ICS 35.030
CSS L 80

中华人民共和国国家标准

GB/T 39204—2022

信息安全技术
关键信息基础设施安全保护要求

Information security technology—
Cybersecurity requirements for critical information infrastructure protection

2022-10-12 发布　　2023-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中央网信办网络安全协调局、公安部网络安全保卫局、中国电子技术标准化研究院、中国信息安全测评中心、国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心、公安部第三研究所、公安部第一研究所、北京赛西科技发展有限责任公司、中国信息安全研究院有限公司、国家工业信息安全发展研究中心、中国网络安全审查技术与认证中心、中国互联网络信息中心。

本文件主要起草人：杨建军、郭启全、郭涛、姚相振、王惠莅、祝国邦、范春玲、陈亮、宋璟、孙晓丽、周亚超、孙军、任卫红、李秋香、江典盛、袁静、宫月、任泽君、张新跃、上官晓丽、杨晨、王凤娇、程娜、马力、刘志磊、于东升、陈翠云、刘志宇、任望、魏军、黄元飞、王博、王姣、王秉政。

引　言

为落实《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》关于保护关键信息基础设施运行安全的要求，在国家网络安全等级保护制度基础上，借鉴我国相关部门在重要行业和领域开展网络安全保护工作的成熟经验，吸纳国内外在关键信息基础设施安全保护方面的举措，结合我国现有网络安全保障体系等成果，从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面，提出关键信息基础设施安全保护要求，采取必要措施保护关键信息基础设施业务连续运行，及其重要数据不受破坏，切实加强关键信息基础设施安全保护。

信息安全技术
关键信息基础设施安全保护要求

1 范围

本文件规定了关键信息基础设施分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面的安全要求。

本文件适用于指导运营者对关键信息基础设施进行全生存周期安全保护，也可供关键信息基础设施安全保护的其他相关方参考使用。

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 信息安全风险评估方法

GB/T 25069 信息安全技术 术语

3 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。

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，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。

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。

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。

4 安全保护基本原则

关键信息基础设施安全保护应在网络安全等级保护制度基础上，实行重点保护，应遵循以下基本原则。

——以关键业务为核心的整体防控。关键信息基础设施安全保护以保护关键业务为目标，对业务所涉及的一个或多个网络和信息系统进行体系化安全设计，构建整体安全防控体系。

——以风险管理为导向的动态防护。根据关键信息基础设施所面临的安全威胁态势进行持续监测和安全控制措施的动态调整，形成动态的安全防护机制，及时有效地防范应对安全风险。

——以信息共享为基础的协同联防。积极构建相关方广泛参与的信息共享、协同联动的共同防护机制，提升关键信息基础设施应对大规模网络攻击能力。

5 主要内容及活动

关键信息基础设施安全保护包括分析识别、安全防护、检测评估、监测预警、主动防御、事件处置六个方面。

a) 分析识别：围绕关键信息基础设施承载的关键业务，开展业务依赖性识别、关键资产识别、风险识别等活动。本活动是开展安全防护、检测评估、监测预警、主动防御、事件处置等活动的基础。

b) 安全防护：根据已识别的关键业务、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、安全运维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。

c) 检测评估：为检验安全防护措施的有效性，发现网络安全风险隐患，应建立相应的检测评估制度，确定检测评估的流程及内容等，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) 监测预警：建立并实施网络安全监测预警和信息通报制度，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) 主动防御：以应对攻击行为的监测发现为基础，主动采取收敛暴露面、捕获、溯源、干扰和阻断等措施，开展攻防演习和威胁情报工作，提升对网络威胁与攻击行为的识别、分析和主动防御能力。

f) 事件处置：运营者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。

6 分析识别

6.1 业务识别

业务识别要求包括：

a) 应识别本组织的关键业务和与其相关联的外部业务；

b) 应分析本组织关键业务对外部业务的依赖性；

c) 应分析本组织关键业务对外部业务的重要性；

d) 应梳理关键业务链，明确支撑关键业务的关键信息基础设施分布和运营情况。

6.2 资产识别

资产识别要求包括：

a) 应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。

6.3 风险识别

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。

6.4 重大变更

在关键信息基础设施发生改建、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。

注：保护工作部门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主管部门、监督管理部门，也是负责关键信息基础设施安全保护工作的部门。

