ICS 00.000
X XX

CIIPA

团　　体　　标　　准

T/CIIPA 00004-2024

关键信息基础设施安全防护能力要求与评价

Requirements and Evaluation of Security Protection Capabilities for Critical Information Infrastructure

（征求意见）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中关村华安关键信息基础设施安全保护联盟　　发布

目　　次

前　言

本文件按照《中关村华安关键信息基础设施安全保护联盟标准管理办法（暂行）》的要求，依据 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。

本文件由中关村华安关键信息基础设施安全保护联盟提出。

本文件由中关村华安关键信息基础设施安全保护联盟网络安全标准专业委员会归口和解释。

本文件起草单位：中关村华安关键信息基础设施安全保护联盟、中广核数字科技有限公司、工业和信息化部教育与考试中心、国家工业信息安全发展研究中心、工业和信息化部电子第五研究所、中国信息通信研究院、中国电力科学研究院有限公司、北京国信城研科学技术研究院、中国信息安全测评中心、中国交通通信信息中心、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）、中国软件评测中心、中国人民财产保险股份有限公司、华为技术有限公司、天津恒御科技有限公司、广州市盛通建设工程质量检测有限公司、上海矢安科技有限公司、北京同创安全可信科技有限公司、深圳市魔方安全科技有限公司、北方实验室(沈阳)股份有限公司、浙江安远检测技术有限公司、国家基础地理信息中心、内蒙古鹏摇科技有限公司、南方电网数字电网集团信息通信科技有限公司、中检集团天帷网络安全技术（合肥）有限公司、北京君航伟业科技发展有限公司。

本文件主要起草人：刘元、李红霞、黄启清、权小康、谭志彬、蒋琳、王诗蕊、才镓赫、刘烨、孙智权、李汪蔚、赵相楠、肖红阳、赵宝春、张少昌、游顺、伊胜伟、王庆、杜渐、贺林佳、刘琛、高媛、李安伦、李强、张博、刘云、李翔、修凤洲、徐彬、伍阳军、任政杰、周亚、于齐齐、孙瑜、王振宇、黄国忠、陈达鑫、张健楠、刘兴华、郑俊杰、汪涛、李恒、李漠颖。

本文件首次发布。

本文件在执行过程中的意见或建议反馈至中关村华安关键信息基础设施安全保护联盟（地址：北京市海淀区板井路 69 号世纪金源商务中心 607，100097，网址：https://www.cnciipa.com，邮箱：guanbaolianmeng@cnciipa.com）。

引　言

在关键信息基础设施安全保护工作中，安全防护是核心环节和工作。随着网络与信息建设的迅猛推进及新技术的广泛应用，网络结构和业务系统变得复杂多变，相互依赖加深，使得安全防护挑战加剧。网络攻击呈现出政治化、军事化、致命化及精准化的新趋势，高级攻击如入侵控制、窃密、摧毁等，对关键信息基础设施构成重大威胁。我国在此领域面临体系化不足、碎片化及同质化严重等问题，单纯依赖安全功能的简单叠加或碎片化建设，已无法满足关键信息基础设施的有效保护需求。

按照《网络安全法》《关键信息基础设施安全保护条例》等法律法规要求，参照《关键信息基础设施安全保护要求》等国家标准要求，在开展网络安全等级保护工作基础上，加强管理能力体系、技术能力体系、运营能力体系和保障能力体系建设，强化落实安全防护重点措施，构建关键信息基础设施综合防御体系，提升关键信息基础设施的安全保护能力。

本文件以网络安全新质战斗力为引领，以关键信息基础设施分析识别、安全防护、检测评估、监测预警、技术对抗（主动防御）、事件处置、数据安全、供应链安全八大能力为主线，深入剖析包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全策略管理、安全运营管理、安全监督管理、安全通信网络、安全区域边界、安全计算环境、新技术新应用领域安全扩展防护、大数据、人工智能等多个层面，设定严格的标准与要求，提出评价方法论和关键要素，旨在指导重点行业及相关单位科学有效地实施安全管理措施和技术防护手段，掌握客观评价安全保护能力水平的方式方法，共同推动安全防护工作的有序进行，保障关键信息基础设施的安全稳定运行。

关键信息基础设施安全防护能力要求与评价

1 范围

本文件确立了关键信息基础设施安全防护总体要求、框架、能力及评价模型，规定了开展关键信息基础设施安全防护工作应具备的能力要求，给出了对安全防护能力水平的评价方法。

本文件适用于指导关键信息基础设施运营者对关键信息基础设施开展安全防护能力建设，以及关键信息基础设施安全保护相关责任方对安全防护能力进行评价，也可适用于保护工作部门和关键信息基础设施安全保护的其他参与者参考，并可供网络安全服务机构在制定安全防护解决方案时参考。

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/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 20984-2022 信息安全技术 信息安全风险评估方法

GB/T 43697-2024 数据安全技术 数据分类分级规则

GB/T 35295-2017 信息技术 大数据 术语

GB/T 42570-2023 信息安全技术 区块链技术安全框架

GB/T 41867-2022 信息技术 人工智能术语

GA/T 2182-2024 关键信息基础设施安全测评要求

3 术语和定义

GB/T 39204-2022、GB/T 22239-2019、GB/T 41867-2022、GB/T 35295-2017 界定的以及下列术语和定义适用于本文件。

3.1

关键信息基础设施 critical information infrastructure

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、丧失功能或者数据泄露，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。

[GB/T 39204-2022，定义 3.1]

3.2

供应链 supply chain

将多个资源和过程联系在一起，并根据服务协议或其他采购协议建立连续供应关系的组织系列。

注：其中每一组织充当需方、供方或双重角色。

[GB/T 39204-2022，定义 3.2]

3.3

关键业务链 critical business chain

组织的一个或多个相互关联的业务构成的关键业务流程。

[GB/T 39204-2022，定义 3.3]

3.4

云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池,并按需自助获取和管理资源的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 22239-2019，定义 3.3]

3.5

区块链 blockchain

将区块顺序相连，并通过共识协议、数字签名、杂凑函数等密码学方式保证的抗篡改和不可伪造的分布式账本。

[GB/T 42570-2023，定义 3.2]

3.6

物联网 internet of things

将感知节点设备通过互联网等网络连接起来构成的系统。

[GB/T 22239-2019，定义 3.15]

3.7

移动互联 mobile communication

采用无线通信技术将移动终端接入有线网络的过程。

[GB/T 22239-2019，定义 3.9]

3.8

大数据 big data

具有体量巨大、来源多样、生成极快、且多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

[GB/T 35295-2017，定义 2.1.1]

3.9

人工智能 artificial intelligence；AI

〈学科>人工智能系统相关机制和应用的研究和开发。

[GB/T 41867-2022，定义 3.1.2]

3.10

人工智能系统 artificial intelligence system

针对人类定义的给定目标，产生诸如内容、预测、推荐或决策等输出的一类工程系统。

注 1：该工程系统使用人工智能相关的多种技术和方法，开发表征数据、知识、过程等的模型，用于执行任务。

注 2：人工智能系统具备不同的自动化级别。

[GB/T 41867-2022，定义 3.1.8]

3.11

工业控制系统 industrial control system

工业控制系统（ICS）是一个通用术语，它包括多种工业生产中使用的控制系统，包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）和其他较小的控制系统，如可编程逻辑控制器（PLC），现已广泛应用在工业部门和关键基础设施中。

[GB/T 22239-2019，定义 3.18]

3.12

网络安全新质战斗力 new quality cybersecurity combat effectiveness

以新质生产力理念，结合网络安全领域的实际情况和发展需求，将新质生产力落实为网络安全新质战斗力。网络安全新质战斗力是以创新为主导，先进技术和大数据为支撑，网络安全机制改革为途

径，高效能和高质量为目标，摆脱传统增长模式和战斗力提升路径，形成符合新发展理念的新型网络安全运行模式和优质先进战斗力质态。

3.13

网络安全防护能力 cybersecurity defense capability

根据识别的关键业务、资产、安全风险，在安全管理制度、安全管理机构、安全管理人员、安全通信网络、安全计算环境、安全建设管理、安全运营管理等方面实施安全管理和技术保护措施，确保关键信息基础设施的运行安全。

3.14

管理能力体系 management capability system

管理能力体系是对制度、机构、人员、建设、策略、运营、监督等多个方面提出管理要求，构建高效、协同、可持续的安全管理体系。

3.15

技术能力体系 technology capability system

技术能力体系是对安全防护、数据安全、供应链安全、新技术新应用安全等多个方面提出技术要求，构建有效、稳定、可信赖的安全技术体系。

3.16

运营能力体系 operation capability system

运营能力体系是对分析识别、检测评估、监测预警、技术对抗、事件处置等多个方面提出运营要求，构建协同、动态、持续、全面的安全运营体系。

3.17

保障能力体系 support capability system

保障能力体系是对组织、人才队伍、经费、跨组织等多个方面提出保障要求，构建强效、可靠、稳定的安全支撑体系。

4 缩略语

下列缩略语适用于本文件。

CII：关键信息基础设施（Critical Information Infrastructure）

DDoS：拒绝服务（Distributed Denial of Service）

DHCPv6：动态主机配置协议第六版（Dynamic Host Configuration Protocol version 6）

ICMPv6：互联网控制消息协议第六版（Internet Control Message Protocol version 6）

XDR：可拓展威胁检测与响应（Extended Detection and Response）

SIEM：安全信息和事件管理(Security Information and Event Management)

