中华人民共和国公安部

公网安〔2025〕2391号

关于印发《网络安全等级保护测评高风险判定实施指引（试行）》的通知

各省、自治区、直辖市网络安全等级保护工作协调小组办公室，各省、自治区、直辖市公安厅、局网络安全保卫总队、新疆生产建设兵团公安局网络安全保卫总队：

近期，我局先后印发《关于进一步做好网络安全等级保护有关工作的函》（公网安〔2025〕1001号）、《关于对网络安全等级保护有关工作事项进一步说明的函》（公网安〔2025〕1846号），指导各单位全面深入推进网络安全风险隐患排查以及保护工作方案制定等工作。为进一步推进重大网络安全风险隐患发现、整改等工作落实，规范和统一全国网络安全等级测评活动中关于网络安全高风险问题的判定准则，同时支撑各地公安机关开展日常网络安全重大风险隐患督办整改等工作，我局研究制定了《网络安全等级保护测评高风险判定实施指引（试行）》。现印发给你们，请结合工作实际参照执行。

附件：《网络安全等级保护测评高风险判定实施指引（试行）》

公安部十一局

2025年5月26日

附件

网络安全等级保护测评高风险判定实施指引（试行）

目　　次

网络安全等级保护测评高风险判定
实施指引（试行）

1 范围

本文件规定了网络安全等级保护测评中的安全通用要求和各类安全扩展要求的高风险判例。

本文件适用于网络安全等级保护测评、安全检查等活动。

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 2887—2011 计算机场地通用规范

GB 17859 计算机信息系统 安全保护等级划分准则

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2022 信息安全技术 术语

GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

GB/T 31168—2023 信息安全技术 云计算服务安全能力要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

GB 17859、GB/T 22239—2019、GB/T 25069—2022、GB/T 31168—2023和GB/T 35273—2020界定的以及下列术语和定义适用于本文件。

3.1

可被利用的高危安全漏洞

指可被攻击者用于进行网络攻击从而导致严重后果的漏洞，包括但不限于缓冲区溢出、权限提升、远程代码执行、严重逻辑缺陷、任意文件上传等。

4 缩略语

下列缩略语适用于本文件。

AP： 无线访问接入点（Wireless Access Point）

DDoS：分布式拒绝服务（Distributed Denial of Service）

E-mail：电子邮件（Electronic Mail）

FTP：文件传输协议（File Transfer Protocol）

IP：互联网协议（Internet Protocol）

LEAP：轻量级可扩展身份验证协议（Lightweight Extensible Authentication Protocol ）

MAC：媒体访问控制（Media Access Control）

Rlogin：远程登录命令（Rlogin）

SSID：服务集标识（Service Set Identifier ）

Telnet：远程终端协议（Telnet）

UPS：不间断电源（Uninterruptible Power Supply）

USB：通用串行总线（Universal Serial Bus）

VPN：虚拟专用网络（Virtual Private Network）

WAP：无线访问接入点（Wireless Access Point）

WEB：全球广域网/万维网（World Wide Web）
WEP：有线等效协议（Wired Equivalent Protocol）
WIDS：无线入侵检测系统（Wireless Intrusion Detection System）
WPA：无线局域网保护访问（Wi-Fi Protected Access）

5 概述

5.1 判例概述

本文件中每一个判例由标准要求、适用范围、问题描述、可能的缓解措施和风险评价构成。其中标准要求表述该条判例对应GB/T 22239—2019的具体要求条款；适用范围表述该条判例适用的定级对象等级；问题描述为不符合该条标准要求的可能问题场景，其中任一安全问题均可能导致定级对象面临高风险；可能的缓解措施则给出经综合风险分析可酌情缓解风险等级的其他安全措施；风险评价为该问题经可能的缓解措施后风险是否可酌情降低的分析及结果。

5.2 判定原则

网络安全等级保护测评过程中，针对等级测评结果中存在的所有安全问题，应采用风险分析的方法进行危害分析和风险等级判定，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业务信息安全和系统服务安全造成影响的程度，综合评价对定级对象造成的安全风险。

本文件基于以下判定原则，符合下列所列任意条件的安全问题均应判高风险：

——违反国家法律法规规定的相关要求；

——不符合或未实现GB/T 22239—2019中各等级关键安全要求及基本安全功能，且没有可缓解措施；

——存在高度可被利用，且对定级对象的业务信息安全和系统服务安全造成严重后果的安全问题。

5.3 场景释义

由于定级对象的应用场景、部署方式、面临威胁、防护措施各不相同，无法枚举，因此，本文件仅针对一般的应用系统场景给出应判为高风险的问题描述及可能的风险缓解措施，供测评人员在进行风险分析时参考。

各行业主管部门可基于本文件制定适合本行业系统特点的判定指引。测评人员可根据本文件内容，结合行业主管部门要求、系统特点、现有措施等综合进行风险分析。

对于本文件未涉及的问题场景及可能的风险缓解措施，或虽然不在指引明确的适用范围内，但确实可能产生安全隐患的情况，测评机构需结合实际情况，对安全问题所引发的风险等级做出客观判断。

6 安全通用要求高风险判例

6.1 安全物理环境

6.1.1 物理访问控制

6.1.1.1 机房出入口访问控制措施缺失

本判例包括以下内容：

a) 标准要求：机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：机房出入口无任何访问控制措施，例如未安装电子或机械门锁（包括机房大门处于未上锁状态），且机房门口无专人值守等。
d) 可能的缓解措施：所在机房的大楼处于受控区域，且机房门口设有专人值守的视频监控系统。
e) 风险评价：机房出入口无任何访问控制措施，但机房所在的大楼处于受控区域，机房门口设有专人值守的视频监控系统，可根据实际措施效果酌情降低风险等级。

6.1.2 防火

6.1.2.1 机房防火措施缺失

本判例包括以下内容：

a) 标准要求：机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：
   1) 机房无任何有效消防措施，例如无检测火情、感应报警设施，机房专用的手提式灭火器（二氧化碳、洁净气体等）等灭火设置已失效或无法正常使用等情况；
   2) 机房所采取的灭火系统或设备不符合国家的相关规定。
d) 可能的缓解措施：机房安排专人值守或机房内设置了专人值守的视频监控系统。
e) 风险评价：机房无有效消防措施或所采取的灭火系统或设备不符合国家的相关规定，但机房安排专人值守或机房内设置了专人值守的视频监控系统，可根据实际措施效果酌情降低风险等级。

6.1.3 电力供应

6.1.3.1 机房短期备用电力供应措施缺失

本判例包括以下内容：

a) 标准要求：应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
b) 适用范围：业务连续性要求高的第三级及以上定级对象。
c) 问题描述：
   1) 机房无短期备用电力供应设备，例如 UPS、柴油发电机、应急供电车等；
   2) 供应设备无法满足短期正常运行。
d) 可能的缓解措施：机房配备多路供电。
e) 风险评价：机房无短期备用电力供应设备或供应设备无法满足短期正常运行，但机房配备多路供电，可根据实际措施效果酌情降低风险等级。

   注：业务连续性要求高一般是指该网络或系统中断后，相关业务无法开展，对运营者或其他组织、社会秩序、公共利益造成较大影响的，如银行业务类系统、电力供应业务类系统等。（以下同）

6.1.3.2 机房应急供电措施缺失

本判例包括以下内容：

a) 标准要求：应提供应急供电设施。
b) 适用范围：业务连续性要求高的第四级定级对象。
c) 问题描述：
   1) 机房未配备应急供电设施，例如柴油发电机、应急供电车等；
   2) 应急供电设施不可用，无法满足定级对象正常运行需求。
d) 可能的缓解措施：采用多数据中心方式部署，且通过技术手段实现应用级灾备。
e) 风险评价：若机房未配备应急供电设施或机房应急供电设施不可用，但采用多数据中心方式部署，且通过技术手段实现应用级灾备，可根据实际措施效果酌情降低风险等级。

6.2 安全通信网络

6.2.1 网络架构

6.2.1.1 网络设备业务处理能力不足

本判例包括以下内容：

a) 标准要求：应保证网络设备的业务处理能力满足业务高峰期需要。
b) 适用范围：业务连续性要求高的第三级及以上定级对象。
c) 问题描述：网络设备、安全设备等网络链路上的关键设备性能无法满足高峰期需求。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.2.1.2 重要网络区域边界访问控制措施缺失

本判例包括以下内容：

a) 标准要求：应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：
   1) 重要网络区域部署在外部网络边界处；
   2) 重要网络区域与其他网络区域之间未采取任何有效的访问控制措施。
d) 可能的缓解措施：所有服务器配置并启用了访问控制策略。
e) 风险评价：
   1) 重要网络区域部署在外部网络边界处，无相应的缓解措施，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险；
   2) 重要网络区域与其他网络区域之间未采取任何有效的访问控制措施，但所有服务器均配置并启用了访问控制策略，可根据实际措施效果酌情降低风险等级。

6.2.1.3 关键线路和设备冗余措施缺失

本判例包括以下内容：

a) 标准要求：应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
b) 适用范围：业务连续性要求高的第三级及以上定级对象。
c) 问题描述：通信线路、关键网络设备、关键安全设备和关键计算设备无冗余措施。
d) 可能的缓解措施：系统采用多数据中心部署且实现应用级灾备。
e) 风险评价：通信线路、关键网络设备和关键计算设备无冗余措施，但应用系统采用多数据中心方式部署，且通过技术手段实现应用级灾备，可根据实际措施效果酌情降低风险等级。