7 安全防护

7.1 网络安全等级保护

应落实国家网络安全等级保护制度相关要求，开展网络和信息系统的定级、备案、安全建设整改和等级测评等工作。

7.2 安全管理制度

安全管理制度要求包括：

a) 应制定适合本组织的网络安全保护计划，明确关键信息基础设施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，支撑关键信息基础设施安全保护工作。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。

b) 应建立管理制度和安全策略，重点考虑基于关键业务链安全需求，并根据关键信息基础设施面临的安全风险和威胁的变化进行相应调整。

注1：安全策略包括但不限于：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、安全运维策略等。

注2：管理制度包括但不限于：风险管理制度、网络安全考核及监督问责制度、网络安全教育培训制度、人员管理制度、业务连续性管理及容灾备份制度、三同步制度（安全措施同步规划、同步建设和同步使用）、供应链安全管理制度等。

7.3 安全管理机构

安全管理机构要求包括：

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，专职管理或分管关键信息基础设施安全保护工作；

b) 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，建立并实施网络安全考核及监督问责机制；

c) 应为每个关键信息基础设施明确一名安全管理责任人；

d) 应将安全管理机构人员纳入本组织信息化决策体系。

7.4 安全管理人员

安全管理人员要求包括：

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。安全管理机构明确关键岗位，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。关键岗位应配备专人，并配备 2 人以上共同管理。

b) 应定期安排安全管理机构人员参加国家、行业或业界网络安全相关活动，及时获取网络安全动态。

c) 应建立网络安全教育培训制度，定期开展网络安全教育培训和技能考核，关键信息基础设施从业人员每人每年教育培训时长不得少于 30 个学时。教育培训内容应包括网络安全相关法律法规、政策标准，以及网络安全保护技术、网络安全管理等。

d) 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。应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施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。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。

e) 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。

7.5 安全通信网络

7.5.1 网络架构

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。

7.5.2 互联安全

互联安全要求包括：

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：在通信前基于密码技术对通信的双方进行验证或鉴别。

7.5.3 边界防护

边界防护要求包括：

a) 应对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互操作、数据交换和信息流向进行严格控制；

b) 应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。

7.5.4 安全审计

应采取网络审计措施，监测、记录系统运行状态、日常操作、故障维护、远程运维等，留存相关日志数据不少于 6 个月。

7.6 安全计算环境

7.6.1 鉴别与授权

鉴别与授权要求包括：

a) 应明确重要业务操作、重要用户操作或异常用户操作行为，并形成清单；
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，或者采用多因子身份鉴别等方式；
c) 针对重要业务数据资源的操作，应基于安全标记等技术实现访问控制。

7.6.2 入侵防范

入侵防范要求包括：
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) 应采取技术手段，实现系统主动防护，及时识别并阻断入侵和病毒行为。

7.6.3 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，应在经过验证后及时修补。

7.7 安全建设管理

应在关键信息基础设施建设、改造、升级等环节，实现网络安全技术措施与关键信息基础设施主体工程同步规划、同步建设、同步使用，并采取测试、评审、攻防演练等多种形式验证。必要时，可建设关键业务的仿真验证环境，予以验证。

7.8 安全运维管理

安全运维管理要求包括：
a) 应保证关键信息基础设施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；
b) 应在运维前与维护人员签订安全保密协议；
c) 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。

7.9 供应链安全保护

供应链安全保护要求包括：
a) 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。建立供应链安全管理制度，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) 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。
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) 应建立和维护合格供应方目录。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。
e) 应强化采购渠道管理，保持采购的网络产品和服务来源的稳定或多样性。
f) 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。
g) 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。

h) 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。
i) 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。
j) 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。
k) 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，涉及重大风险的应按规定向相关部门报告。

7.10 数据安全防护

数据安全防护要求包括：

a) 应建立数据安全管理责任和评价考核制度，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) 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。
d) 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、脱敏、去标识化等技术手段保护敏感数据安全。
e) 应建立业务连续性管理及容灾备份机制，重要系统和数据库实现异地备份。
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，确保关键信息基础设施一旦被破坏，可及时进行恢复和补救。
g) 应在关键信息基础设施退役废弃时，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。

8 检测评估

8.1 制度

应建立健全关键信息基础设施安全检测评估制度，包括但不限于检测评估流程、方式方法、周期、人员组织、资金保障等。

8.2 方式和内容

方式和内容要求包括：

a) 应自行或者委托网络安全服务机构对关键信息基础设施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关键信息基础设施安全检测评估，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，尤其关注关键信息基础设施跨系统、跨区域间的信息流动，及其资产的安全防护

情况；

d) 在关键信息基础设施发生改建、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，评估上述变更给关键信息基础设施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，检测关键信息基础设施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 监测预警