TLS/SSL：传输层安全性协议/安全套接层协议（Transport Layer Security/Secure Sockets Layer）

5 CII 安全保护总体要求

CII 运营者应落实网络安全等级保护制度、关键信息基础设施安全保护制度以及数据安全保护制度，按照《信息安全技术 网络安全等级保护基本要求》《信息安全技术 关键信息基础设施安全保护要求》《信息安全技术 信息系统密码应用基本要求》等标准要求，构建 CII 管理、技术、运营和保障四大安全保护体系，提升分析识别、安全防护、检测评估、监测预警、技术对抗、事件处置、数据安全、供应链安全八大能力。突出保护重点，采取加强举措，守住关键，保住要害，实现以关键业务和重要数据为核心的整体防控、以风险管理和隐患防范为导向的动态防护、以信息共享和业务联动为基础的协同联防、以智能聚合和实战弈升为特征的智能运营，切实保障 CII 持续、稳定运行。

5.1 以网络安全新质战斗力引领 CII 安全保护

按照“人工智能技术+大数据+专业力量专业能力+新型运行机制”四位一体、四轮驱动的网络安全新质战斗力核心理念，从生产力与生产关系的内在本质关系出发，通过改革创新，全面提升网络安全理论、技术、专业、装备、实战的能力和水平，以 CII 网络安全新质战斗力为引领，实现 CII 网络安全业务和能力提档升级。

5.2 在落实网络安全等级保护制度基础上，加强 CII 安全保护

开展 CII 的定级、备案、等级测评、建设整改和监督检查工作。根据《信息安全技术 网络安全等级保护定级指南》拟定 CII 的安全保护等级，按照有关政策要求向公安机关备案；选择等级测评机构，依据《信息安全技术 网络安全等级保护测评要求》等有关标准规范，对 CII 开展检测评估；按照国家有关法律、政策以及《信息安全技术 网络安全等级保护基本要求》《信息安全技术 网络安全等级保护安全设计技术要求》等国家标准，开展安全建设整改。

CII 网络安全等级保护测评结果应达到主管部门要求。

5.3 以 CII 安全保护能力为主线，建立 CII 综合防御体系

以提升分析识别、安全防护、检测评估、监测预警、技术对抗、事件处置、数据安全、供应链安全八大能力为主线，提出以下重点要求：

（一）加强组织领导。建立 CII 安全保护领导体系和工作体系，组织制定网络安全保护计划和年度规划。

（二）重要制度结合落实。将网络安全等级保护制度、关键信息基础设施保护制度、数据安全保护制度、个人信息保护制度有机结合，确保在分析识别、安全防护、检测评估、监测预警、技术对抗、事件处置、数据安全、供应链安全等方面协调统一。

（三）建立并落实责任制。建立 CII 安全责任制和问责制度，确保国家有关法律法规、政策文件、标准要求落实到位。

（四）识别认定 CII。保护工作部门结合本行业、本领域实际，制定 CII 认定规则，根据认定规则负责组织认定本行业、本领域的 CII，及时将认定结果通知运营者，并通报国务院公安部门。

（五）分析识别资产和风险威胁。围绕 CII 承载的关键业务，开展业务依赖性识别、关键资产识别、风险识别活动，为开展安全保护奠定基础。

（六）采取加强型保护。根据已识别的关键业务、资产、安全风险，在开展等级保护基础上，从安全管理制度、机构、人员、通信网络、区域边界、计算环境、建设管理、运营管理、供应链安全、数据安全等方面，采取加强型和特殊型保护。

（七）安全检测评估。开展以等级保护测评、数据安全检测评估、商用密码应用安全性评估为基础，CII 测评为重点的检测评估工作，检验保护措施的有效性，并针对发现的安全隐患和外部风险威胁，制定切实可行的建设整改方案并进行整改。

（八）落实“三化六防”要求。落实“实战化、体系化、常态化”和 “动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施，建立网络安全综合防御体系。

（九）开展监测预警。落实实时监测措施，健全完善网络安全监测预警机制、信息通报机制和信息共享机制，强化预知预判、预警预防，提升发现攻击能力和监测预警能力。

（十）事件处置。建立重大事件和威胁报告制度，落实重大事件处置措施，制定应急预案并演练，落实协同联动措施，提升事件处置能力。

（十一）技术对抗。科学设计网络架构，对网络应用进行集约化建设。以监测发现为基础，采取收敛暴露面、捕获、溯源、干扰和阻断等技术应对措施；开展演习和威胁情报工作，落实识别分析网络威胁与攻击行为的措施，提升技术对抗能力。

（十二）挂图作战。建设网络安全监控指挥中心和 CII 安全保护平台，实施“挂图作战”，提升整体实战能力。

（十三）供应链安全。在网络的规划设计、建设、运营、产品、服务等各环节中，加强对服务商和产品供应商的安全管理，落实供应链安全管控措施，提升防范化解供应链风险能力。

（十四）技术创新。按照“理论支撑技术、技术支撑实战”理念，在网络空间地理学理论指导下，突破网络空间资产测绘、可视化表达、图谱构建、行为认知等核心技术，支撑综合防御体系建设和“挂图作战”。

（十五）数据安全建章立制。建立重要数据安全管理制度，包括数据安全检测评估、安全审查、出境安全评估、风险监测、通报预警、应急处置、事件调查等机制，以及数据流转、交易、出境等管理制度。

（十六）数据安全审查认证。根据数据安全法律法规、政策和数据安全审查制度要求，数据处理者应建立数据审查和认证制度，对数据及其相关安全管理负责人、关键岗位人员以及数据处理活动全流程开展审查，保障重要数据安全关键岗位人员可信、可靠，数据处理活动合规有序；配合相关部门开展数据安全审查工作。

（十七）强化数据安全责任制落实。建立完善数据安全责任制和问责制度，明确行业主管部门、监管部门、数据处理者、服务提供者的四方责任，确保国家有关法律法规、政策文件、标准要求落实到位。

（十八）重要数据容灾备份。按照业务连续性管理需求，建立重要数据和数据库容灾备份机制，重要数据和数据库采取异地备份措施。业务安全性要求高的可采取数据异地实时备份，业务连续性要求高的可采取重要系统异地备份。

（十九）数据应用安全。推动各类网络联通、数据大流动，发挥数据应用价值。一是优化政策，原则上任何网络都可以采用隔离装置联通；二是确定好数据传输规则，采取量子技术、密码技术、IPv6 等核心技术，确保数据传输安全；三是采取多方计算、区块链、人工智能等新技术，对不能外发的数据，采取建桥、建模、加密传输等新理念新措施，确保数据安全应用。

（二十）网络安全建设和运营。加强数字化生态网络安全管理、网络安全技术、网络安全运营和网络安全保障等四个体系建设，提高网络与数据安全日常管理能力和水平。

（二十一）恶意代码分析。恶意代码是承载攻击的执行体、网络战的武器、网络犯罪的工具，几乎所有的网络攻击行动都依赖恶意代码的投放和执行。因此，网络运营者应掌握恶意代码分析技术和方法，深入理解和揭示恶意软件的行为和特性，快速识别和处理网络攻击。

（二十二）漏洞挖掘与渗透测试。深入研究漏洞挖掘和渗透测试技术，掌握网络攻击的方法和手段，更好地开展网络安全防御，以攻促防。

（二十三）商用密码应用。密码是构建网络信任体系的基石，是保障网络空间安全的核心技术。深入研究密码算法、密码协议、密码工程技术、密码标准和产品，开发和应用自主、安全的密码，为保护网络安全、数据安全提供重要支撑。

（二十四）人工智能技术赋能网络安全。人工智能不仅推动了网络空间智能化进程，催生自动驾驶、智能无人机等新业态新产品，还应赋能网络安全。在保障人工智能算法模型安全、训练数据安全、平台安全、应用安全基础上，研发应用于网络安全各业务的大模型，并将人工智能技术有效应用于攻防两端，使攻防格局和态势发生革命性变化。

（二十五）威胁情报。建立社会化的网络安全威胁情报支撑体系，企业和研究机构等应加大力度，基于大数据，利用大数据分析挖掘技术、人工智能技术等，开展威胁信息搜集、分析、挖掘等工作，提升威胁情报能力。

（二十六）综合保障。加强机构、编制、人员、经费、科研、工程建设等各项保障，实施自主可控和创新工程，加强教育训练和人才培养，提升综合保障能力。

（二十七）实施信息技术应用创新。CII 要按照国家总体要求，将基础软硬件产品、数据库、终端、业务系统和工业控制系统的核心产品等实施信息技术应用创新替代。

（二十八）严密防范勒索攻击。加强行为监测、勒索诱捕、系统防护、进程防护、数据保护、备份恢复六个主要环节的安全防护，利用云防护、设置蜜罐等技术措施防范勒索攻击。

（二十九）网络安全保险。在网络与数据安全领域引入保险机制，提高风险治理能力。加强顶层设计，研究网络与数据安全保险法律、政策、标准规范，共同培育市场，试点先行，支持保险机构构建“保险+风险管控+服务”模式。

（三十）加强新技术新应用的安全管控。在 CII 建设中，大量应用云计算、大数据分析、移动互联、物联网、工业控制、5G、区块链、IPv6、人工智能等新技术，应建设针对性的安全保护能力，确保新技术新应用在 CII 中得到充分保护。

6 安全防护能力评价

6.1 能力模型

CII 安全防护能力体系主要包括管理能力体系、技术能力体系、运营能力体系和保障能力体系四个方面。CII 安全防护能力体系模型见图 1，CII 安全防护能力评价模型见图 2。

