安装的软件 －当软件补丁可以帮助消除和减少安全脆弱性时，应该应用之。 －供应商提供的用于互联网操作系统的软件应保持其支持和服务的水平

		—组织应考虑在操作系统中使用的依赖无服务支持的软件（包括开源软件）的风险 —操作系统中使用的开源软件应保持到软件的最新适当版本 —针对脆弱性的其他应对措施包括： • 改变操作实践 • 重新配置技术系统 • 通过管理互联网接入来避免风险 • 培训工作人员和用户 • 采用纵深防御措施，即当一种控制失败时，有另一种独立的方法继续防御 • 系统安全测试，安全 SDLC 和补丁测试，部署前更新
8.9	配置管理	控制： 应建立、记录、实施、监视和评审硬件、软件、服务和网络的配置，包括安全配置
8.10	网络空间信息删除	控制： 当不再需要时，应删除存储在网络空间信息系统、设备或任何其他存储媒体中的网络空间信息
8.11	数据脱敏	控制： 应根据组织关于访问控制的特定主题策略和其他相关的特定主题策略以及业务要求使用数据脱敏，并考虑到适用的法律法规
8.12	数据防泄露	控制： 数据防泄露措施应用于处理、存储或传输敏感网络空间信息的系统、网络和任何其他设备
8.13	网络空间信息备份	控制： 网络空间信息、软件和系统的备份副本应按商定的备份特定主题策略进行维护和定期测试
8.14	网络空间信息处理设施的冗余	控制： 网络空间信息处理设施应具有足够的冗余以满足可用性要求
8.15	日志	控制： 应生成、存储、保护和分析用于记录活动、异常、故障及其他相关事态的日志
		网络空间特定控制： —应生成、保护、保存和分析记录活动、异常、故障和其他相关事件的日志 —日志应受到保护，并保存在安全的位置，以便进行日志分析和审核 —某些国家、地区的法规要求将日志存储一定时限
8.16	监视活动	控制： 应监视网络、系统和应用程序，以发现异常行为，并采取适当措施评价潜在的网络空间信息安全事件
		网络空间特定控制： 应监测面向互联网的网络、系统和应用程序的异常行为，并采取适当行动评估潜在的信息安全事件
8.17	时钟同步	控制： 组织使用的网络空间信息处理系统的时钟应与批准的时间源同步
8.18	特权实用程序的使用	控制： 应限制并严格控制可能超越系统和应用程序控制的实用程序的使用
		网络空间特定控制：
8.19	运行系统软件的安装	控制： 应实施规程和措施以安全地管理运行系统上的软件安装

8.20	网络安全	控制： 应保护、管理和控制网络和网络设备以保护系统和应用程序中的网络空间信息
		网络空间特定控制： －应实施控制措施，以确保连接到互联网的信息的安全，并保护连接的服务免受未经授权的访问 －应建立控制措施，以保护通过互联网传递的数据的机密性和完整性，并保护连接的系统和应用程序 －可以连接到互联网的系统应受到限制，如可能，应进行用户身份验证 －与组织的互联网基础设施相关的网络设备、系统的记录和监控应用于记录和检测可能影响和与互联网安全相关的行为 －网络安全措施应考虑以下因素： • 确保组织的网络和互联网之间有一个受监控的可靠接口，确保所有实体的访问控制，而不单是授权人员 • 在授予对内部基础设施的访问权限前，还应控制信息和应用程序 • 监测和分析内部流量，以发现和阻止非法活动。 • 确保互联网及其服务的访问和使用（包括与物理设施外工作的人员的通信等）得到保护 • 基于网络的 IDS 和 IPS 技术应与人工智能、机器学习一起部署，以应对最新、高层级的互联网攻击，包括具有已知特征模式和行为的攻击 •根据其网络设置，组织可以考虑内置各种网络安全模块的网络设备，例如防火墙、IPS、DL Band 等，以防止针对 DNS 的攻击
8.21	网络服务的安全	控制： 应识别、实施和监视网络服务的安全机制、服务级别和服务要求
		网络空间特定控制： 应制定关于使用互联网和通过互联网访问服务的规则，至少包括： －用户可访问的互联网上的网络服务以及该服务的授权过程 －确定网络管理、技术控制和程序，以保护通过互联网访问互联网连接和网络服务 －用于通过互联网访问互联网和服务的手段（例如 HTTPS、VPN 等） －监控通过互联网访问的服务（例如带宽监控、SIEM 等）
8.22	网络隔离	控制： 应在组织的网络中隔离网络空间信息服务组、用户组和网络空间信息系统组
		网络空间特定控制： －组织应考虑通过将连接到互联网的系统与其他组织网络（例如专用网络和 DMZ 等）隔离，以管理系统的安全性 －该隔离网络的边界应明确定义，并应使用网关（例如防火墙、过滤路由器等）进行控制 －通过创建具有足够访问控制的竖井或集群隔离，构建内部网络，将主要关键的资产与通用资产隔离开来，确保子网络具有过滤路由器和嵌入式子网络，以避免直接通往关键资产 －组织应该考虑能够更优的应对基于互联网的攻击的防火墙技术；该设备的目的是提供保护，以防止来自互联网的威胁，并防止专有信息不受控制地传输到互联网 －路由器技术可以部署内置功能和附加模块，以增强网络安全，并可以解决 DoS 和 DDoS 攻击等网络风险
8.23	网页过滤	控制： 应管理对外部网站的访问，以减少对恶意内容的暴露