6.2.2 通信传输

6.2.2.1 采用无加密措施的网络通道传输重要数据

本判例包括以下内容：

a) 标准要求：应采用密码技术保证通信过程中数据的保密性。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：采用无加密措施的网络通道传输鉴别数据、敏感个人信息或重要业务数据等。
d) 可能的缓解措施：
   1) 采取密码技术实现重要数据自身加密；
   2) 采用加密传输协议进行数据传输。
e) 风险评价：
   1) 采用无加密措施的网络通道传输鉴别数据、敏感个人信息或重要业务数据等重要数据，但重要数据自身采取密码技术实现加密，可根据实际措施效果酌情降低风险等级；
   2) 采用无加密措施的网络通道传输鉴别数据、敏感个人信息或重要业务数据等重要数据，但应用系统采用加密协议进行数据传输，如使用 HTTPS 协议进行业务访问及数据传输等，可根据实际措施效果酌情降低风险等级。

6.3 安全区域边界

6.3.1 边界防护

6.3.1.1 网络边界接入设备或端口不可控

本判例包括以下内容：

a) 标准要求：应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：
   1) 网络边界链路接入设备未配置明确的上联链路端口；
   2) 网络边界链路接入设备端口 IP 及路由策略不明确；

3) 网络边界链路接入设备未关闭不使用的端口。

d) 可能的缓解措施：网络边界配置严格的访问控制策略。

e) 风险评价：网络边界链路接入设备未配置明确的上联链路端口，或设备端口 IP 及路由策略不明确，或未关闭不使用的端口，但网络边界部署有访问控制措施，且配置了严格的访问控制策略，细粒度达到 IP、端口级别，可根据实际措施效果酌情降低风险等级。

6.3.1.2 无线网络管控措施缺失

本判例包括以下内容：

a) 标准要求：应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

b) 适用范围：第三级及以上定级对象。

c) 问题描述：内部重要网络与无线网络互联，且不通过任何受控的边界设备或边界设备访问控制策略设置不当。

d) 可能的缓解措施：对接入到无线网络的设备及用户进行有效管控（如 IP/MAC 绑定）或强身份认证。

e) 风险评价：内部重要网络与无线网络互联，且不通过任何受控的边界设备或边界设备访问控制策略设置不当。但网络中采取技术措施对接入到无线网络的设备及用户进行有效管控（如 IP/MAC 绑定）或强身份认证，可根据实际措施效果酌情降低风险等级。

6.3.2 访问控制

6.3.2.1 重要网络区域边界访问控制措施缺失或配置不当

本判例包括以下内容：

a) 标准要求：应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。

b) 适用范围：第二级及以上定级对象。

c) 问题描述：重要网络区域与其他网络区域之间（包括内部区域边界和外部区域边界）访问控制设备缺失或访问控制措施失效。

d) 可能的缓解措施：所有服务器配置并启用了访问控制策略。

e) 风险评价：重要网络区域与其他网络区域之间（包括内部区域边界和外部区域边界）访问控制设备缺失或访问控制措施失效，但所有服务器均配置并启用了访问控制策略，可根据实际措施效果酌情降低风险等级。

6.3.3 入侵防范

6.3.3.1 外部网络攻击防御措施缺失

本判例包括以下内容：

a) 标准要求：应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。

b) 适用范围：第二级及以上定级对象。

c) 问题描述：

1) 关键网络节点无任何网络攻击行为检测手段和防护手段；

2) 网络攻击行为检测措施的策略库/规则库半年及以上未更新。

d) 可能的缓解措施：所有主机设备部署入侵检测、防御措施，且策略库/规则库更新及时。

e) 风险评价：关键网络节点无任何网络攻击行为检测手段和防护手段或网络攻击行为检测措施的策略库/规则库半年及以上未更新。但所有主机操作系统部署入侵防范产品，且策略库/规则库更新及时，能够对攻击行为进行检测、阻断或限制，可根据实际措施效果酌情降低风险等级。

注：策略库/规则库的更新周期可根据部署环境、行业或设备特性缩短或延长。

6.3.3.2 内部网络攻击防御措施缺失

本判例包括以下内容：

a) 标准要求：应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。

b) 适用范围：第三级及以上定级对象。

c） 问题描述：
1） 关键网络节点无任何网络攻击行为检测手段和防护手段；
2） 网络攻击行为检测措施的策略库/规则库半年及以上未更新。
d） 可能的缓解措施：所有主机设备部署入侵检测、防御措施，且策略库/规则库更新及时。
e） 风险评价：关键网络节点无任何网络攻击行为检测手段和防护手段或网络攻击行为检测措施的策略库/规则库半年及以上未更新，但所有主机操作系统部署入侵防范产品，且策略库/规则库更新及时，能够对攻击行为进行检测、阻断或限制，可根据实际措施效果酌情降低风险等级。

注：策略库/规则库的更新周期可根据部署环境、行业或设备特性缩短或延长。

6.3.3.3 网络行为分析措施缺失

本判例包括以下内容：
a） 标准要求：应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。
b） 适用范围：关键行业的第三级及以上定级对象。
c） 问题描述：
1） 关键网络节点对新型网络攻击行为网络访问行为无任何分析手段，例如未部署抗 APT 系统、全流量分析系统、沙箱系统、具备行为分析功能的态势感知系统、威胁情报系统等；
2） 基于威胁情报、行为分析模型进行行为分析的安全措施，半年及以上未更新威胁情报库、事件分析模型，无法满足防护需求。
d） 可能的缓解措施：网络环境采取物理隔离或采取强逻辑强隔离措施，且具有物理访问控制措施和设备强准入控制措施。
e） 风险评价：关键网络节点对新型网络攻击行为无任何分析手段或基于威胁情报、行为分析模型进行行为分析的安全措施，或半年及以上未更新威胁情报库、事件分析模型，但对于与互联公共通信网络完全物理隔离或采取强逻辑隔离措施的系统，具有物理访问控制措施和设备强准入控制措施，可根据实际措施效果酌情降低风险等级。

6.4 安全计算环境

6.4.1 身份鉴别

6.4.1.1 存在空口令、弱口令、通用口令或无身份鉴别措施

本判例包括以下内容：
a） 标准要求：应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。
b） 适用范围：第二级及以上定级对象。
c） 问题描述：
1） 存在可登录的空口令账户、无身份鉴别措施或身份鉴别措施可被绕过等；
2） 存在可登录的弱口令账户，如长度在 6 位以下，或存在单个、相同、连续数字/字母/字符及常见字典等易猜测的口令；
3） 多个不同被测对象的管理账户口令相同、或同一被测对象中多个不同管理账户口令相同。
d） 可能的缓解措施：
1） 具有仅限本地登录，或具有登录地址限制、登录终端限制、物理位置限制等远程登录管控措施；
2） 采用不可绕过的两种或两种以上组合的身份鉴别措施。
e） 风险评价：
1） 存在可登录的空口令账户、弱口令账户、通用口令、以及无身份鉴别措施或身份鉴别措施可被绕过等情况时，但被测对象仅限本地访问，或具有登录地址限制、登录终端限制、物理位置限制等远程登录管控措施，可根据实际措施效果酌情降低风险等级；
2） 存在可登录的空口令账户、弱口令账户、通用口令、以及无身份鉴别措施或身份鉴别措施可被绕过等情况时，但被测对象采用两种或两种以上身份鉴别措施，可根据实际措施效果酌情降低风险等级。

6.4.1.2 鉴别信息明文传输

本判例包括以下内容：

a) 标准要求：当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：
   1) 鉴别信息以明文方式在网络环境中传输；
   2) 鉴别信息使用编码、隐藏等形式进行传输，但仍可以被还原出明文。
d) 可能的缓解措施：采用不可绕过的两种或两种以上组合的身份鉴别措施，仅获得口令无法成功登录。
e) 风险评价：鉴别信息以明文方式传输，或鉴别信息使用编码、隐藏等形式进行传输，但仍可以被还原出明文的，但采用不可绕过的两种或两种以上组合的身份鉴别措施，仅获得口令无法成功登录，可根据实际措施效果酌情降低风险等级。

6.4.1.3 未采用两种或两种以上组合身份鉴别技术

本判例包括以下内容：

a) 标准要求：应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：未采用两种或两种以上组合鉴别技术对用户进行身份鉴别。
d) 可能的缓解措施：
   1) 在登录和访问过程中，多次进行身份鉴别，且每次鉴别信息动态变化；
   2) 在完成重要业务操作前的不同阶段采用不同的鉴别方式进行身份鉴别；
   3) 仅限本地登录或具有带外管理等措施。
e) 风险评价：
   1) 未采用两种或两种以上组合鉴别技术对用户进行身份鉴别，但在登录和访问过程中，多次进行身份鉴别，且每次鉴别信息动态变化，可根据实际措施效果酌情降低风险等级；
   2) 未采用两种或两种以上组合鉴别技术对用户进行身份鉴别，但在完成重要业务操作前的不同阶段采用不同的鉴别方式进行身份鉴别，可根据实际措施效果酌情降低风险等级；
   3) 未采用两种或两种以上组合鉴别技术对用户进行身份鉴别，但仅限本地登录或具有带外管理等措施，可根据实际措施效果酌情降低风险等级。