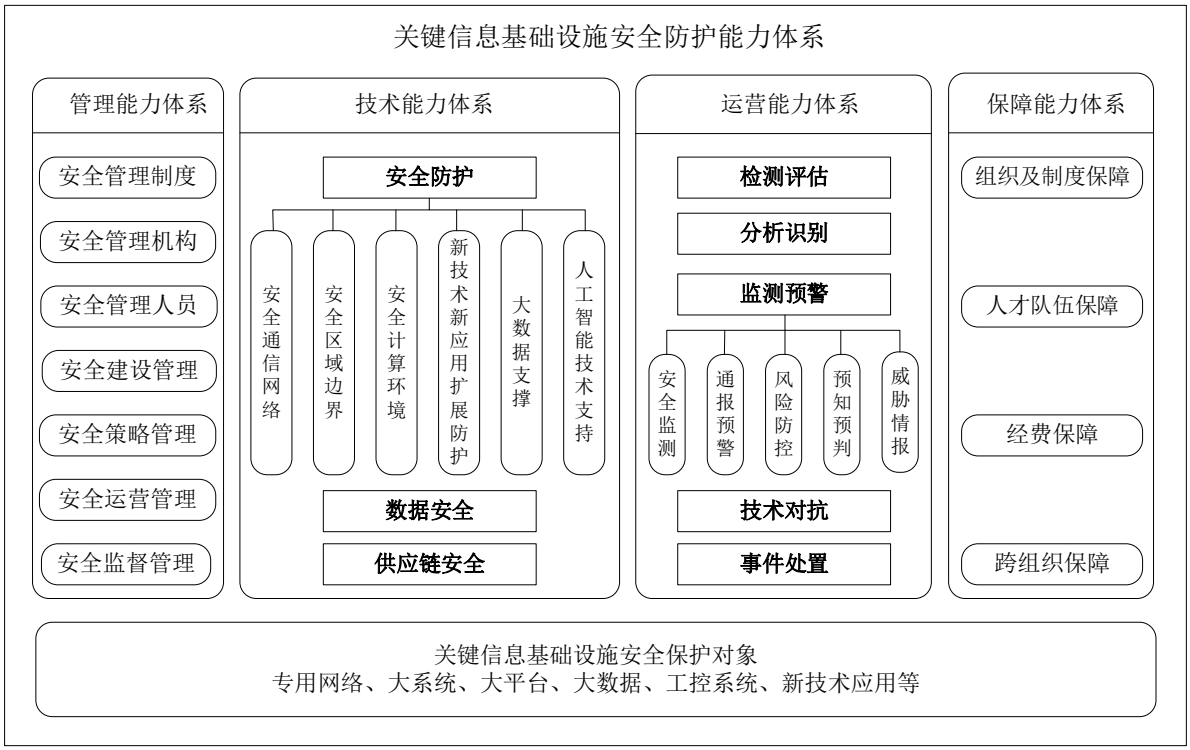

图 1 CII 安全防护能力体系模型

图 2 CII 安全防护能力评价体系模型

a） 管理能力体系包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全策略管理、安全运营管理、安全监督管理七个能力项。

b） 技术能力体系包括安全防护、数据安全及供应链安全三个能力项，其中安全防护细分为安全通信网络、安全区域边界、安全计算环境、新技术新应用安全扩展防护、大数据支撑及人工智能技术支持六个能力子项。

c） 运营能力体系包括分析识别、检测评估、监测预警、技术对抗、事件处置五个能力项，其中监测预警包括安全监测、通报预警、风险防控、预知预判及威胁情报五个能力子项。

d） 保障能力体系包括组织及制度保障、人才队伍保障、经费保障、跨组织保障四个能力项。

CII 安全防护能力评价为 CII 运营者提供能力评价方法，从管理能力体系、技术能力体系、运营能力体系、保障能力体系四大维度进行全面评价。

6.2 能力评价

6.2.1 能力评价项

运营者安全防护能力评价项分为通用评价项及扩展评价项。

a） 管理能力体系，共计通用评价项 67 项；

b） 技术能力体系，共计通用评价项 57 项，扩展能力项中云平台安全防护 9 项、移动互联安全 5 项、物联网安全 2 项、工业控制系统安全 7 项、5G 网络技术安全 4 项、区块链技术安全 5 项、IPv6 技术安全 4 项、大数据及平台安全 3 项、人工智能安全 8 项；

c） 运营能力体系，共计通用评价项 68 项；

d） 保障能力体系，共计通用评价项 32 项。

CII 安全防护能力评价应至少实施通用评价项，涉及新技术新应用领域的应增加相应扩展部分评价项（例如：采用云计算技术的 CII 增加云计算及平台扩展能力项）。

6.2.2 能力评价要求

a） 评价流程一般包括确定评价目的、制定评价方案、收集评价信息、遴选评价专家、综合分析评价、形成评价结果等基本步骤；

b） 评价形式可采用自评估或第三方单位评估的形式；

c） 评价活动应明确评价报告的格式，至少包含以下内容：参评机构与评价主体的基本信息、评价活动基本情况、评价专家与评价主体的意见、评价专家与评价主体的签字或盖章等；

d） 对于评价结果应明确其作用范围与时效性。

6.3.3 能力评价方法

CII 安全防护能力评价包括单元评价、关联评价和整体评估。

a) 单元评价。单元评价是针对本文中各能力评价项及子项的评价。单元评价是 CII 安全评价工作的基本活动。通过单元评价可以识别出本文提出的要求在单点上已采取的安全措施以及存在的安全问题。单元评价结果可以输出安全问题及已采取的安全措施，作为关联评价及整体评估的基础。

符合率计算：对于同一能力评价项，当所有 CII 对象及组件均为符合或存在个别不适用时，该能力评价项为符合；当所有 CII 对象及组件均为不符合或存在个别不适用时，该能力评价项为不符合；当所有 CII 对象及组件均为不适用时，该能力评价项为不适用，其余情况为部分符合。

对于“可”的能力评价项，在符合率计算时可自行选择是否作为评价项。

总项数=通用评价项+相应领域的扩展能力项。

符合率=单项符合总项数/（总项数-不适用项数）*100%。

b) 关联评价。CII 关联评价应在信息收集的基础上，针对可能的威胁，结合单元评价中发现的漏洞及安全问题，从攻击者视角利用各种攻击技术对 CII 可能遭受的攻击路径进行非破坏性质的攻击性测试。关联评价包括信息收集、入侵痕迹分析、模拟攻击路径设计和渗透测试等过程。通过关联评价可以发现 CII 整体性的安全问题。关联评价需要与 CII 的实际业务及信息化情况相结合，评价人员应根据被测 CII 的实际情况，结合本文件的要求，多角度多层面实施关联评价（具体评价方法参考 GA/T 2182-2024）。

针对等级测评和关联评价发现的安全问题，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对 CII 造成影响的程度，并综合评价这些安全问题对 CII 所承载关键业务及国家安全造成的安全风险。关联评价的结果可分为高风险、中风险、低风险三档。其中高风险判定可参考附录 A。

c) 整体评估。CII 安全防护能力评价主要由单项符合率结合高风险项进行判定。具体判定依据如表 1 所示。

表 1 安全保护能力评价表

评价结论	判定依据
优	被评价 CII 符合率≥90%，且无高风险判定。
良	被评价 CII 符合率≥75%且＜90%；或者符合率≥90%且存在高风险判定。
中	被评价 CII 符合率≥60%且＜75%。
差	被评价 CII 符合率＜60%。

7 管理能力体系

7.1 安全管理制度

7.1.1 建立 CII 网络安全保护计划

a) 应制定适合本组织的网络安全保护计划，明确 CII 安全保护工作的目标，从管理体系、技术体系、运营体系、保障体系等方面进行规划，加强机构、人员、经费、装备等资源保障，支撑 CII 安全保护工作；

b) 应在网络安全保护计划中明确本组织需建立的CII安全管理制度，包括安全管理机构和核心岗位人员管理制度、安全责任制和责任追究制度、安全保护制度、数据安全管理制度和供应链安全管理制度等；

c) 网络安全保护计划应形成文档并经审批后发送至相关人员。网络安全保护计划应每年至少修订一次，或发生重大变化时进行修订。

7.1.2 建立安全管理机构和关键岗位人员管理制度

a) 应建立 CII 网络安全管理机制，设立网络安全管理机构，明确网络安全管理机构在安全管理、应急演练、事件处置、教育培训和评价考核等日常工作中承担的责任；

b) 应建立CII人员管理机制，明确人员岗位要求、录用流程、工作要求等；应对关键岗位人员进行严格的背景审查；关键岗位人员应参与CII有关的项目立项、方案设计、方案评审和项目验收等环节的工作；

c) 应建立CII关键岗位人员授权管理机制，按照最小授权原则开展岗位权限分级管理，并定期进行权限审核和调整。

7.1.3 建立CII安全责任制和责任追究制度

a) 应建立CII安全责任机制，明确网络安全工作委员会或领导小组、网络安全管理机构的责任要求，建立CII保护责任清单，将CII安全保护工作细化并分解到具体的岗位和人员；应定期更新责任清单，以适应安全形势变化和岗位职责调整，确保安全保护工作持续高效开展；

b) 应建立CII安全责任追究机制，建立健全考核机制，明确考核内容、方法，明确违规情形和责任追究事项，确定问责范围，明确相应处罚措施；

c) 应建立数据安全责任制和问责机制，确保国家有关法律法规、政策文件、标准要求落实到位；

d) 应建立关键岗位考核机制，明确奖励和惩处措施。针对不同关键岗位分别设置不同类型的考核指标；

e) 应定期进行网络安全考核，并将考核结果纳入组织绩效考核体系。

7.1.4 建立CII安全保护制度

a) 应建立CII分析识别机制，系统化管理CII的资产、业务及风险，建立资产识别规范、业务识别准则、风险管理机制；

b) 应建立 CII 安全防护机制，包括安全防护三同步制度、安全控制策略与实施机制，提升 CII 网络安全防护能力，保障 CII 安全运行；

c) 应建立 CII 检测评估机制，确定检测评估流程、方式方法、周期、人员组织、资金保障等，开展安全检测与风险隐患评估，分析潜在安全风险可能引发的安全事件；

d) 应建立 CII 监测预警和信息通报机制，确定网络安全预警分级准则，明确监测策略、监测内容和预警流程，对 CII 的安全风险进行监测预警，针对发生的网络安全事件或发现的网络安全威胁，提前或及时发出安全警示。建立威胁情报和信息共享机制，落实相关措施，提高主动发现攻击能力；

e) 应建立 CII 技术对抗机制，制定互联网接入安全管理规范，收敛暴露面；建立攻防演练机制，提高技术对抗和风险管理能力；

f) 应建立 CII 事件处置机制，制定 CII 网络安全应急预案，明确应急组织机构与职责，对网络安全事件进行报告和处置，并采取适当的应对措施，恢复由于网络安全事件而受损的功能或服务；建立定期应急演练机制，通过定期的应急演练活动来检验应急预案的可行性、应急准备的充分性以及联动机制的协调性；制定重大事件和威胁报告规范，明确报告流程和方法。