8.24	密码技术的使用	控制： 应定义并实施有效使用密码技术的规则，包括密钥管理
		网络空间特定控制： －应使用密码学来保护通过互联网传输的信息的机密性、真实性和完整性 －VPN 和 HTTPS（超文本传输协议安全）应使用加密技术进行安全连接 －加密算法、密钥长度和操作实践应根据最佳实践进行选择 －适当的密钥管理需要生成、存储、归档、检索、分发、报废和销毁加密密钥等的安全过程 －应保护所有加密密钥不被修改和丢失 －密钥和私钥需要防止未经授权的使用以及泄露 －用于生成、存储和归档密钥的设备应在相关情况下进行物理保护 －在使用加密技术时，考虑不同的法规和国家地区限制可能要求不同加密技术的使用，和导致加密信息的跨境流动问题
8.25	安全开发生存周期	控制： 应建立并应用软件和系统安全开发规则
		网络空间特定控制：
8.26	应用程序安全要求	控制： 在开发或获取应用程序时，应识别、规定和批准网络空间信息安全要求
		网络空间特定控制： －应分析新技术的安全风险，并根据已知的攻击模式对设计进行评审 －在设计系统时应考虑嵌入安全性 －还应定期审查该系统，以确保它们在应对任何新的潜在威胁方面保持最新，并适用于正在应用的技术和解决方案的进步 －面向互联网的应用程序及其代码应是从安全角度设计的，即它总是会受到攻击，无论是错误还是恶意事件。 －组织应制定安全和适当使用互联网资源的规则，包括对不受欢迎和不适当的网站、基于网络的应用程序的任何限制，并相应地通知其工作人员，并规则应该保持最新版本 －对于通过互联网处理交易的应用程序，应考虑以下内容： • 维护交易细节的机密性和完整性所需的保护级别要求 • 通过具有适当安全控制（例如加密传输路径、数字证书等）的互联网传输交易细节 •将交易详细信息存储在任何可公开访问的环境之外，并确保存储介质不能从互联网直接访问 •抵御攻击的弹性要求，包括保护相关应用服务器和确保提供服务所需的网络互连可用性的要求 •如果需要高度依赖软件产品的安全性，则应根据标准中所述的通用标准方案对产品进行独立验证。
8.27	系统安全架构和工程原则	控制： 应建立、文件化、维护系统安全工程的原则，并将其应用于所有的网络空间信息系统开发活动
		网络空间特定控制： －组织应采用安全工程原则，包括实施安全的开发生命周期，以识别和减轻正在开发的产品和解决方案中的风险 －应考虑威胁建模、用户身份验证技术、供应链组件、安全会话控制和数据验证、消毒和面向安全的设计审查等，以帮助识别面向互联网的系统上的安全脆弱性
8.28	安全编码	控制：

		应于软件开发中应用安全编码原则
		网络空间特定控制： －应遵循安全编码标准来设计和开发应用程序 －如果应用程序所有者可以通过直接远程访问服务器来访问脚本应配置 Web 服务器以防止目录浏览；OWASP 指南可作为安全应用程序设计和测试的有益参考 －组织应记录代码行为，并评估该行为是否属于间谍软件和欺骗性软件的潜在领域 －组织应使用合格的评估员来评估代码是否符合反间谍软件供应商遵守最佳实践的客观标准，以确保组织为最终用户提供的软件工具不会被反间谍软件供应商标记为间谍软件 －组织应为其二进制文件实施数字代码签名，以便反恶意软件和反间谍软件供应商能够轻松确定文件的所有者 －ISV 使用包括数字代码签名在内的最佳实践一致生产的软件可以被归类为可能是安全的 －如果组织发现有助于减少间谍软件和恶意软件问题的有用软件技术，组织应考虑与供应商合作，使其广泛可用
8.29	开发和验收中的安全测试	控制： 应在开发生存周期中定义和实施安全测试过程
		网络空间特定控制： －在暴露于互联网之前，安全测试应该是系统和组件测试的一个组成部分 －组织应利用自动化工具，如代码分析工具和脆弱性扫描仪，并应在使系统在互联网上运行之前验证安全相关缺陷的补救措施 －安全测试应包括以下测试： • 安全功能，例如用户身份验证、访问限制、API 的安全使用和密码的使用等 • 包括操作系统、防火墙和其他安全组件的安全配置
8.30	开发外包	控制： 组织应指导、监视和评审系统开发外包相关的活动
8.31	开发、测试和生产环境的隔离	控制： 应隔离并保护开发、测试和生产环境
8.32	变更管理	控制： 网络空间信息处理设施和网络空间信息系统的变更应遵循变更管理规程
		网络空间特定控制： －应制定变更管理策略和流程，以确保组织更容易对信息基础架构进行变更，管理信息系统和应用程序的变更，从而防止计划外的中断、数据损坏和丢失 －组织的变更管理流程应涵盖与互联网上托管系统的互联网安全相关的变更。该流程有助于组织请求、确定优先级、授权、批准、安排和实施任何更改 －变更管理策略包括关于系统管理员的责任和义务、导入软件和文件、访问控制等的声明 －应对网络组件和结构的所有更改（修改、移动、移除和添加等）进行管理，以保持架构和基础设施设计图的最新状态
8.33	测试网络空间信息	控制： 应适当地选择、保护和管理测试网络空间信息
8.34	在审计测试中保护网络	控制： 应对涉及运行系统评估的审计测试和其他保障活动进行规划，并在测试人员和适合的管

	空间信息系统	理人员之间达成一致