6.4.2 访问控制

6.4.2.1 未重命名默认账户名且未修改默认口令

本判例包括以下内容：

a) 标准要求：应重命名或删除默认账户，修改默认账户的默认口令。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：存在公开的默认账户或默认口令，未重命名默认账户且未修改默认口令。
d) 可能的缓解措施：
   1) 采用不可绕过的两种或两种以上组合的身份鉴别措施，仅使用默认口令无法成功登录；
   2) 具有登录地址限制、登录终端限制、物理位置限制等远程登录管控措施，使用默认口令无法成功登录。
e) 风险评价：
   1) 存在公开的默认账户或默认口令，未重命名默认账户且未修改默认口令，但采用不可绕过的两种或两种以上组合的身份鉴别措施，仅使用默认口令无法成功登录，可根据实际措施效果酌情降低风险等级；
   2) 存在公开的默认账户和默认口令，未重命名默认账户且未修改默认口令，但具有登录地址限制、登录终端限制、物理位置限制等远程登录管控措施，仅使用默认口令无法成功登录，可根据实际措施效果酌情降低风险等级。

6.4.2.2 访问控制策略存在缺陷或不完善，存在越权访问可能

本判例包括以下内容：

a) 标准要求：应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：
   1) 业务应用系统/平台访问控制策略存在缺陷或不完善，可非授权访问系统功能模块或查看、操作其他用户的数据；
   2) 数据库管理系统访问控制策略存在缺陷或不完善，存在数据库的超级管理员权限被授予非数据库管理员用户、或数据库的默认超级管理员账户被用于非数据库管理用途；
   3) 操作系统访问控制策略存在缺陷或不完善，存在以操作系统超级管理员权限运行的数据库、中间件、应用程序等非操作系统级进程或服务。
d) 可能的缓解措施：具有仅限本地访问，或具有登录地址限制、登录终端限制、物理位置限制等远程访问管控措施，以及操作行为审计等监控措施。
e) 风险评价：业务应用系统/平台、数据库管理系统、操作系统等访问控制策略存在缺陷或不完善，存在越权访问可能，但具有仅限本地访问，或具有登录地址限制、登录终端限制、物理位置限制等远程访问管控措施，以及操作行为审计等监控措施，可根据实际措施效果酌情降低风险等级。

6.4.3 入侵防范

6.4.3.1 开启多余的系统服务、默认共享和高危端口

本判例包括以下内容：

a) 标准要求：应关闭不需要的系统服务、默认共享和高危端口。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：开启多余的系统服务、默认共享和高危端口，且可被远程访问。
d) 可能的缓解措施：
   1) 具有登录地址限制、登录终端限制、物理位置限制等远程访问管控措施，使得多余系统服务、默认共享和高危端口相关漏洞难以利用；
   2) 具有主机入侵检测或恶意代码检测等防护措施，相关检测和防护功能正常有效，使得多余系统服务、默认共享和高危端口相关漏洞难以利用。
e) 风险评价：
   1) 开启多余的系统服务、默认共享和高危端口，且可被远程访问，但具有登录地址限制、登录终端限制、物理位置限制等远程访问管控措施，使得多余系统服务、默认共享和高危端口相关漏洞难以利用，可根据实际措施效果酌情降低风险等级；
   2) 开启多余的系统服务、默认共享和高危端口，且可被远程访问，但具有主机入侵检测或恶意代码检测等防护措施，相关检测和防护功能正常有效，使得多余系统服务、默认共享和高危端口相关漏洞难以利用，可根据实际措施效果酌情降低风险等级。

6.4.3.2 存在可被利用的高危安全漏洞

本判例包括以下内容：

a) 标准要求：应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：
   1) 通过互联网管理或访问的系统或设备，存在外界披露的可被利用的高危安全漏洞；
   2) 通过非互联网等公共通信网络管理或访问的系统或设备，经测试验证确认存在缓冲区溢出、越权访问、远程代码执行等可被利用的高危安全漏洞。
d) 可能的缓解措施：
   1) 通过互联网管理或访问的系统或设备，存在外界披露的可被利用的高危安全漏洞，无缓解措施；

2) 通过非互联网等公共通信网络管理或访问的系统或设备，具有仅限本地访问，或具有登录地址限制、登录终端限制、物理位置限制等远程访问管控措施，使得高危漏洞难以利用；
3) 通过非互联网等公共通信网络管理或访问的系统或设备，具有主机入侵检测或恶意代码检测等防护措施，相关检测和防护功能正常有效，使得高危漏洞难以利用。

e) 风险评价：
1) 通过互联网管理或访问的系统或设备，存在外界披露的可被利用的高危安全漏洞，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险；
2) 通过非互联网等公共通信网络管理或访问的系统或设备，存在外界披露的可被利用的高危安全漏洞，但具有仅限本地访问，或具有登录地址限制、登录终端限制、物理位置限制等远程访问管控措施，使得高危漏洞难以利用，可根据实际措施效果酌情降低风险等级；
3) 通过非互联网等公共通信网络管理或访问的系统或设备，具有主机入侵检测或恶意代码检测等防护措施，相关检测和防护功能正常有效，使得高危漏洞难以利用，可根据实际措施效果酌情降低风险等级。

6.4.3.3 数据有效性检验功能缺失或不完善

本判例包括以下内容：

a) 标准要求：应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：未提供数据有效性检验功能或数据有效性校验功能不完善，存在 SQL 注入、跨站脚本、文件上传等造成严重后果的高风险安全漏洞。
d) 可能的缓解措施：
1) 不对互联网等公共通信网络提供服务，且具有仅限本地访问，或具有登录地址限制、登录终端限制、物理位置限制等远程访问管控措施，以及操作行为审计等技术措施，使得高风险安全漏洞难以利用；
2) 采用 WEB 应用防火墙、WEB 流量过滤、网页防篡改等技术措施进行防护，使得高风险安全漏洞难以利用。
e) 风险评价：
1) 未提供数据有效性检验功能或数据有效性校验功能不完善，存在 SQL 注入、跨站脚本、文件上传等造成严重后果的高风险安全漏洞，但由于不对互联网等公共通信网络提供服务，且具有仅限本地访问，或具有登录地址限制、登录终端限制、物理位置限制等远程访问管控措施，以及操作行为审计等技术措施，使得高风险安全漏洞难以利用，可根据实际措施效果酌情降低风险等级；
2) 未提供数据有效性检验功能或数据有效性校验功能不完善，存在 SQL 注入、跨站脚本、文件上传等造成严重后果的高风险安全漏洞，但采用 WEB 应用防火墙、WEB 流量过滤、网页防篡改等技术措施进行防护，使得高风险安全漏洞难以利用，可根据实际措施效果酌情降低风险等级。

6.4.4 恶意代码防范

6.4.4.1 恶意代码防范措施缺失

本判例包括以下内容：

a) 标准要求：应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库（第二级）；应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断（第三级）。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：
1) 未采取恶意代码检测和清除措施；
2) 恶意代码防范产品授权已过期；
3) 恶意代码特征库/规则库等一个月以上未更新。

d) 可能的缓解措施：
   1) 使用了 Linux、Unix、Solaris、CentOS、AIX、Mac 等非 Windows 操作系统的定级对象，且不对互联网等公共通信网络提供服务，具有 USB 介质管控、软件白名单、主机入侵检测、主机安全审计等技术措施；
   2) 使用了 Linux、Unix、Solaris、CentOS、AIX、Mac 等非 Windows 操作系统的定级对象，且在关键网络节点处采取了有效的恶意代码检测和清除的技术措施；
   3) 使用 Windows 操作系统的定级对象，未采取恶意代码检测和清除措施，或恶意代码防范产品授权已过期，或恶意代码特征库/规则库等一个月以上未更新，无缓解措施。
e) 风险评价：
   1) 未采取恶意代码检测和清除措施，或恶意代码防范产品授权已过期，或恶意代码特征库/规则库等一个月以上未更新，但使用了 Linux、Unix、Solaris、CentOS、AIX、Mac 等非 Windows 操作系统的定级对象，且不对互联网等公共通信网络提供服务，具有 USB 介质管控、软件白名单、主机入侵检测、主机安全审计等技术措施，可根据实际措施效果酌情降低风险等级；
   2) 未采取恶意代码检测和清除措施，或恶意代码防范产品授权已过期，或恶意代码特征库/规则库等一个月以上未更新，但使用了 Linux、Unix、Solaris、CentOS、AIX、Mac 等非 Windows 操作系统的定级对象，且在关键网络节点处采取了有效的恶意代码检测和清除的技术措施，可根据实际措施效果酌情降低风险等级；
   3) 未采取恶意代码检测和清除措施，或恶意代码防范产品授权已过期，或恶意代码特征库/规则库等一个月以上未更新，所使用的操作系统为 Windows 操作系统，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.4.5 数据保密性

6.4.5.1 重要数据明文传输

本判例包括以下内容：
a) 标准要求：应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：鉴别信息、重要个人信息或重要业务数据等以明文的方式在网络环境中传输。
d) 可能的缓解措施：
   1) 鉴别信息以明文的方式在网络环境中传输，但采用不可绕过的两种或两种以上组合的身份鉴别措施，获得鉴别信息无法成功登录；
   2) 重要个人信息或重要业务数据等以明文的方式在网络环境中传输，无缓解措施。
e) 风险评价：
   1) 鉴别信息以明文的方式在网络环境中传输，但采用不可绕过的两种或两种以上组合的身份鉴别措施，获得鉴别信息无法成功登录，可根据实际措施效果酌情降低风险等级；
   2) 重要个人信息或重要业务数据等以明文的方式在网络环境中传输，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.4.5.2 重要数据明文存储

本判例包括以下内容：
a) 标准要求：应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：鉴别信息、重要个人信息、具有保密性需求的重要业务数据以明文的方式存储。
d) 可能的缓解措施：
   1) 不对互联网等公共通信网络提供服务，且具有仅限本地访问或带外管理等措施；
   2) 具有数据库防火墙、数据防泄露等技术措施，相关防护功能和策略正确有效。
e) 风险评价：