7.1.5 建立供应链安全管理制度

a) 应建立供应链安全管理机制，提供用于供应链安全管理的资金、人员和权限等可用资源；

b) 应建立供应链安全管理策略，包括：风险管理策略、供应方选择和管理策略、产品开发采购策略、安全维护策略等；

c) 应建立软件供应链管理机制，加强软件供应链安全管理，包括：开源软件安全管理、第三方组件安全管理、集成和分发的安全管理、可追溯性管理等。

7.1.6 建立数据安全管理制度

a) 应建立数据安全管理责任和评价考核机制，编制数据安全保护计划，实施数据安全技术防护，开展数据安全风险评估，制定数据安全事件应急预案，及时处置安全事件，组织数据安全教育、培训；

b) 应建立基于数据分类分级的数据安全保护策略，明确重要数据和个人信息保护的相应措施；

c) 应建立数据安全检测评估、出境安全评估机制，以及数据流转、交易、出境等管理机制；

d) 应建立数据安全审查机制，对数据及其相关安全管理负责人、关键岗位人员以及为数据处理活动全流程开展审查，保障重要数据安全关键岗位人员可信、可靠，数据处理活动合规有序，并配合相关部门开展数据安全审查工作；

e) 应建立数据安全业务连续性管理计划，例如：系统切换、降级运行等机制；

f) 应建立数据安全容灾备份机制，重要系统和数据库实现异地备份。

7.2 安全管理机构

7.2.1 成立网络安全工作委员会或领导小组

a) 应成立网络安全工作委员会或领导小组，由组织主要负责人担任其领导职务，明确一名领导班子成员作为首席网络安全官，专职管理或分管 CII 安全保护工作；

b) 网络安全工作委员会或领导小组成员应包括组织内各核心部门的负责人，可邀请外部网络安全专家或顾问作为决策咨询成员，为决策提供专业支持。

7.2.2 设置网络安全管理机构

a) 应设置专门的网络安全管理机构（以下简称“安全管理机构“），明确机构负责人及岗位，机构负责人应具有足够权限，直接向网络安全工作委员会或领导小组汇报。

b) 应为每一个 CII 明确一名安全管理责任人；

c) 应将安全管理机构人员纳入本组织信息化决策体系；

d) 应每季度至少召开一次全体会议，及时跟进网络安全工作进展和重要事项。在出现重大安全威胁、发生网络安全事件、外部环境变化以及 CII 发生重大变更时，应立即召开紧急会议，分析安全形势与风险，制定应对方案，并部署保障措施，确保风险得到有效控制。

7.2.3 认定 CII 安全关键岗位

a) 应对 CII 中的各个岗位进行重要性评估，认定 CII 安全关键岗位，明确岗位职责、专业技能和资质要求，关键岗位通常包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位；

b) 关键岗位应配备专人，并配备 2 人以上共同管理。

7.3 安全管理人员

7.3.1 岗前审查

a) 应对安全管理机构的负责人和关键岗位的人员进行安全背景审查和安全技能考核，符合要求的人员方能上岗；与 CII 直接相关的系统管理、网络管理、安全管理等重要岗位人员应内部选拔；

b) 当安全管理机构的负责人和关键岗位人员的身份、安全背景等发生变化（例如：取得非中国国籍）或必要时，应根据情况重新按照相关要求进行安全背景审查；

c) 应明确从业人员安全保密职责和义务，包括安全职责、奖惩机制、离岗后的脱密期限等，并签订安全保密协议。

7.3.2 岗位考核

a) 应在关键岗位人员上岗前进行安全技能考核，确保符合岗位要求后方能上岗。考核标准应针对各类岗位制定清晰、具体的内容，全面涵盖岗位职责所需的技能、知识、经验和个人素质等方面，包括理论考核和实操考核；

b) 应定期对考核效果进行评估，优化和完善考核内容，提高考核的针对性和有效性；

c) 应定期对关键岗位人员进行安全技能考核，明确复训和考核周期，留存考核记录。

7.3.3 离职管理

a) 应在人员发生内部岗位调动时，重新评估调动人员对 CII 的逻辑和物理访问权限，修改访问权限并通知相关人员或角色；

b) 应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份鉴别相关的软硬件设备，进行面谈并通知相关人员或角色。

7.4 安全建设管理

7.4.1 建设规划管理

a) 应在 CII 建设、改造、升级等环节，实现网络安全技术措施与 CII 主体工程同步规划、同步建设、同步使用；

b) 应加强全过程的网络安全管理，与规划、设计和建设单位应签署安全保密协议；

c) 应加强全过程的文档管理，对设计、开发、运行维护文档等进行留存归档。

7.4.2 方案设计管理

a) 应基于等级保护、商用密码、数据安全等有关网络安全法规标准要求，结合风险评估、渗透测试发现的问题，开展网络安全方案设计；

b） 应采取测试、评审、攻防演练等多种形式验证安全方案。必要时，可建设关键业务的仿真验证环境，予以验证；

c） 安全方案及其配套文件的合理性和正确性应进行论证和审定，经过批准后才能正式实施。

7.4.3 工程实施管理

a） 工程实施过程中应建立安全管理规定，对物理环境、安装调试、数据备份、测试验收等方面提出安全要求；

b） 应使用受控的调试设备、安全的调试网络开展 CII 工程实施过程。

7.4.4 系统验收管理

a） 应制订系统安全方案的验收测试方案，并依据方案实施测试验收，出具测试验收报告；

b） 应进行系统上线前的安全性测试（例如：渗透测试、风险评估、代码审查等方式），并出具安全测试报告。

7.5 安全策略管理

a） 应制定安全策略管理机制，重点考虑基于关键业务链安全需求，明确安全互联策略、安全审计策略、身份管理策略、入侵防范策略、数据安全防护策略、自动化机制策略（配置、漏洞、补丁、病毒库等）、供应链安全管理策略、安全运维策略，并根据 CII 面临的安全风险和威胁的变化进行相应调整；

b） 应制定安全策略备份机制，明确备份对象包括安全策略、系统架构、应用软件及配置、数据库数据、系统日志、系统监控数据等，以及备份方法、备份时间间隔、备份保存时间等，并在策略调整后重新备份；

c） 应在确定安全策略的基础上，制定配套操作规范、流程和工单，以保证安全策略得到落实。

7.6 安全运营管理

a） 应建立运营管理机制，明确网络安全运营工作的总体目标、范围、原则、安全运营方案等，形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全运营管理机制；

b） 应明确网络安全运营年度工作计划，设定可量化的阶段性里程碑和运营绩效指标，确保运营工作的可追踪性和可评估性；

c） 应保证 CII 的运维地点位于中国境内，如确需境外运维，应符合我国相关规定；

d) 应指定专门的部门或人员进行系统管理，对账户操作、系统变更、物理访问和系统接入等事项建立授权审批程序，明确授权审批事项、审批部门和批准人，对重要活动建立逐级审批机制；

e) 应明确安全运营的工作内容，包括日常巡检、安全实时监测、威胁情报、通报预警、应急处置、指挥调度、安全策略维护、数据备份等；

f) 应组织建立一支包括技术人员、管理人员、内外部专家在内的提供 7×24 小时安全运营保障的专业队伍，形成安全运营人员名单，签订安全保密协议；

g) 应确保优先使用已在本组织登记备案的运维工具，如确需使用未登记备案的运维工具，应在使用前通过恶意代码检测等测试；

h) 应建立和准备安全运营物资库（例如：系统恢复工具、备件物资等），保障运营物资供应的充足性和及时性；应定期对运营物资进行安全检查和维护；

i) 应推进安全运营持续改进文化建设，鼓励相关人员提出改进建议和创新想法，可设立改进项目和创新基金，对有价值的建议给予奖励和支持，同时建立持续改进的跟踪和评估机制，确保改进措施得到有效实施并取得预期效果。

7.7 安全监督管理

a) 应落实本单位的网络安全监督问责机制，明确规定本单位的监督管理部门及职责；

b) 监督管理应全面审视安全制度的执行、管理效能、技术防护的有效性、员工安全意识及跨部门协作等，确保 CII 在管理、技术、运营和保障等多维度上均得到有效保护；

c) 应每年至少开展一次 CII 安全监督检查工作。

8 技术能力体系

8.1 安全防护

8.1.1 安全通信网络

8.1.1.1 网络架构安全

应实现通信线路“一主双备”的多电信运营商多路由保护，宜对网络关键节点和重要设施实施“双节点”冗余备份。

8.1.1.2 互联安全

a) 应建立或完善不同网络安全等级保护系统之间、不同业务系统之间、不同区域的系统之间、不同运营者运营的系统之间的安全互联策略；

b) 应保持同一用户其用户身份和访问控制策略等在不同网络安全等级保护系统、不同业务系统、不同区域中的一致性；

c) 对不同局域网之间远程通信时应采取安全防护措施，例如：在通信前应基于采用商用密码、量子加密等先进加密技术，对通信的双方进行验证或鉴别、建立加密通道防止数据在传输过程中被截获和篡改等。