9.1 制度

制度要求包括：

a) 应建立并落实常态化监测预警、快速响应机制。制定自身的监测预警和信息通报制度，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，对关键信息基础设施的安全风险进行监测预警。

b) 应关注国内外及行业关键信息基础设施安全事件、安全漏洞、解决方法和发展趋势，并对涉及的关键信息基础设施安全性进行研判分析，必要时发出预警。

c) 应建立关键信息基础设施的预警信息报告和响应处置程序，明确不同级别预警的报告、响应和处置流程。

d) 应建立通报预警及协作处置机制，建立和维护外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

e) 应建立与外部组织之间、与其他运营者之间，以及运营者内部管理人员、内部网络安全管理机构与内部其他部门之间的沟通与合作机制，定期召开协调会议，共同研判、处置网络安全问题。

f) 应建立网络安全信息共享机制，例如：建立与保护工作部门、同一关键信息基础设施的其他运营者、研究机构、网络安全服务机构、业界专家之间的沟通与合作机制，网络安全共享信息可以是漏洞信息、威胁信息、最佳实践、前沿技术等。当网络安全共享信息为漏洞信息时，应符合国家关于漏洞管理制度的要求。

9.2 监测

监测要求包括：

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，构建违规操作模型、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，分析关键信息基础设施的网络安全态势。关键信息基础设施跨组织、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（例如：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。

9.3 预警

预警要求包括：

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。例如：恶意代码防御机制、入侵检测设备或者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。

10 主动防御

10.1 收敛暴露面

收敛暴露面要求包括：

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，压缩互联网出口数量；

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

c) 不应在公共存储空间（例如：代码托管平台、文库、网盘等）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。

10.2 攻击发现和阻断

攻击发现和阻断要求包括：

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，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。

10.3 攻防演练

攻防演练要求包括：

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，关键信息基础设施跨组织、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，采取沙盘推演的方式进行攻防演练。
b) 应将关键信息基础设施核心供应链、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。

10.4 威胁情报

威胁情报要求包括：

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。

11 事件处置

11.1 制度

制度要求包括：

a) 应建立网络安全事件管理制度，明确不同网络安全事件的分类分级、不同类别和级别事件处置的流程等，制定应急预案等网络安全事件管理文档。事件处置制度应符合国家联防联控相关要求，及时将信息共享给相关方。
b) 应为网络安全事件处置提供相应资源，组织建立专门网络安全应急支撑队伍、专家队伍，保障安全事件得到及时有效处置。
c) 应按规定参与和配合相关部门开展的网络安全应急演练、应急处置、案件侦办等工作。

11.2 应急预案和演练

应急预案和演练要求包括：

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) 应对网络安全应急预案定期进行评估修订，并持续改进。
f) 应每年至少组织开展 1 次本组织的应急演练。关键信息基础设施跨组织、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。

11.3 响应和处置

11.3.1 事件报告

事件报告要求包括：

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。

11.3.2 事件处理和恢复

事件处理和恢复要求包括：

a） 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；

b） 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；

c） 在事件处理完成后，应采用手工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；

d） 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业务和信息系统遭受再次破坏、危害或故障；

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，并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。

11.3.3 事件通报

应及时将安全事件及其处置情况通报到可能受影响的部门和相关人员，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。

11.4 重新识别

应根据检测评估、监测预警、主动防御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。

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 20988—2007 信息安全技术 信息系统灾难恢复规范

[3] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

[4] GB/T 32914—2016 信息安全技术 信息安全服务提供方管理要求

[5] GB/T 32921—2016 信息安全技术 信息技术产品供应方行为安全准则

[6] GB/T 32924—2016 信息安全技术 网络安全预警指南

[7] 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,中华人民共和国主席令(第53号)].

[8] 关键信息基础设施安全保护条例(2021年4月27日国务院第133次常务会议通过,中华人民共和国国务院令第745号).

[9] 国家网络安全事件应急预案(2017年1月10日中央网络安全和信息化领导小组办公室〔2017〕4号文公布).

[10] 云计算服务安全评估办法(2019年7月2日国家互联网信息办公室 国家发展和改革委员会 工业和信息化部 财政部关于发布《云计算服务安全评估办法》的公告〔2019〕第2号).

[11] 网络安全审查办法(2020年4月13日国家互联网信息办公室等12部委〔2020〕第6号).

[12] 贯彻落实网络安全等保制度和关键信息基础设施安全保护制度的指导意见(2020年7月22日公安部公网安〔2020〕1960号文公布).

[13] 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).

[14] Framework for Improving Critical Infrastructure Cybersecurity,NIST,2018.

[15] NIST SP800-53 Rev.4;2013 Security and Privacy Controls for Federal Information Systems and Organizations.