1) 鉴别信息、重要个人信息、重要业务数据以明文的方式存储，但不对互联网等公共通信网络提供服务，且具有仅限本地访问或带外管理等措施，可根据实际措施效果酌情降低风险等级；
2) 鉴别信息、重要个人信息、重要业务数据以明文的方式存储，但具有数据库防火墙策略、数据防泄露等技术措施，相关防护功能和策略正确有效，可根据实际措施效果酌情降低风险等级。

6.4.6 数据备份恢复

6.4.6.1 重要数据无本地备份措施

本判例包括以下内容：
a) 标准要求：应提供重要数据的本地数据备份与恢复功能。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：
1) 重要数据未提供任何数据备份措施；
2) 重要数据备份到互联网网盘或相关存储环境。
d) 可能的缓解措施：
1) 采用多数据中心或冗余方式部署，重要数据存在多个可用副本；
2) 重要数据备份到互联网网盘或相关存储环境，无缓解措施。
e) 风险评价：
1) 重要数据未提供任何数据备份措施，但系统采用多数据中心或冗余方式部署，重要数据存在多个可用副本，可根据实际措施效果酌情降低风险等级；
2) 重要数据备份到互联网网盘或相关存储环境，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.4.6.2 数据处理系统冗余措施缺失

本判例包括以下内容：
a) 标准要求：应提供重要数据处理系统的热冗余，保证系统的高可用性。
b) 适用范围：业务连续性要求高的第三级及以上定级对象。
c) 问题描述：对于业务连续性要求较高的被测对象，处理重要数据的设备（如重要服务器、重要数据库管理系统等）未采用热冗余方式部署，发生故障后可能导致重要业务中断。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.4.6.3 无异地灾备措施

本判例包括以下内容：
a) 标准要求：应建立异地灾难备份中心，提供业务应用的实时切换。
b) 适用范围：业务连续性要求高的第四级及以上定级对象。
c) 问题描述：
1) 未设立异地应用级容灾中心；
2) 异地应用级容灾中心无法实现业务切换。
d) 可能的缓解措施：无。
e) 风险评价：上述任一安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.4.7 个人信息保护

6.4.7.1 违规采集和存储个人信息

本判例包括以下内容：
a) 标准要求：应仅采集和保存业务必需的用户个人信息。
b) 适用范围：第二级及以上定级对象。

c） 问题描述：系统在未授权情况下，违规采集、存储用户个人隐私信息，或法律法规、主管部门严令禁止采集、保存的个人信息。
d） 可能的缓解措施：无。
e） 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.4.7.2 违规访问和使用个人信息

本判例包括以下内容：
a） 标准要求：应禁止未授权访问和非法使用用户个人信息。
b） 适用范围：第二级及以上定级对象。
c） 问题描述：未按国家相关法律法规、政策标准、以及行业主管部门要求等相关规定使用个人信息，包括但不限于在未授权情况下将用户信息提交给第三方处理、未脱敏的个人信息用于其他非核心业务系统或测试环境、非法交易、泄漏用户个人信息等、未严格控制个人信息查询及导出权限等。
d） 可能的缓解措施：无。
e） 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.5 安全管理中心

6.5.1 集中管控

6.5.1.1 远程管理路径安全防护措施不足

本判例包括以下内容：
a） 标准要求：应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
b） 适用范围：第三级及以上定级对象。
c） 问题描述： 对网络设备、安全设备或安全组件进行远程管理时，未采取安全的信息传输路径。
d） 可能的缓解措施：无。
e） 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.5.1.2 审计记录存储时间不满足要求

本判例包括以下内容：
a） 标准要求：应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。
b） 适用范围：第三级及以上定级对象。
c） 问题描述：网络设备、安全设备、主机设备（包括操作系统、数据库等）及应用系统的重要操作、安全事件等审计记录留存不满足法律法规规定的相关要求（不少于六个月）。
d） 可能的缓解措施：无。
e） 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。
注：对于定级对象上线运行时间不足六个月，可从当前日志保存情况、日志备份策略、日志存储容量等角度进行分析，如被测评系统有能力将日志数据存储六个月以上，则认为其符合安全要求。

6.6 安全管理制度

6.6.1 管理制度

6.6.1.1 管理制度缺失

本判例包括以下内容：
a） 标准要求：应对安全管理活动中的各类管理内容建立安全管理制度。
b） 适用范围：第三级及以上定级对象。
c） 问题描述：
1） 未建立任何与安全管理活动相关的管理制度；
2） 相关管理制度无法适用于当前定级对象。
d） 可能的缓解措施：无。

e) 风险评价：上述任一安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.7 安全管理机构

6.7.1 岗位设置

6.7.1.1 未建立网络安全工作领导机构

本判例包括以下内容：

a) 标准要求：应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：未成立指导和管理网络安全工作的委员会或领导小组。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.8 安全管理人员

6.8.1 外部人员访问管理

6.8.1.1 外部人员接入网络管理措施缺失

本判例包括以下内容：

a) 标准要求：应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：管理制度中未明确外部人员接入受控网络访问系统的申请、审批流程以及相关安全控制要求且无法提供外部人员接入申请、审批等相关记录。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.9 安全建设管理

6.9.1 产品采购和使用

6.9.1.1 违规采购和使用网络安全产品

本判例包括以下内容：

a) 标准要求：应确保网络安全产品采购和使用符合国家的有关规定。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：网络安全产品的采购和使用违反国家有关规定（2023 年 7 月 1 日起采购并使用的网络安全专用产品不在《网络关键设备和网络安全专用产品目录》中；或 2023 年 7 月 1 日前采购并使用未获得《计算机信息系统安全专用产品销售许可证》或国家信息安全产品认证证书的网络安全产品）。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.9.2 外包软件开发

6.9.2.1 外包软件开发代码审计措施缺失

本判例包括以下内容：

a) 标准要求：应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：未对重要业务系统进行源代码安全审计，且开发单位未提供任何第三方机构提供的安全性检测证明。
d) 可能的缓解措施：

1) 定期进行软件源代码安全审计，并能够提供安全审计报告，且当前管理制度中明确规定外包开发代码需进行代码审计；
2) 通过合同等方式与开发单位明确安全责任并采取相关技术手段进行防控。

e) 风险评价：
1) 若未对重要业务系统进行源代码安全审计，且开发单位未提供任何第三方机构提供的安全性检测证明，但定期进行软件源代码安全审计，并能够提供安全审计报告，且当前管理制度中明确规定外包开发代码需进行审计，可根据实际措施效果酌情降低风险等级；
2) 若未对重要业务系统进行源代码安全审计，且开发单位未提供任何第三方机构提供的安全性检测证明，但通过合同等方式与开发单位明确安全责任并采取相关技术手段进行防控，可根据实际措施效果酌情降低风险等级。

6.9.3 测试验收

6.9.3.1 上线前未开展安全测试

本判例包括以下内容：

a) 标准要求：应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

b) 适用范围：第三级及以上定级对象。

c) 问题描述：
1) 系统上线前未开展任何安全性测试；
2) 未对测试发现的高风险问题进行安全整改。

d) 可能的缓解措施：
1) 系统上线前未开展任何安全性测试，上线后定期开展安全检测，且检测未发现高危风险；
2) 未对测试发现的高风险问题进行安全整改，无缓解措施。

e) 风险评价：
1) 系统上线前未开展任何安全性测试，但系统上线后定期开展安全检测，检测未发现高危风险，可根据实际措施效果酌情降低风险等级；
2) 系统未对测试发现的高风险问题进行安全整改，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.9.4 等级测评

6.9.4.1 未定期进行等级测评

本判例包括以下内容：

a) 标准要求：应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。

b) 适用范围：第三级及以上定级对象。

c) 问题描述：系统定级备案后，未每年开展一次等级测评，且上次测评发现的高风险问题未及时整改。

d) 可能的缓解措施：无。

e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.9.4.2 选择的测评机构不符合国家相关要求

本判例包括以下内容：

a) 标准要求：应确保测评机构的选择符合国家有关规定。

b) 适用范围：第三级及以上定级对象。

c) 问题描述：
1) 选择的测评机构不符合国家相关要求；
2) 选择被通报处理的测评机构（包括认证证书暂停和整改期内）开展等级测评。

d) 可能的缓解措施：无。

e) 风险评价：上述任一安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.10 安全运维管理

6.10.1 应急预案管理

6.10.1.1 未制定重要事件应急预案

本判例包括以下内容：

a) 标准要求：应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：
   1) 未制定重要事件的应急预案；
   2) 应急预案内容不完整，未明确重要事件的应急处理流程、恢复流程等内容。
d) 可能的缓解措施：无。
e) 风险评价：上述任一安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

6.10.1.2 未定期开展应急预案培训和演练

本判例包括以下内容：

a) 标准要求：应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：未定期（至少每年一次）对相关人员进行应急预案培训，且未根据不同的应急预案进行应急演练。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7 云计算安全扩展要求高风险判例

7.1 安全物理环境

7.1.1 物理位置选择

7.1.1.1 云计算基础设施位于中国境外

本判例包括以下内容：

a) 标准要求：应保证云计算基础设施位于中国境内。
b) 适用范围：第二级及以上云计算平台。
c) 问题描述：由硬件资源和资源抽象控制组件构成的支撑云计算的基础设施不在中国境内。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.2 安全通信网络

7.2.1 网络架构

7.2.1.1 云计算平台承载高于其安全保护等级的业务系统

本判例包括以下内容：

a) 标准要求：应保证云计算平台不承载高于其安全保护等级的业务应用系统。
b) 适用范围：第二级及以上云计算平台。
c) 问题描述：云计算平台承载高于其安全保护等级（SXAY）的业务应用系统。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.2.1.2 云计算平台虚拟网络隔离措施缺失