8.1.1.3 安全审计

a) 应设计全面的安全审计策略，监测、记录系统运行状态、日常操作、故障维护、远程运维等，对各种审计信息进行集中收集；利用大数据分析、机器学习等人工智能技术进行实时分析，自动识别异常行为、安全漏洞、安全事件，定期生成安全审计报告；

b) 应定期备份并留存相关日志数据，留存相关日志数据不少于 6 个月。

8.1.2 安全区域边界

8.1.2.1 边界防护

a) 在不同网络安全等级保护系统之间、不同业务系统之间、不同区域的系统之间、不同运营者运营的系统之间，应采用物理隔离技术、逻辑隔离技术等，对互操作、数据交换和信息流向进行严格控制；

b) 使用无线网络进行跨业务系统、跨区域访问时，应保证无线网访问控制措施与各系统、各区域边界的访问控制措施一致。

8.1.2.2 软硬件接入管控

a) 在软硬件接入系统前，应进行安全评估，确保不存在已知安全漏洞和风险；

b) 应设置严格的设备接入策略和机制，对未授权设备进行动态发现及管控，只允许通过运营者授权的软硬件运行；

c) 应采用多种认证技术和方法，例如：口令、数字证书、生物识别技术等，对跨区域通信的设备、通过外部网络接入到内部网络的设备等进行多因素身份鉴别。

8.1.3 安全计算环境

8.1.3.1 鉴别与授权

a) 应建立并持续更新重要业务操作、关键用户操作及异常用户行为的清单，确保所有关键活动均被纳入其中，并经安全团队严格审核与批准，以维护操作行为的规范性和安全性；
b) 应对设备、用户、服务或应用、数据进行安全管控，对于重要业务操作、重要用户操作或异常用户操作行为，建立动态的身份鉴别方式，或者采用多因素身份鉴别等方式；
c) 针对重要业务数据资源的操作，应对主体（例如：用户、进程）和客体（例如：文件、数据库表）实施安全标记管理，并基于安全标记和强制访问控制策略，限制主体对客体的访问。

8.1.3.2 入侵防范

a) 应采取技术手段，提高对高级可持续威胁（APT）等网络攻击行为的入侵防范能力；
b) 应采用主机入侵检测系统（HIPS）、EDR、可信计算、沙箱等技术，实现系统主动防护，及时识别、告警、干扰和阻断入侵、恶意代码、病毒等行为；
c) 应采取行为监测、勒索诱捕、系统防护、进程防护、数据保护、备份恢复等技术手段，例如：利用云防护、设置蜜罐和联动沙箱、接入零信任系统、部署联动迷阵和联动防火墙、建设网络安全威胁监测系统和智能态势感知系统、部署人工智能安全监测专业大模型等，重点防范勒索攻击。

8.1.3.3 自动化工具

应使用自动化工具来支持系统账户、配置、漏洞、补丁、病毒库等的管理，对于漏洞、补丁，应在经过测试验证其有效性和安全性后，及时进行修补。

8.1.3.4 容灾备份与恢复

a) 应按照业务连续性管理需要，建立重要数据、数据库等容灾备份机制，对业务安全性要求高的可采取数据异地实时备份，业务连续性要求高的可采取重要系统异地备份；
b) 应定期进行数据和系统备份的恢复验证，例如：系统发生重大变更前后、固定周期。

8.1.4 新技术、新应用扩展防护

8.1.4.1 云平台安全

对于自身就是 CII 的云平台：

a） 云服务提供者承担 CII 运营者的角色对云平台实施安全保护，此类云平台应申请并通过《云计算服务安全评估》。

b） 应在各云服务客户虚拟网络之间，采取有效的隔离措施，例如：VLAN 隔离、网络虚拟化等。并配备通信传输、边界防护和入侵防范等技术措施，保证云服务客户网络区域安全；

c） 在云平台网络边界，应配置基于角色的访问控制策略，采用逻辑隔离、入侵检测、高级威胁检测等措施，重点监测和防范 DDoS 等网络攻击；

d） 应支持云服务客户自定义安全策略，例如：基于 IP/端口的访问控制、IP 黑白名单等，并允许接入符合标准的第三方安全产品或服务，以增强云平台安全防护；

e） 云服务提供商应采用数字签名等技术，建立加固的镜像和完整性校验机制，确保数据的完整性。在数据迁移时采用加密传输技术，防止数据泄露；

f） 应建立云平台的安全检查与数据备份机制，定期进行数据备份恢复验证，确保数据的可恢复性与业务连续性；

g） 应通过监测预警、态势感知、溯源分析等技术，实现云平台安全态势实时、集中监测，发现潜在威胁与异常行为，开展安全事件的追踪与处置；

h） 应强化云平台及应用程序内生安全，使用安全加固的云操作系统及应用软件，将安全性嵌入代码本身，确保云应用程序自上线之日起即具备高安全性，且能在其整个生命周期内持续保持符合安全标准的状态。

对于 CII 业务系统部署在云上，涉及自建云的：

a） 云上 CII 的安全保护不仅包括对云上 CII 业务系统的保护，也包括对其所在云平台的安全保护。CII 所在云可自行或委托“云计算服务安全评估专业机构”开展安全评估。

8.1.4.2 移动互联安全

a） 应制定移动互联安全管理制度，明确移动终端的安全配置标准、使用规范、维护及报废处理要求，并设立安全审计机制，定期审查移动终端的使用记录与安全状态，确保移动终端的安全可控；

b） 应建设具有准入控制功能的无线移动终端统一管理系统，建立终端设备白名单机制，采用数字证书、生物特征识别等方式对终端设备无线接入进行身份认证，确保仅授权合法设备可接入系统；

c) 应选择具有终端设备准入控制功能的无线网络设备，采用支持 WPA3 企业级加密、MAC 地址绑定、802.1X 认证等安全接入技术，实现移动终端的安全接入与访问控制；

d) 移动应用应在上线前，委托具有资质的专业测评机构进行安全性检测，检测内容包括应用代码的安全性、数据加密与传输安全、用户隐私保护等；

e) 应建立移动应用版本更新、维护与安全复审机制，确保应用安全补丁及时发布、持续符合安全要求。

8.1.4.3 物联网安全

a) 应加强对物联网感知节点物理安全防护，根据环境特点，对于物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等加强保护，例如：增加物理防护装置、配置安全物理锁、增加视频监控、配置冗余电源、采用抗干扰、防屏蔽手段等；

b) 在工业物联网场景（如：智能电网、智能油田）中，应采用强身份认证机制，例如：基于数字证书的身份认证体系，结合数据加密与完整性校验技术，保护物联网通信过程中的数据安全与完整性；在智慧交通、车联网等场景中，应实施车辆与设备身份认证与访问控制机制，采用车联网专用安全通信协议，确保车辆与基础设施间的通信安全，同时，对敏感数据进行加密存储与传输，防止数据泄露。

8.1.4.4 工业控制系统安全

a) 工业控制系统机房所处建筑应采取有效防水、防潮、防火、防静电、防雷击、防盗窃、防破坏措施，采取措施保障工业控制系统可靠供电，应当配置电子门禁系统以加强物理访问控制，必要时应当安排专人值守，应当对关键区域实施电磁屏蔽；

b) 应建立工业控制系统与 CII 运营者其他系统之间的安全互联策略，采用符合国家标准或行业规定的专用产品实现单向安全隔离；

c) 应在不影响业务实时性前提下，采用商用密码技术，保障通信数据传输和存储过程中的完整性和保密性；

d) 可采用可信验证措施实现安全免疫，具备控制能力的业务模块可逐步应用可信计算技术，实现设备安全启动及系统引导程序、系统程序、重要配置参数和应用程序的完整性度量，有效保证计算环境和网络环境安全可信，免疫未知恶意代码破坏，应对高级别的恶意攻击；

e) 应关闭、物理封堵或拆除工业控制系统设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等,确需保留的应采用外设管控系统进行接管，实施严格的监控管理，可配合具有杀毒标记的安全介质，实现数据的安全摆渡；

f) 对于高可用性的控制系统，安全防护设备应采用旁路监听、硬件 BYPASS、紧急逃生等技术，保障安全措施失效时不中断业务基本功能；

g) 应强化工业控制系统内生安全，使用安全加固的操作系统及应用软件，将安全性嵌入代码本身，确保工业控制系统自上线之日起即具备高安全性。

8.1.4.5 5G 网络技术安全

a) 应严格执行 5G 网络准入控制，融合多因素认证技术确保用户身份的真实性与安全性，防止非法接入，同时采用 TLS/SSL 或量子加密技术保障数据传输过程中的保密性；

b) 应实施精细化的 5G 专网终端访问控制策略，基于角色的权限管理，结合 MAC 地址绑定、IP 白名单等技术手段，确保接入设备的合法性与合规性，防止资源的非授权访问；

c) 应加强对 5G 关键终端的安全防护，部署终端安全管理软件，定期进行安全审计与漏洞扫描，及时修补已知漏洞；

d) 应遵循数据最小化原则，只收集必要的用户数据，避免过度收集用户隐私信息；同时提供用户更多的隐私控制权，使用户能够管理自己的隐私设置，选择是否分享数据。

8.1.4.6 区块链技术安全

a) 应采用密码技术确保用户身份的唯一性和可信任性，例如：使用数字签名、多重签名等技术进行身份验证。同时限制用户的访问权限，确保只有经过授权的用户才能访问和操作区块链系统；

b) 应使用密码技术确保区块链数据的机密性和完整性，例如：使用对称、非对称加密算法或量子安全加密算法对敏感数据进行加密存储和传输；

c) 选用密码算法及技术产品与服务时，应符合国家密码管理部门及行业标准规范要求，例如：SM2、SM3、SM4 等商用密码算法，以及经过认证的加密模块和安全芯片，确保区块链数据的安全传输和存储；

d) 应选择安全可靠的共识算法，例如：工作量证明（PoW）、权益证明（PoS）等，并进行安全性验证和评估，应关注共识算法可能面临的攻击，例如：51%攻击、双重支付攻击等，并采取相应的防护措施；同时加强对智能合约的审核与测试，通过形式化验证、静态分析等技术手段，确保其完整性和抗抵赖性；

e） 应建立有效的审计机制，对区块链系统进行定期审计，确保安全措施的有效性。

8.1.4.7 IPv6 技术安全

a） 应通过隐私地址保护、地址分配管理等，实现用户隐私和网络安全防护，例如：利用 IPv6 隐私扩展地址定期更换源地址；采用 DHCPv6 对设备的 IPv6 地址进行集中管理和分配；

b） 应开展协议安全防护，例如：使用邻居发现协议保护、ICMPv6 报文过滤防护等技术，有效防止恶意 NDP 欺骗攻击、ICMPv6 泛洪攻击、重定向攻击等；

c） 应为 IPv6 提供认证、完整性和加密服务，确保数据传输安全，防范泄露与篡改风险；

d） 应执行 IPv6 地址白名单策略，严格管理网络设备信息，控制接入权限，提升 IPv6 网络安全性。

8.1.4.8 大数据及平台安全

a） 应建立大数据安全管理制度，明确约定各方权限和责任；

b） 应采用自然语言处理和机器学习等技术， 对结构化与非结构化数据进行内容识别，强化数据的分级分类管理；

c） 应对数据采集、存储、处理等各个环节进行安全审计，可采用 AI 行为探测、动态水印、区块链存证、动态脱敏等技术。

8.1.4.9 人工智能安全

a） CII 人工智能应用系统应采取本地化部署方式，采用动态数据脱敏、联邦学习等技术，避免核心数据泄露；

b） 应严格限制人工智能系统对 CII 的操作和控制权限，保留重要操作的人工监督和接管能力；

c） 应采用密码技术对敏感数据进行端到端加密，确保训练数据与模型参数的传输和存储安全性；

d） 应采用沙箱隔离等手段，隔离 AI 系统与其他业务模块，限制横向攻击面；

e） 应采用差分隐私等技术，在数据集内添加噪声保护个体隐私；

f） 应建立算法审计机制，定期检测模型逻辑漏洞与潜在偏见，确保决策透明性与公平性；

g） 应采取对抗性训练等措施，提升模型鲁棒性，抵御对抗样本攻击（例如：输入数据篡改）；

h） 应通过定期审计加强对人工智能系统安全性、可靠性、可控性的监测，并实施合理的数据访问限制和加密保护。

8.1.5 大数据支撑

a) 可采用大数据分析挖掘技术、人工智能技术等，进行威胁信息搜集、分析、挖掘、整合，构建动态更新的威胁情报库；

b) 可在态势感知平台中部署和应用大数据技术，对网络运行状态进行持续检测，通过管理分析技术对异常行为进行识别和报警；

c) 可采用大数据技术结合自动化扫描工具和威胁情报，智能排序和分析漏洞优先级，提供专业有效的修复方案；

d) 可基于大数据技术，增强 XDR 与 SIEM 的自动化和智能化，识别复杂攻击路径，提供深入的安全事件分析，并生成可操作的响应策略；

e) 可采用大数据技术对事件分析和响应流程优化，提升安全运营中心威胁识别能力。

8.1.6 人工智能技术支持

a) 可采用机器学习和深度学习等人工智能技术，对网络流量、日志数据和历史攻击事件等进行分析和训练，自动发现异常行为和潜在威胁；

b) 可采用人工智能技术自适应学习新攻击模式，结合自动化响应机制，在钓鱼检测、威胁情报分析、安全策略制定方面提供优化建议；

c) 可采用人工智能技术深度分析网络流量，识别高级可持续威胁（APT）和零日漏洞利用，提升入侵防御能力；可采用人工智能技术检测逃逸（例如：恶意软件免杀）和身份认证攻击，强化终端安全和集权设备监控，提升高级威胁对抗能力；

d) 可采用人工智能技术分析恶意代码特征（例如：静态代码结构、动态行为模式），进行特征提取与行为预测，建立恶意软件库，快速识别未知变种，提升未知威胁检测能力；

e) 可采用人工智能技术分析用户登录时间、设备使用习惯等数据，构建正常行为基线，进行用户行为分析和内部威胁检测，一旦偏离正常行为基线（例如：异常数据访问），系统自动触发警报；

f) 可采用人工智能技术（例如：自然语言处理技术）识别敏感信息，进行脱敏或加密处理，并实时分析用户操作和网络流量，预警潜在泄露风险；

g) 可采用人工智能分析软件代码和配置，预测潜在漏洞，并提供修复建议；可采用大模型技术实现自适应漏洞修复；

h) 可采用人工智能技术整合网络设备、日志、威胁情报等数据，生成实时安全态势报告，评估企业网络环境中的风险等级，提供针对性防护策略；

i） 可采用人工智能技术（例如：GAN 创建虚假网络拓扑、协议级混淆技术、DNS 投毒、漏洞武器库污染等）实现人工智能驱动的动态对抗和反制。

8.2 数据安全

a） 将在我国境内运营中收集和产生的个人信息和重要数据存储在境内。因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估。法律、行政法规另有规定的，依照其规定；

b） 应实施数据分类分级管理，依据数据的敏感度、重要性等因素，通过数据安全组件（例如：数据水印设备、数据加密设备、数据审计系统等）的联动，实现数据的自动分类、分级，为不同等级的重要数据和个人信息提供差异化安全保护；

c） 应严格控制重要数据的使用、加工、传输、提供和公开等关键环节，并采取加密（例如：量子加密、商用密码、IPv6 等）、脱敏、去标识化等技术手段保护敏感数据安全；

d） 应强化数据访问控制机制，采用基于角色的访问控制、最小权限原则等技术手段，对不同用户或系统赋予必要的、最小化的数据访问权限，确保数据只能被授权人员或系统访问；同时，加强鉴权过程的安全保护，提升数据访问的安全性；

e） 应构建数据安全监测与预警平台，实时监测数据的安全状态，及时发现并预警潜在的数据安全风险，快速响应数据安全事件；

f） 数据可用性要求高的，应采取数据库异地实时备份措施。业务连续性要求高的，应采取系统异地实时备份措施，确保 CII 一旦被破坏，可及时进行恢复和补救；

g） 应在 CII 退役废弃时，按照数据安全保护策略对存储的数据进行处理；

h） 应建立数据处理活动全流程的安全能力，并符合相关国家标准关于数据安全保护的要求；

i） 应定期开展数据安全审计与风险评估，对数据全生命周期的各环节的合规性、安全性进行审计与评估，及时发现并纠正数据安全管理中的问题和漏洞。

8.3 供应链安全

a） 采购网络关键设备和网络安全专用产品目录中的设备产品时，应采购通过国家检测认证的设备和产品；

b） 应优先采购国产安全可信的网络产品和服务，对包括软硬件产品、数据库、终端、业务系统和工业控制系统的核心产品等实施信息技术应用创新替代；

c） 应形成年度采购的网络产品和服务清单。采购、使用的网络产品和服务应符合相关国家标准的要求。可能影响国家安全的，应通过国家网络安全审查；

d） 应定期梳理和更新供应链中的企业、产品以及人员信息，绘制供应链安全管理的动态图谱，建立和维护合格供应方目录，并采用可视化工具等技术手段，对供应链进行管理；

e） 应选择有保障的供应方，防范出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险；

f） 应强化采购渠道管理，保持采购渠道的稳定性和多样性；

g） 采购网络产品和服务时，应明确提供者的安全责任和义务，要求提供者对网络产品和服务的设计、研发、生产、交付等关键环节加强安全管理。要求提供者声明不非法获取用户数据、控制和操纵用户系统和设备，或利用用户对产品的依赖性谋取不正当利益或者迫使用户更新换代；

h） 应与网络产品和服务的提供者签订安全保密协议，协议内容应包括安全职责、保密内容、奖惩机制、有效期等；

i） 应要求网络产品和服务的提供者对网络产品和服务研发、制造过程中涉及的实体拥有或控制的已知技术专利等知识产权获得 10 年以上授权，或在网络产品和服务使用期内获得持续授权；

j） 应要求网络产品和服务的提供者提供中文版运行维护、二次开发等技术资料；

k） 应自行或委托第三方网络安全服务机构对定制开发的软件进行源代码安全检测，或由供应方提供第三方网络安全服务机构出具的代码安全检测报告；

l） 当使用的网络产品和服务存在安全缺陷、漏洞等风险时，应及时采取措施消除风险隐患，对安全事件进行应急响应和处置。对于涉及重大风险的情况，应按照规定及时向相关部门报告；

m） 应对关键业务链开展供应链安全风险分析，及时发现风险隐患和风险点，并进行风险处置；

n） 应强化应用开发阶段的供应链安全管理，采用安全开发工具，例如：开源软件成分分析、源代码扫描、漏洞扫描等，在开发和测试验证阶段发现和解决潜在的安全隐患。

9 运营能力体系

9.1 分析识别

9.1.1 业务识别

a） 应识别本组织的关键业务和与其相关联的外部业务；

b） 应开展多维度业务分析，综合运用自动化工具和人工分析，构建包括业务网络架构、逻辑关系、边界界定以及业务间相互关系在内的业务关联图谱；

c） 应分析本组织关键业务对外部业务的依赖性和重要性；

d） 可在核心交换机的关键位置部署流量监测探针，构建全网流量监测系统，绘制 CII 的数据流量全景图，分析关键业务流量与外部业务流量之间的依赖性和重要性；

e） 应梳理关键业务链，明确支撑关键业务的 CII 分布和运营情况。

9.1.2 资产识别

a） 应采用资产检测探针、资产分析工具等多种技术手段，识别关键业务链所依赖的资产，建立关键业务链相关的网络、系统、数据、服务和其他类资产的资产清单；

b） 应基于资产类别、资产重要性和支撑业务的重要性，确定资产防护的优先级；

c） 应采用资产探测技术识别资产，并根据关键业务链所依赖资产的实际情况动态更新。

9.1.3 风险识别

a） 应按照 GB/T 20984 等风险评估标准，对关键业务链开展安全风险分析，识别关键业务链各环节的威胁、脆弱性，确认已有安全控制措施，分析主要安全风险点，确定风险处置的优先级，形成安全风险报告；