本判例包括以下内容：

a) 标准要求：应实现不同云服务客户虚拟网络之间的隔离。

b) 适用范围：第二级及以上云计算平台。
c) 问题描述：云计算平台未采取网络隔离技术实现不同云服务客户虚拟网络之间的隔离。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.2.1.3 未单独划分独立的资源池

本判例包括以下内容：
a) 标准要求：应为第四级业务应用系统划分独立的资源池。
b) 适用范围：第四级云计算平台。
c) 问题描述：云计算平台未为第四级业务应用系统划分独立的物理计算资源池和存储资源池。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.2.1.4 云计算平台未提供安全防护能力

本判例包括以下内容：
a) 标准要求：应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。
b) 适用范围：第二级及以上云计算平台。
c) 问题描述：云计算平台无法提供满足云服务客户业务需要的通信传输、边界防护、入侵防范等安全机制。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.3 安全区域边界

7.3.1 访问控制

7.3.1.1 虚拟化网络边界访问控制措施缺失

本判例包括以下内容：
a) 标准要求：应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。
b) 适用范围：第二级及以上云计算平台和云服务客户系统。
c) 问题描述：
   1) 云计算平台未在不同云服务客户系统的虚拟网络之间的边界部署访问控制措施；
   2) 云服务客户系统未在虚拟网络中的不同虚拟子网/区域之间的边界、虚拟网络与外部网络之间的边界部署访问控制措施。
d) 可能的缓解措施：云服务客户系统在所有服务器均配置并启用了访问控制策略。
e) 风险评价：
   1) 云计算平台未在不同云服务客户的虚拟网络之间的边界部署访问控制措施，无相应的缓解措施，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险；
   2) 云服务客户系统未在虚拟网络中的不同虚拟子网/区域之间的边界、虚拟网络与外部网络之间的边界部署访问控制措施，但所有服务器均配置并启用了访问控制策略，可根据实际措施效果酌情降低风险等级。

7.3.2 入侵防范

7.3.2.1 云计算平台网络攻击防御措施缺失

本判例包括以下内容：
a) 标准要求：应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
b) 适用范围：第三级及以上云计算平台。
c) 问题描述：

1） 云计算平台对云服务客户发起的网络攻击行为无任何检测手段；
2） 网络攻击行为检测措施的策略库/规则库半年及以上未更新。

d） 可能的缓解措施：所有主机设备部署入侵检测、防御措施，且策略库/规则库更新及时。

e） 风险评价：云计算平台对云服务客户发起的网络攻击行为无任何检测手段或者网络攻击行为检测措施的策略库/规则库半年及以上未更新，但所有主机操作系统部署入侵防范产品，且策略库/规则库更新及时，能够对攻击行为进行检测、阻断或限制，可根据实际措施效果酌情降低风险等级。

7.4 安全计算环境

7.4.1 镜像和快照保护

7.4.1.1 镜像和快照保护措施缺失

本判例包括以下内容：

a） 标准要求：应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。

b） 适用范围：第三级及以上云计算平台。

c） 问题描述：云计算平台虚拟机镜像、快照未加密或访问控制技术手段缺失，可对镜像或快照等敏感资源进行非法访问。

d） 可能的缓解措施：无。

e） 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.4.2 数据完整性和保密性

7.4.2.1 云服务客户数据、个人信息违规出境

本判例包括以下内容：

a） 标准要求：应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。

b） 适用范围：第二级及以上云计算平台。

c） 问题描述：云服务客户数据、用户个人信息等数据存储在境外，且出境未遵循国家相关规定。

d） 可能的缓解措施：无。

e） 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.4.3 数据备份恢复

7.4.3.1 云服务客户未在本地保存业务数据的备份

本判例包括以下内容：

a） 标准要求：云服务客户应在本地保存其业务数据的备份。

b） 适用范围：第二级及以上云服务客户系统。

c） 问题描述：云服务客户在云计算平台同一区域内保存其业务数据的备份。

d） 可能的缓解措施：云服务客户将业务数据备份保存至所在云计算平台的不同区域或不同云计算平台。

e） 风险评价：云服务客户在云计算平台同一区域内保存其业务数据的备份，但将业务数据的备份保存至所在云计算平台的不同区域或不同云计算平台，可根据实际措施效果酌情降低风险。

7.4.3.2 未提供云计算平台迁移技术手段

本判例包括以下内容：

a） 标准要求：应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

b） 适用范围：第二级及以上云计算平台。

c） 问题描述：无相关技术措施配合云服务客户迁移业务系统及数据。

d） 可能的缓解措施：无。

e） 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.4.4 剩余信息保护

7.4.4.1 云服务客户删除业务应用数据时，云计算平台未删除所有副本

本判例包括以下内容：

a） 标准要求：云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。
b） 适用范围：第二级及以上云计算平台。
c） 问题描述：云服务客户删除业务应用数据或解除存储资源使用后，云服务商无任何存储数据清除手段，可以对删除数据进行恢复。
d） 可能的缓解措施：无。
e） 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.5 安全管理中心

7.5.1 集中管控

7.5.1.1 云计算平台管理流量与云服务客户业务流量未分离

本判例包括以下内容：

a） 标准要求：应保证云计算平台管理流量与云服务客户业务流量分离。
b） 适用范围：第三级及以上云计算平台。
c） 问题描述：云服务商未对云计算平台中的信息流进行梳理，管理流量和客户业务流量未分离。
d） 可能的缓解措施：云计算平台设置严格的访问控制措施，不能访问云服务客户业务流量。
e） 风险评价：云计算平台管理流量与云服务客户业务流量未分离，但云计算平台设置严格的访问控制措施，可根据实际措施效果酌情降低风险等级。

7.6 安全建设管理

7.6.1 云服务商选择

7.6.1.1 云服务客户选择服务商不合规

本判例包括以下内容：

a） 标准要求：应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。
b） 适用范围：第二级及以上云服务客户系统。
c） 问题描述：云服务客户未选择具有相应等级安全保护能力的云计算平台（如云计算平台安全保护等级低于云服务客户系统、未进行等级保护测评、测评报告超出有效期或者等级保护测评结论为差等）。
d） 可能的缓解措施：无。
e） 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.6.2 供应链管理

7.6.2.1 供应商的选择不符合国家有关规定

本判例包括以下内容：

a） 标准要求：应确保供应商的选择符合国家有关规定。
b） 适用范围：第三级及以上云计算平台。
c） 问题描述：
   1） 云服务商未采取任何供应链保护措施，未对供应商进行筛选，并建立合格供应商列表；
   2） 云服务商的供应商中存在严重违法违规行为；
   3） 政务云云计算平台关键产品或服务的供应商来自境外。
d） 可能的缓解措施：无。
e） 风险评价：上述任一安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

7.7 安全运维管理

7.7.1 云计算环境管理

7.7.1.1 云计算平台运维地点不位于中国境内，且运维操作未遵循国家相关规定

本判例包括以下内容：

a) 标准要求：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。
b) 适用范围：第二级及以上云计算平台。
c) 问题描述：云计算平台的运维地点不位于中国境内，境外对境内云计算平台实施运维操作未遵循国家相关规定。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

8 移动互联安全扩展要求高风险判例

8.1 安全物理环境

8.1.1 无线接入点的物理位置

8.1.1.1 无线接入点过度覆盖

本判例包括以下内容：

a) 标准要求：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。
b) 适用范围：第四级及以上定级对象。
c) 问题描述：
   1) 未根据无线信号强度、范围和干扰设计接入位置、强度，造成无线信号过度覆盖，外部区域未授权访问无线网络；
   2) 未使用法拉第笼或白噪音方式等在无线网络覆盖范围内进行无线信号屏蔽。
d) 可能的缓解措施：采用 MAC 地址过滤等方式对无线接入设备进行准入控制。
e) 风险评价：
   1) 未根据无线信号强度、范围和干扰设计接入位置、强度，造成无线信号过度覆盖，但采用 MAC 地址过滤等方式对无线接入设备进行准入控制，可根据实际措施效果酌情降低风险等级；
   2) 在无线网络覆盖范围内未使用法拉第笼或白噪音方式等进行无线信号屏蔽，但采用 MAC 地址过滤等方式对无线接入设备进行准入控制，可根据实际措施效果酌情降低风险等级。

8.2 安全区域边界

8.2.1 边界防护

8.2.1.1 有线网络与无线网络边界防护缺失

本判例包括以下内容：

a) 标准要求：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：有线网络与无线网络边界之间未部署无线接入网关设备，不能对无线接入进行统一管理。
d) 可能的缓解措施：对接入到无线网络的设备及用户进行有效管控（如 IP/MAC 绑定）或强身份认证。
e) 风险评价：有线网络与无线网络边界之间未部署无线接入网关设备，不能对无线接入进行统一管理，但网络中采取技术措施对接入到无线网络的设备及用户进行有效管控（如 IP/MAC 绑定）或强身份认证，可根据实际措施效果酌情降低风险等级。

8.2.2 访问控制

8.2.2.1 无线接入设备认证功能缺失

本判例包括以下内容：

a) 标准要求：无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：无线接入设备未开启接入认证功能，不能认证无线接入设备。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