b） 应采用探测扫描、检测评估、攻防验证以及情报共享等技术手段，对 CII 的网络结构、网络设备、安全防护设备、中间件、数据库等关键组成部分的安全状况进行全面审查，以识别组织可能面临的网络安全风险；

c） 应实现风险的动态持续监测，重点关注残余风险和新出现的风险情况，每年至少进行一次全面的风险评估。

9.1.4 重大变更

在 CII 发生改建、扩建、所有人变更等较大变化时，应重新开展识别工作，可能影响认定结果的，应及时将相关情况报告保护工作部门，并更新资产清单。

9.2 检测评估

a） 应自行或者委托网络安全服务机构对 CII 安全性和可能存在的风险，每年至少进行一次检测评估，并及时整改发现的问题；

b) 在涉及多个运营者时，应定期组织或参加跨运营者的CII安全检测评估，并及时整改发现的问题；

c) 在检测评估时，内容应包括但不限于网络安全制度（国家和行业相关法律、法规、政策文件及运营者制定的制度）落实情况、组织机构建设情况、人员和经费投入情况、教育培训情况、网络安全等级保护制度落实情况、商用密码应用安全性评估情况、技术防护情况、数据安全防护情况、供应链安全保护情况、云计算服务安全评估情况（适用时）、风险评估情况、应急演练情况、攻防演练情况等，尤其关注CII跨系统、跨区域间的信息流动，及其资产的安全防护情况；

d) 在CII发生改建、扩建、所有人变更等较大变化时，应自行或者委托网络安全服务机构进行检测评估，分析关键业务链以及关键资产等方面的变更，评估上述变更给CII带来的风险变化情况，并依据风险变化以及发现的安全问题进行有效整改后方可上线；

e) 应针对特定的业务系统或系统资产，经有关部门批准或授权，采取模拟网络攻击方式，检测CII在面对实际网络攻击时的防护和响应能力；

f) 在安全风险抽查检测工作中，应配合提供网络安全管理制度、网络拓扑图、重要资产清单、关键业务链、网络日志等必要的资料和技术支持，针对抽查检测工作中发现的安全隐患和风险建立清单，制定整改方案，并及时整改。

9.3 监测预警

9.3.1 安全监测

a) 应在网络边界、网络出入口等网络关键节点部署攻击监测设备，发现网络攻击和未知威胁；

b) 应对关键业务所涉及的系统进行监测（例如：对不同网络安全等级保护系统、不同区域的系统之间的网络流量进行监测等），对监测信息采取保护措施，防止其受到未授权的访问、修改和删除；

c) 应全面采集网络通信数据，分析系统通信流量或事态的模式，建立常见系统通信流量或事态的模型，并使用这些模型调整监测工具参数，以减少误报和漏报；

d) 应全面收集网络安全日志，构建常规操作模型、攻击入侵模型、异常行为模型，强化监测预警能力；

e) 应采用自动化机制，对关键业务所涉及的系统的所有监测信息进行整合分析，以便及时关联资产、脆弱性、威胁等，分析 CII 的网络安全态势。CII 跨组织、跨地域建设时，构建集中统一指挥、多点全面监测、多级联动处置的动态感知能力；

f) 应将关键业务运行所涉及的各类信息进行关联，并分析整体安全态势，包括：分析不同存储库的审计日志并使之关联；将多个信息系统内多个组件的审计记录关联；将信息系统审计记录信息与物理访问监控的信息关联；将来自非技术源的信息（如：供应链信息、关键岗位人员信息等）与信息系统审计信息关联；网络安全共享信息的信息关联等；

g) 应通过安全态势分析结果来确定安全策略和安全控制措施是否合理有效，必要时进行更新；

h) 应建立 7×24 小时网络安全监控运营中心，对 CII 资产风险、系统运行状态、告警、业务资产外部连接、内外部威胁分析、安全运营分析、攻击事件分析、处置状态追踪、预警与通知进行监视管理。

9.3.2 通报预警

a) 应将监测工具设置为自动模式，当发现可能危害关键业务的迹象时，能自动报警，并自动采取相应措施，降低关键业务被影响的可能性。如恶意代码防御机制、入侵检测设备或防火墙等弹出对话框，发出声音或者向相关人员发出电子邮件等方式进行报警；

b) 应对网络安全共享信息和报警信息等进行综合分析、研判，必要时生成内部预警信息。对于可能造成较大影响的，应按照相关部门要求进行通报。内部预警信息的内容应包括：基本情况描述、可能产生的危害及程度、可能影响的用户及范围、宜采取的应对措施等；

c) 应能持续获取预警发布机构的安全预警信息，分析、研判相关事件或威胁对自身网络安全保护对象可能造成损害的程度，必要时启动应急预案，获取的安全预警信息应按照规定通报给相关人员和相关部门；

d) 采取相关措施对预警信息进行响应，当安全隐患得以控制或消除时，应执行预警解除流程。

9.3.3 风险防控

a) 应围绕 CII 承载的关键业务，通过风险评估技术，例如：漏洞扫描、渗透测试、安全审计等，识别系统中的薄弱点；应利用威胁情报结合大数据分析，识别异常行为和潜在攻击；

b) 应采用分层防御策略，以云防御、零信任架构、威胁情报网关、暴露面管理、终端防护等技术，进行威胁控制；

c） 应开展风险防控能力评估，检验防控措施的有效性，并针对发现的安全隐患和外部风险威胁进行整改。

9.3.4 预知预判

a） 应分析历史数据和网络活动，识别潜在威胁模式和异常行为；

b） 应整合来自外部的安全事件信息，提供最新的攻击趋势和威胁情报，预见可能的攻击手段；

c） 应采用模拟攻击、安全评估工具测试等方式验证可能的攻击手段，提前识别潜在漏洞和薄弱环节，及时采取预防措施。

9.3.5 威胁情报

a） 应建立本部门、本单位网络威胁情报共享机制，组织联动上下级单位，开展威胁情报搜集、加工、共享、处置；

b） 应整合多源安全信息，并集成到检测评估、监测预警等相关管理系统中，增强检测和响应能力；

c） 应建立外部协同网络威胁情报共享机制，与权威网络威胁情报机构开展协同联动，实现跨行业领域网络安全联防联控。

9.4 技术对抗

9.4.1 收敛暴露面

a） 应识别和减少互联网和内网资产的互联网协议地址、端口、应用服务等暴露面，关停废弃或过时的网络资产，压缩互联网出口数量；

b） 应减少对外暴露组织架构、邮箱账户、组织通信录等内部信息，防范社会工程学攻击；

c） 不应在公共互联网平台（例如：代码托管平台、文库、网盘、人工智能平台等）上传或存储可能被攻击者利用的技术文档（例如：网络拓扑图、源代码、互联网协议地址规划等）；

d） 应强化暴露面风险防范措施，开展常态化暴露面风险监测，动态监测和识别域名、IP、端口服务、移动应用、公众号、小程序等资产暴露面，并进行安全加固。

9.4.2 攻击发现和阻断

a） 应分析网络攻击的方法、手段，针对拒绝服务攻击等各类攻击，采取有针对性的防护策略和技术措施（例如：部署蜜罐、沙箱等），制定总体技术应对方案；

b) 应针对监测发现的攻击活动，分析攻击路线、攻击目标，设置多道防线，采取捕获、干扰、阻断、封控、加固等多种技术手段，切断攻击路径，快速处置网络攻击；

c) 应及时对网络攻击活动开展溯源，对攻击者进行画像，为案件侦查、事件调查、完善防护策略和措施提供支持；

d) 应系统全面地分析网络攻击意图、技术与过程，进行关联分析与还原，并以此改进安全保护策略，并加以落实。

9.4.3 攻防演练

a) 应围绕关键业务的可持续运行设定演练场景，定期组织开展攻防演练，CII 跨组织、跨地域运行的，组织或参加实网攻防演练。在不适合开展实网攻防演练场景下，采用沙盘推演、虚实靶场的方式进行攻防演练；

b) 应将 CII 核心供应链、紧密上下游产业链等业务相关单位纳入演练范畴；

c) 应制定年度攻防演练工作计划，包括实网攻防、渗透测试、沙盘推演、跨单位联合演练等各种形式，按计划组织演练；

d) 应针对攻防演练中发现的安全问题及风险进行及时整改，消除结构性、全局性风险，评估修订应急预案。

9.5 事件处置

9.5.1 应急预案和演练

a) 应在国家网络安全事件应急预案的框架下，根据行业和地方的特殊要求，制定网络安全事件应急预案；

b) 应在应急预案中明确，一旦信息系统中断、受到损害或者发生故障时，需要维护的关键业务功能，并明确遭受破坏时恢复关键业务和恢复全部业务的时间。应急预案不仅应包括本组织应急事件的处理，也应包括多个运营者间的应急事件的处理；

c) 在制定应急预案时，应同所涉及的运营者内部相关计划（例如：业务持续性计划、灾难备份计划等）以及外部服务提供者的应急计划进行协调，以确保连续性要求得以满足；

d) 应在应急预案中包括非常规时期、遭受大规模攻击时等处置流程；

e) 应在应急预案中包括 CII 应急物资管理要求（例如：系统恢复工具、备件物资等），保障应急物资供应的充足性和及时性；应定期对应急物资进行安全检查和维护，确保应急物资的可用性；