8.2.3 入侵防范

8.2.3.1 无线接入设备高风险功能开启

本判例包括以下内容：

a) 标准要求：应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：
   1) 未禁用 SSID 的默认广播，且未使用基于 WPA2 或 WPA3 的身份认证和加密解决方案；
   2) 使用基于 WEP 的身份认证方案，基于密钥长度较短的 RC4 算法，采用重复使用的 IV 向量；
   3) 使用基于 LEAP 的身份认证协议，且未使用复杂密码；
   4) 未禁用默认启用的 WPS 功能，或 WPS 关闭功能无效或无法关闭。
d) 可能的缓解措施：
   1) 使用 MAC 过滤器进行移动设备授权访问；
   2) 使用 WIDS 对无线接入设备和无线接入网关存在风险的功能进行扫描，并对相关设备进行监测。
e) 风险评价：
   1) 无线接入设备和无线接入网关未禁用 SSID 的默认广播、WPS 功能，使用 WEP 的身份认证、LEAP 的身份认证协议等，但使用了 MAC 过滤器进行移动设备授权访问，可根据实际措施效果酌情降低风险等级；
   2) 无线接入设备和无线接入网关未禁用 SSID 的默认广播、WPS 功能，使用 WEP 的身份认证、LEAP 的身份认证协议等，但使用了 WIDS 对无线接入设备和无线接入网关存在风险的功能进行扫描，并对相关设备进行监测，可根据实际措施效果酌情降低风险等级。

8.2.3.2 多个 AP 使用相同简单认证密钥

本判例包括以下内容：

a) 标准要求：应禁止多个 AP 使用同一个认证密钥。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：多个 AP 使用相同简单认证密钥。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

8.2.3.3 无法检测到针对无线接入设备的网络攻击行为

本判例包括以下内容：

a) 标准要求：应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密码破解、中间人攻击和欺骗攻击等行为。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：无法检测到针对无线接入设备的网络扫描、DDoS 攻击、密码破解、中间人攻击和欺骗攻击等行为。
d) 可能的缓解措施：移动终端部署终端管控软件，能够发现终端异常操作行为，且策略库/规则库及时更新。

e) 风险评价：无法检测到针对无线接入设备的网络扫描、DDoS 攻击、密码破解、中间人攻击和欺骗攻击等行为，但在移动终端部署终端管控软件，能够发现终端异常操作行为，且策略库/规则库及时更新，可根据实际措施效果酌情降低风险等级。

8.3 安全计算环境

8.3.1 移动应用管控

8.3.1.1 移动终端安装未经指定证书签名的应用软件

本判例包括以下内容：

a) 标准要求：应只允许指定证书签名的应用软件安装和运行。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：移动终端未在应用软件安装和运行前验证软件完整性。
d) 可能的缓解措施：移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。
e) 风险评价：移动终端未在应用软件安装和运行前验证软件完整性，但移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名，可根据实际措施效果酌情降低风险等级。

8.3.1.2 移动终端安装有高风险恶意软件

本判例包括以下内容：

a) 标准要求：应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：移动终端未采用白名单方式进行终端应用软件安装、运行控制。
d) 可能的缓解措施：移动终端采用管理流程进行终端应用软件安装、运行审批管理。
e) 风险评价：移动终端未采用白名单方式进行终端应用软件安装、运行控制，但采用管理流程进行终端应用软件安装、运行审批管理，可根据实际措施效果酌情降低风险等级。

8.4 安全建设管理

8.4.1 移动应用软件采购

8.4.1.1 未知渠道应用软件安装

本判例包括以下内容：

a) 标准要求：应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：
   1) 移动终端安装、运行的应用软件来自第三方应用商店或其他未知渠道；
   2) 无应用软件签名机制，以及安装和运行前证书签名验证机制。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

8.4.1.2 安装使用未经安全评估的开源软件

本判例包括以下内容：

a) 标准要求：应保证移动终端安装、运行的应用软件由指定的开发者开发。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：未从官方渠道获取稳定版本开源软件，且未对开源代码和应用程序进行安全评估检测。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

9 物联网安全扩展要求高风险判例

9.1 安全物理环境

9.1.1 感知节点设备物理防护

9.1.1.1 感知节点设备所处物理环境对感知节点造成物理破坏

本判例包括以下内容：

a) 标准要求：感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：物联网感知节点设备所处的物理环境对设备造成物理破坏，影响设备正常工作。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

9.2 安全区域边界

9.2.1 接入控制

9.2.1.1 非授权感知节点设备能够接入网络中

本判例包括以下内容：

a) 标准要求：应保证只有授权的感知节点可以接入。
b) 适用范围：第二级及以上定级对象。
c) 问题描述：感知节点设备（例如感知节点接入网关、传感器等设备）未经授权可以接入网络。
d) 可能的缓解措施：无。
e) 风险评价：上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

9.3 安全计算环境

9.3.1 感知节点设备安全

9.3.1.1 非授权用户可对感知节点设备的软件应用进行配置或变更

本判例包括以下内容：

a) 标准要求：应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：感知节点设备未配置访问控制措施或访问控制措施无效，非授权用户可对感知节点设备的软件应用进行配置或变更。
d) 可能的缓解措施：感知节点设备所处物理环境具有访问控制措施。
e) 风险评价：感知节点设备未配置访问控制措施或访问控制措施无效，非授权用户可对感知节点设备的软件应用进行配置或变更，但感知设备所处物理环境具有访问控制措施，可根据实际措施效果酌情降低风险等级。

9.3.2 网关节点设备安全

9.3.2.1 网关节点设备连接无身份鉴别措施

本判例包括以下内容：

a) 标准要求：应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：网关节点设备对合法连接设备（包括终端节点、路由节点、数据处理中心）无任何身份鉴别措施。
d) 可能的缓解措施：网关节点设备具有设备连接管控措施、物理访问控制等措施。
e) 风险评价：网关节点设备对合法连接设备（包括终端节点、路由节点、数据处理中心）无任何身份鉴别措施，但网关节点设备具有设备连接管控措施、物理访问控制等措施，可根据实际措施效果酌情降低风险等级。

10 工业控制系统安全扩展要求高风险判例

10.1 安全物理环境

10.1.1 室外控制设备物理防护

10.1.1.1 室外控制设备防护缺失

本判例包括以下内容：

a) 标准要求：室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等。

b) 适用范围：第二级及以上定级对象。

c) 问题描述：

1) 室外控制设备裸露放置、无固定措施，无法做到防水、防盗和防火；

2) 放置控制设备的箱体或装置不具有相关检测验收报告，不具有透风、散热、防盗、防雨和防火能力。

d) 可能的缓解措施：控制设备所在位置处于受控区域，且控制设备本身具备防水、防火等特性。

e) 风险评价：室外控制设备裸露放置、无固定措施，或放置控制设备的箱体或装置不具有透风、散热、防盗、防雨和防火能力，但控制设备所在位置处于受控区域，且控制设备本身具备防水、防火等特性，可根据实际措施效果酌情降低风险等级。

10.2 安全通信网络

10.2.1 网络架构

10.2.1.1 工业控制系统网络隔离措施缺失

本判例包括以下内容：

a) 标准要求：工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段。

b) 适用范围：第二级及以上定级对象。

c) 问题描述：

1) 工业控制系统与企业其他系统之间未划分单独的网络区域；

2) 数据交互未采用单向隔离装置或单向隔离装置未配置有效的访问控制策略。

d) 可能的缓解措施：在无行业特殊要求的情况下，工业控制系统与企业其他系统之间部署具有工业控制系统协议内容安全性检测能力的边界访问控制设备，且严格限制了访问控制策略，仅能进行必要的数据传输。

e) 风险评价：

1) 工业控制系统与企业其他系统之间未划分单独的网络区域，无相应的缓解措施，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险；

2) 数据交互未采用单向隔离装置，或单向隔离装置未配置有效的访问控制策略，但在工业控制系统与企业其他系统之间部署具有工业控制系统协议内容安全性检测能力的边界访问控制设备，且严格限制了访问控制策略，可根据实际措施效果酌情降低风险等级。

10.2.1.2 工业控制系统所在网络区域划分不当，访问控制措施缺失

本判例包括以下内容：

a) 标准要求：工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段；

b) 适用范围：第二级及以上定级对象。

c) 问题描述：

1) 工业控制系统所在的生产网络未根据不同工业控制系统业务特点划分不同安全域；

2) 不同安全域之间无任何访问控制措施或访问控制措施无效。

d) 可能的缓解措施：不同工业控制系统业务之间采用串口通信等方式进行严格的数据传输控制。

e) 风险评价：

1) 工业控制系统所在的生产网络未根据不同工业控制系统业务特点划分不同安全域，无相应的缓解措施，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险；
2) 工业控制系统不同安全域之间无任何访问控制措施或访问控制措施无效，但不同工业控制系统业务之间采用串口通信等方式进行严格的数据传输控制，能够避免入侵行为和恶意病毒的扩散，可根据实际措施效果酌情降低风险等级。

10.2.2 通信传输

10.2.2.1 工业控制系统广域网传输控制指令防护措施缺失

本判例包括以下内容：

a) 标准要求：在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：
   1) 未使用基于密码技术的身份鉴别技术；
   2) 未使用密码技术保证数据传输过程中的完整性和保密性。
d) 可能的缓解措施：
   1) 对通信设备采用多种身份鉴别技术、限定通信地址等措施；
   2) 广域网具有设备接入认证措施。
e) 风险评价：
   1) 未使用基于密码技术的身份鉴别技术，但对通信设备采用多种身份鉴别技术、限定通信地址等措施，可根据实际措施效果酌情降低风险等级；
   2) 未使用密码技术保证数据传输过程中的完整性和保密性，但广域网具有设备接入认证措施，可根据实际措施效果酌情降低风险等级。