f） 应对网络安全应急预案定期进行评估修订，并持续改进；

g） 应每年至少组织开展 1 次本组织的应急演练。CII 跨组织、跨地域运行的，应定期组织或参加跨组织、跨地域的应急演练。

9.5.2 响应和处置

a） 当发生有可能危害关键业务的安全事件时，应及时向安全管理机构报告，并组织研判，形成事件报告；

b） 应及时将可能危害关键业务的安全事件通报到可能受影响的内部部门和人员，并按照规定向供应链涉及的、与事件相关的其他组织通报安全事件；

c） 应按照事件处置流程、应急预案进行事件处理，恢复关键业务和信息系统到已知的状态；

d） 应按照先应急处置、后调查评估的原则，在事件发生后尽快收集证据，按要求进行信息安全取证分析，并确保所有涉及的响应活动被适当记录，便于日后分析，在进行取证分析时，应与业务连续性计划相协调；

e） 在进行事件处理活动时，应协调组织内部多个部门和外部相关组织，以更好地对事件进行处理。

9.5.3 事件恢复

a） 在事件处理完成后，应采用手动或者自动化机制形成完整的事件处理报告。事件处理报告包括：不同部门对事件的处理记录、事件的状态和取证相关的其他必要信息、评估事件细节、趋势和处理；

b） 在恢复关键业务和信息系统后，应对关键业务和信息系统恢复情况进行评估，查找事件原因，并采取措施防止关键关键业务和信息系统遭受再次破坏、危害或故障；

c） 应及时将安全事件及其处置情况通报到可能受到影响的部门或相关人员，向供应链涉及的，与事件相关的其他组织提供安全事件信息，并按照法律政策规定报告相关部门；

d） 将事件处理活动的经验教训纳入事件响应规程、培训以及测试，并进行相应变更。

9.5.4 重新识别

应根据检测评估、监测预警、技术对抗中发现的安全隐患或发生的安全事件，以及处置结果，并结合安全威胁和风险变化情况开展评估，必要时重新开展业务、资产和风险识别工作，并更新安全策略。

10 保障能力体系

10.1 组织及制度保障

a) 应建立合理的组织架构和CII网络安全管理机构,确保网络安全工作有明确的领导和责任划分，并保持整体组织机构的稳定性；

b) 应建立清晰的符合组织业务范围的CII安全管理制度，由决策层批准，并通过运营者的主要信息发布渠道进行广泛发布；

c) 管理层应提供保障和支持，提供清晰的指导，明确CII安全职责的分配，提供对安全的主动支持；

d) 应分离某些任务的管理、执行和职责范围，加强监督力度，以降低非法修改或误用职权带来的风险；

e) 应建立网络安全管理部门与内外部业务部门之间的合作与沟通机制，定期召开协调会议，共同协作处理网络安全问题；

f) 应定期或在有重要变更时，对组织的CII安全管理制度进行独立审核，以保持制度的适用性、充分性和有效性；

g) 应建立安全管理制度的反馈机制，并根据反馈进行制度的持续改进；

h) 应制定符合CII业务安全特点并适合本组织的CII安全长期规划，明确CII安全保护目标，并将长期规划合理分解，形成CII安全短期规划；根据CII内外部环境的发展变化，适时地维护更新安全规划；

i) 可引入保险机制，构建“保险+风险管控+服务”模式，提高风险治理能力。

10.2 人才队伍保障

a) 应指定或授权专门的部门或人员负责CII相关人员的管理工作，建立网络安全人才培养机制、技能认证机制及培训评价机制，形成实战型人才教育训练体系，打造攻防兼备的人才队伍；

b) 应通过网络安全比武竞赛等活动，发现、选拔人才，建立并维护动态更新的CII人才库，涵盖行业内外优秀人才，为本单位CII人才选拔、任用提供支撑；

c) 应构建实战型网络安全人才培养的课程体系，包括基础课程、专业课程、实践环节、实战活动等，全方位促进CII安全人才成长与发展；

d) 应建立并维护网络安全师资队伍。一是与高校、公安机关、企业、研究机构等合作加强实战型师资培养，进行定期交流；二是聘请有实战经验的专家进行授课；

e) 应开展实战型实训环境建设，按照战训结合原则共建共享攻防实验室、网络靶场、模拟仿真实验室、训练平台等。实训环境应具备实施网络攻击、网络对抗的方法、手段、技术、战术，以及检验、验证、展示等能力；

f) 应开展年度网络安全教育培训，确保每人每年不少于 30 学时，内容覆盖法规政策标准、网络安全管理制度、网络安全防护技术等；

g) 应定期组织网络安全沙盘推演、攻防对抗、实战演练等活动，提升应对复杂安全挑战的实战能力；

h) 应对人才培训、实践、实战活动等效果进行综合评定和考核，并进行奖惩；

i) 应定期安排 CII 从业人员参加国家、行业或业界的网络安全相关交流活动，及时获取网络安全动态，推动 CII 人员能力的提升；

j) 应为 CII 人才建立专项薪酬和福利保障等激励机制，包括绩效奖金、股权激励、健康保险、退休福利等，保障队伍稳定。

10.3 经费保障

a) 应建立 CII 经费保障机制，列支 CII 安全年度预算，包括 CII 安全防护设备购置、安装、调试、维护，以及系统升级、改造、监督检查、教育培训等，并设立专项应急响应与恢复费用，用于应对和处理突发网络安全事件，减少事件对 CII 的影响；

b) 应建立合理的投资和预算规划，根据业务需要、威胁形势变化和技术进步动态优化资金配置，确保设备采购、系统升级、应急响应等关键领域和项目获得重点支持；

c) 应加强资金使用的监督管理，加强内部管理和外部监督，对资金使用中的违规行为进行责任追究，确保资金安全、合理、透明使用；

d) 应定期进行资金使用审计和评估，发现资金使用中的不足，及时调整策略；

e) 应建立资金保障的长效机制，将资金保障纳入长期规划，确保连续性和稳定性，加强与主管部门、行业机构等合作，争取更多政策和资金支持。

10.4 跨组织保障

a) 应建立跨组织的有关职能机构、运营商、服务方等的沟通、协调、联动机制。应建立和维护内外部联系列表，包括单位名称、合作内容、联系人和联系方式等信息，设立协作小组，明确目标与责任分配，确保各参与方清晰知晓其角色与任务；

b） 应建立高效沟通机制。包括定期会议、在线协作平台及紧急联络流程，确保 CII 安全有关活动的有效沟通和实施；

c） 应统一业务流程与数据标准。制定协作手册，明确协作规范与工作流程，提升合作效率；

d） 应注重敏感信息管理。对跨组织协作中的敏感信息进行严格保护，防止泄露或滥用；

e） 应在建立跨组织信息共享平台，确保信息从发现到共享的平均时间不超过 24 小时；

f） 应定期组织跨组织网络安全应急演练，对演练过程中发现的问题进行记录和整改，不断优化跨组织应急响应流程；

g） 应建立跨组织协同联动绩效评估体系，从资源调配、响应时间及问题解决效率等方面设定执行效果评估指标，制定奖惩措施并确保实施；

h） 应开展跨组织安全培训及文化交流活动，确保所有相关人员了解跨组织协同联动基本要求、必要性及各自承担的安全责任。

附录 A CII 高风险评价

（资料性）

关联评价的结果可分为高风险、中风险、低风险三档：

高风险：风险发生会对国家安全、社会秩序和公共利益造成影响；对公民、法人和其他组织的合法权益造成非常严重影响；导致 CII 关键业务开展受到严重影响；触犯国家法律法规；或造成非常严重的财产损失。

中风险：风险发生会对公民、法人和其他组织的合法权益造成影响；导致关键业务开展受到严重影响；造成严重的财产损失。

低风险：风险发生会对公民、法人和其他组织的合法权益造成一定影响；导致关键业务开展受到一定影响；造成一定的财产损失。

在上述风险评价的基础上，若存在以下情况之一的，应认定该 CII 的关键业务安全风险为高：

a） 物理访问控制缺失，外部人员可随意进入 CII 核心机房、重要操作区、核心设备区的；

b） CII 核心网络与其它网络（互联网服务区、办公区等）间隔离措施失效或存在旁路的，或私自把无线网络接入 CII 核心网络的；

c） 涉及 CII 关键业务的关键网络设备、关键安全设备、关键计算设备、核心业务系统无安全审计措施，不能对重要用户行为、重要安全事件进行审计的；

d） 支撑 CII 关键业务的网络设备、安全设备、计算设备单机运行，且无应急处置方案的；

e） 关键资产识别严重缺失的；

f） 通过关联评价可以获取 CII 关键业务应用服务器权限的；

g） CII 核心设备被恶意代码入侵的；

h） CII 范围内存在被植入后门、木马，或重要管理账号口令被窃取，导致 CII 范围内的服务器、运维管理终端、重要应用可被控的；

i） CII 范围内存在 g）和 h）情况以及存在 CII 核心设备被入侵，但未监测发现的；

j） 对重大预警信息未按应急预案要求及时进行排查且存在重大隐患的；

k） 未采用密码技术对 CII 核心业务、关键操作的通信保密性、完整性进行保护的；

l） CII 对外服务存在可被利用的已公开高危漏洞的；

m） CII 中重要业务数据、个人信息可被任意读取，或重要信息、关键操作指令可被篡改的；

n） 大量敏感数据被暴露在互联网的；

o） 未经出境评估将重要数据存储在中国境外的；

p） 业务逻辑安全设计存在重大缺陷和漏洞的；

q） 未按要求定期开展 CII 安全检测评估的；

r） 1 年内出现 2 起及以上瞒报、漏报、谎报重大网络安全事件的；

s） 未将网络安全事件纳入考核机制的；

t） 在有关部门组织的安全相关专项工作中发现有突出问题和较大安全隐患的；

u） 等级测评、风险评估、密码应用安全性评估、数据安全评估结果中有高风险安全问题的；

v） 经评估一致认为会对 CII 安全稳定运行有严重风险隐患的。