10.3 安全区域边界

10.3.1 访问控制

10.3.1.1 工业控制系统与企业其他系统之间未对通用网络服务进行限制

本判例包括以下内容：

a) 标准要求：应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、WEB、Telnet、Rlogin、FTP 等通用网络服务；
b) 适用范围：第二级及以上定级对象。
c) 问题描述：
   1) 工业控制系统与企业其他系统之间未部署访问控制设备；
   2) 工业控制系统与企业其他系统之间未对任何通用的网络服务如 E-Mail、WEB、Telnet、Rlogin、FTP 等进行限制。
d) 可能的缓解措施：无。
e) 风险评价：上述任一安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

10.3.2 无线使用控制

10.3.2.1 无线设备管控措施缺失

本判例包括以下内容：

a) 标准要求：对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为。
b) 适用范围：第三级及以上定级对象。
c) 问题描述：对非授权设备接入无线网络环境中或干扰控制系统的行为，无识别和告警信息，如行为进行审计、报警及联动管控等。
d) 可能的缓解措施：具有对无线设备接入的管控措施和身份鉴别措施。

e） 风险评价：对非授权设备接入无线网络环境中或干扰控制系统的行为，无识别和告警信息，但具有对无线设备接入的管控措施和身份鉴别措施，可根据实际措施效果酌情降低风险等级。

10.4 安全计算环境

10.4.1 控制设备安全

10.4.1.1 控制设备未更新

本判例包括以下内容：

a） 标准要求：应使用专用设备和专用软件对控制设备进行更新。

b） 适用范围：第三级及以上定级对象。

c） 问题描述：

1） 未对工业控制系统的控制设备进行更新；

2） 未使用专用设备和软件对工业控制系统的控制设备进行更新。

d） 可能的缓解措施：工业控制系统采取严格的网络边界隔离措施（如物理隔离、单向隔离和网闸隔离）和物理访问控制措施。

e） 风险评价：

1） 未对工业控制系统的控制设备进行更新，但工业控制系统采取严格的网络边界隔离措施（如物理隔离、单向隔离和网闸隔离）和物理访问控制措施，控制设备的安全漏洞不易被利用，可根据实际措施效果酌情降低风险等级；

2） 未使用专用设备和软件对工业控制系统的控制设备进行更新，无相应的缓解措施，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

10.4.1.2 控制设备上线前恶意代码检测措施缺失

本判例包括以下内容：

a） 标准要求：应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序。

b） 适用范围：第三级及以上定级对象。

c） 问题描述：

1） 控制设备上线前未进行安全检测，无法发现设备固件中可能存在的恶意代码程序；

2） 安全检测中发现高风险问题且未进行整改。

d） 可能的缓解措施：上线后定期开展安全检测，且检测的高风险问题均已整改。

e） 风险评价：

1） 控制设备上线前未进行安全检测，但上线后定期开展安全检测，且检测的高风险问题均已整改，可根据实际措施效果酌情降低风险等级；

2） 若安全检测中发现高风险问题且未进行整改，无相应的缓解措施，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

10.5 安全建设管理

10.5.1 产品采购和使用

10.5.1.1 工业控制系统重要设备未开展安全检测

本判例包括以下内容：

a） 标准要求：工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。

b） 适用范围：第二级及以上定级对象。

c） 问题描述：

1） 工业控制系统采购的重要控制设备，未经过国家专业机构的检测；

2） 检测发现高风险问题未进行整改。

d） 可能的缓解措施：上线后定期开展系统的安全检测，且检测的高风险问题均已整改。

e） 风险评价：

1） 采购的重要控制设备未经过国家专业机构的检测，但上线后定期开展系统的安全检测，且检测的高风险问题均已整改，可根据实际措施效果酌情降低风险等级；

2) 安全检测中发现高风险问题且未进行整改，无相应的缓解措施，上述安全问题一旦被威胁利用后，可能会导致等级保护对象面临高风险。

附 录 A
（资料性附录）
基本要求与判例对应关系

为方便测评人员在测评过程中使用本文件，表A.1给出了本文件中高风险判例与GB/T 22239—2019相关等级基本要求的对应关系表。

表A.1 基本要求与判例对应关系表

序号	通用/扩展	层面	控制点	控制项	对应编号	对应判例	适用范围
1	安全通用要求	安全物理环境	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。	6.1.1.1	机房出入口访问控制措施缺失	第三级及以上定级对象
2			防火	机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。	6.1.2.1	机房防火措施缺失	第三级及以上定级对象
3			电力供应	应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。	6.1.3.1	机房短期备用电力供应措施缺失	业务连续性要求高的第三级及以上定级对象
4				应提供应急供电设施。	6.1.3.2	机房应急供电措施缺失	业务连续性要求高的第四级定级对象
5		安全通信网络	网络架构	应保证网络设备的业务处理能力满足业务高峰期需要。	6.2.1.1	网络设备业务处理能力不足	业务连续性要求高的第三级及以上定级对象
6				应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	6.2.1.2	重要网络区域边界访问控制措施缺失	第二级及以上定级对象
7				应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。	6.2.1.3	关键线路和设备冗余措施缺失	业务连续性要求高的第三级及以上定级对象
8			通信传输	应采用密码技术保证通信过程中数据的保密性。	6.2.2.1	采用无加密措施的网络通道传输重要数据	第三级及以上定级对象

序号	通用/扩展	层面	控制点	控制项	对应编号	对应判例	适用范围
9		安全区域边界	边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。	6.3.1.1	网络边界接入设备或端口不可控	第二级及以上定级对象
10				应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。	6.3.1.2	无线网络管控措施缺失	第三级及以上定级对象
11			访问控制	应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。	6.3.2.1	重要网络区域边界访问控制措施缺失或配置不当	第二级及以上定级对象
12			入侵防范	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。	6.3.3.1	外部网络攻击防御措施缺失	第二级及以上定级对象
13				应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。	6.3.3.2	内部网络攻击防御措施缺失	第三级及以上定级对象
14				应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。	6.3.3.3	网络行为分析措施缺失	关键行业的第三级及以上定级对象
15		安全计算环境	身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。	6.4.1.1	存在空口令、弱口令、通用口令或无身份鉴别措施	第二级及以上定级对象
16				当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。	6.4.1.2	鉴别信息明文传输	第二级及以上定级对象
17				应采用口令、密码技术、生物技术等两种或两种以上组	6.4.1.3	未采用两种或两种以上组合身份鉴别技术	第三级及以上定级对象

序号	通用/扩展	层面	控制点	控制项	对应编号	对应判例	适用范围
				合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。			
18			访问控制	应重命名或删除默认账户，修改默认账户的默认口令。	6.4.2.1	未重命名默认账户名且未修改默认口令	第二级及以上定级对象
19				应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。	6.4.2.2	访问控制策略存在缺陷或不完善，存在越权访问可能	第三级及以上定级对象
20			入侵防范	应关闭不需要的系统服务、默认共享和高危端口。	6.4.3.1	开启多余的系统服务、默认共享和高危端口	第二级及以上定级对象
21				应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	6.4.3.2	存在可被利用的高危安全漏洞	第二级及以上定级对象
22				应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。	6.4.3.3	数据有效性检验功能缺失或不完善	第二级及以上定级对象
23			恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	6.4.4.1	恶意代码防范措施缺失	第二级及以上定级对象
24			数据保密性	应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	6.4.5.1	重要数据明文传输	第三级及以上定级对象
25				应采用密码技术保证重要数据在存储过程中的保密性，	6.4.5.2	重要数据明文存储	第三级及以上定级对象

序号	通用/扩展	层面	控制点	控制项	对应编号	对应判例	适用范围
				包括但不限于鉴别数据、重要业务数据和重要个人信息等。			
26			数据备份恢复	应提供重要数据的本地数据备份与恢复功能。	6.4.6.1	重要数据无本地备份措施	第三级及以上定级对象
27				应提供重要数据处理系统的热冗余，保证系统的高可用性。	6.4.6.2	数据处理系统冗余措施缺失	业务连续性要求高的第三级及以上定级对象
28				应建立异地灾难备份中心，提供业务应用的实时切换。	6.4.6.3	无异地灾备措施	业务连续性要求高的第四级定级对象
29			个人信息保护	应仅采集和保存业务必需的用户个人信息。	6.4.7.1	违规采集和存储个人信息	第二级及以上定级对象
30				应禁止未授权访问和非法使用用户个人信息。	6.4.7.2	违规访问和使用个人信息	第二级及以上定级对象
31		安全管理中心	集中管控	应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。	6.5.1.1	远程管理路径安全防护措施不足	第三级及以上定级对象
32				应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。	6.5.1.2	审计记录存储时间不满足要求	第三级及以上定级对象
33		安全管理制度	管理制度	应对安全管理活动中的各类管理内容建立安全管理制度。	6.6.1.1	管理制度缺失	第三级及以上定级对象
34		安全管理机构	岗位设置	应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权。	6.7.1.1	未建立网络安全工作领导机构	第三级及以上定级对象
35		安全管理人员	外部人员访问管理	应在外部人员接入受控网络访问系统前先提出书面申	6.8.1.1	外部人员接入网络管理措施缺失	第二级及以上定级对象

序号	通用/扩展	层面	控制点	控制项	对应编号	对应判例	适用范围
				请，批准后由专人开设账户、分配权限，并登记备案。			
36		安全建设管理	产品采购和使用	应确保网络安全产品采购和使用符合国家的有关规定。	6.9.1.1	违规采购和使用网络安全产品	第二级及以上定级对象
37			外包软件开发	应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。	6.9.2.1	外包软件开发代码审计措施缺失	第三级及以上定级对象
38			测试验收	应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。	6.9.3.1	上线前未开展安全测试	第三级及以上定级对象
39			等级测评	应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。	6.9.4.1	未定期进行等级测评	第三级及以上定级对象
40				应确保测评机构的选择符合国家有关规定。	6.9.4.2	选择的测评机构不符合国家相关要求	第三级及以上定级对象
41		安全运维管理	应急预案管理	应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。	6.10.1.1	未制定重要事件应急预案	第二级及以上定级对象
42				应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。	6.10.1.2	未定期开展应急预案培训和演练	第三级及以上定级对象
43	云计算安全扩展要求	安全物理环境	物理位置选择	应保证云计算基础设施位于中国境内。	7.1.1.1	云计算基础设施位于中国境外	第二级及以上云计算平台
44		安全通信网络	网络架构	应保证云计算平台不承载高于其安全保护等级的业务应用系统。	7.2.1.1	云计算平台承载高于其安全保护等级的业务系统	第二级及以上云计算平台
45				应实现不同云服务客户虚拟	7.2.1.2	云计算平台虚拟网络隔离措施缺失	第二级及以上云计算平台

序号	通用/扩展	层面	控制点	控制项	对应编号	对应判例	适用范围
				网络之间的隔离。			
46				应为第四级业务应用系统划分独立的资源池。	7.2.1.3	未单独划分独立的资源池	第四级云计算平台
47				应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。	7.2.1.4	云计算平台未提供安全防护能力	第二级及以上云计算平台
48		安全区域边界	访问控制	应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。	7.3.1.1	虚拟化网络边界访问控制措施缺失	第二级及以上云计算平台和云服务客户系统
49			入侵防范	应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。	7.3.2.1	云计算平台网络攻击防御措施缺失	第三级及以上云计算平台
50		安全计算环境	镜像和快照保护	应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。	7.4.1.1	镜像和快照保护措施缺失	第三级及以上云计算平台
51			数据完整性和保密性	应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。	7.4.2.1	云服务客户数据、个人信息违规出境	第二级及以上云计算平台
52			数据备份恢复	云服务客户应在本地保存其业务数据的备份。	7.4.3.1	云服务客户未在本地保存业务数据的备份	第二级及以上云服务客户业务系统
53				应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。	7.4.3.2	未提供云计算平台迁移技术手段	第二级及以上云计算平台
54			剩余信息保护	云服务客户删除业务应用数据时，云计算平台应将云存	7.4.4.1	云服务客户删除业务应用数据时，云计算平台未删除所有副本	第二级及以上云计算平台

序号	通用/扩展	层面	控制点	控制项	对应编号	对应判例	适用范围
				储中所有副本删除。			
55		安全管理中心	集中管控	应保证云计算平台管理流量与云服务客户业务流量分离。	7.5.1.1	云计算平台管理流量与云服务客户业务流量未分离	第三级及以上云计算平台
56		安全建设管理	云服务商选择	应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。	7.6.1.1	云服务客户选择服务商不合规	第二级及以上云服务客户业务系统
57			供应链管理	应确保供应商的选择符合国家有关规定。	7.6.2.1	供应商的选择不符合国家有关规定	第三级及以上云计算平台
58		安全运维管理	云计算环境管理	云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。	7.7.1.1	云计算平台运维地点不位于中国境内，且运维操作未遵循国家相关规定	第二级及以上云计算平台。
59	移动互联安全扩展要求	安全物理环境	无线接入点的物理位置	应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。	8.1.1.1	无线接入点过度覆盖	第四级定级对象
60		安全区域边界	边界防护	应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。	8.2.1.1	有线网络与无线网络边界防护缺失	第三级及以上定级对象
61			访问控制	无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码。	8.2.2.1	无线接入设备认证功能缺失	第二级及以上定级对象
62			入侵防范	应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP 认证等。	8.2.3.1	无线接入设备高风险功能开启	第三级及以上定级对象。
63				应禁止多个 AP 使用同一个认证密钥。	8.2.3.2	多个AP使用相同简单认证密钥	第二级及以上定级对象

序号	通用/扩展	层面	控制点	控制项	对应编号	对应判例	适用范围
64				应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密码破解、中间人攻击和欺骗攻击等行为。	8.2.3.3	无法检测到针对无线接入设备的网络攻击行为	第三级及以上定级对象
65		安全计算环境	移动应用管控	应只允许指定证书签名的应用软件安装和运行。	8.3.1.1	移动终端安装未经指定证书签名的应用软件	第三级及以上定级对象
66				应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。	8.3.1.2	移动终端安装有高风险恶意软件	第三级及以上定级对象
67		安全建设管理	移动应用软件采购	应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。	8.4.1.1	未知渠道应用软件安装	第三级及以上定级对象
68				应保证移动终端安装、运行的应用软件由指定的开发者开发。	8.4.1.2	安装使用未经安全评估的开源软件	第三级及以上定级对象
69	物联网安全扩展要求	安全物理环境	感知节点设备物理防护	感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动。	9.1.1.1	感知节点设备所处物理环境对感知节点造成物理破坏	第三级及以上定级对象
70		安全区域边界	接入控制	应保证只有授权的感知节点可以接入。	9.2.1.1	非授权感知节点设备能够接入网络中	第二级及以上定级对象
71		安全计算环境	感知节点设备安全	应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更。	9.3.1.1	非授权用户可对感知节点设备的软件应用进行配置或变更	第三级及以上定级对象
72			网关节点设备安全	应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力。	9.3.2.1	网关节点设备连接无身份鉴别措施	第三级及以上定级对象
73	工业控制系统安全扩展要求	安全物理环境	室外控制设备物理防护	室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中	10.1.1.1	室外控制设备防护缺失	第二级及以上工业控制系统

序号	通用/扩展	层面	控制点	控制项	对应编号	对应判例	适用范围
				并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等。			
74		安全通信网络	网络架构	工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用单向的技术隔离手段。	10.2.1.1	工业控制系统网络隔离措施缺失	第二级及以上工业控制系统
75				工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。	10.2.1.2	工业控制系统所在网络区域划分不当，访问控制措施缺失	第二级及以上工业控制系统
76			通信传输	在工业控制系统内使用广域网进行控制指令或相关数据交换的应采用加密认证技术手段实现身份认证、访问控制和数据加密传输。	10.2.2.1	工业控制系统广域网传输控制指令防护措施缺失	第三级及以上工业控制系统
77		安全区域边界	访问控制	应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的E-Mail、WEB、Telnet、Rlogin、FTP等通用网络服务。	10.3.1.1	工业控制系统与企业其他系统之间未对通用网络服务进行限制	第二级及以上工业控制系统
78			无线使用控制	对采用无线通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的行为。	10.3.2.1	无线设备管控措施缺失	第三级及以上工业控制系统
79		安全计算环境	控制设备安全	应使用专用设备和专用软件	10.4.1.1	控制设备未更新	第三级及以上工业控制系统

序号	通用/扩展	层面	控制点	控制项	对应编号	对应判例	适用范围
				对控制设备进行更新。			
80				应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序。	10.4.1.2	控制设备上线前恶意代码检测措施缺失	第三级及以上工业控制系统
81		安全建设管理	产品采购和使用	工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。	10.5.1.1	工业控制系统重要设备未开展安全检测	第二级及以上工业控制系统

附 录 B
（资料性附录）
高风险判例整改建议

针对本文件中提出的高风险场景，表B.1基于一般场景，给出每条判例对应的整改建议，测评人员可根据建议内容，并结合定级对象实际场景，提出有针对性、可落地实施的整改建议。

图B.1 高风险判例对应整改建议

序号	编号	对应判例	整改建议
1	6.1.1.1	机房出入口访问控制措施缺失	建议机房出入口配备电子门禁系统或安排专人值守，对进出机房的人员进行控制、鉴别、并记录相关人员信息。
2	6.1.2.1	机房防火措施缺失	建议机房设置火灾自动消防系统，能够自动检测火情、报警及灭火，相关消防设备如灭火器等应定期检查，确保防火措施持续有效。
3	6.1.3.1	机房短期备用电力供应措施缺失	建议机房配备容量合理的后备电源，并定期对相关设施进行定期巡检，确保在外部电力供应中断的情况下，备用供电设备能满足系统短期正常运行。
4	6.1.3.2	机房应急供电措施缺失	建议配备柴油发电机、应急供电车等备用发电设备。
5	6.2.1.1	网络设备业务处理能力不足	建议更换性能满足业务高峰期需要的网络设备，并合理预估业务增长情况，制定合适的扩容计划。
6	6.2.1.2	重要网络区域边界访问控制措施缺失	建议合理规划网络架构，避免重要网络区域部署在边界处；重要网络区域与其他网络边界处，尤其是外部非安全可控网络、内部非重要网络区域之间边界处应部署访问控制设备，并合理配置相关控制策略，确保控制措施有效。
7	6.2.1.3	关键线路和设备冗余措施缺失	建议关键网络链路、关键网络设备、关键计算设备采用冗余设计和部署，例如采用热备、负载均衡等部署方式，保证系统的高可用性。
8	6.2.2.1	采用无加密措施的网络通道传输重要数据	建议采用密码技术为重要敏感数据在传输过程中的保密性提供保障，相关密码技术符合国家密码管理主管部门的规定。
9	6.3.1.1	网络边界接入设备或端口不可控	建议明确边界接入设备，禁用空闲端口，在网络中部署网络管理系统，通过自动拓扑发现功能发现非授权的网络出口链路。
10	6.3.1.2	无线网络管控措施缺失	无特殊需要，建议内部重要网络不应与无线网络互联；若因业务需要，则建议加强对无线网络设备接入的管控，并通过边界设备对无线网络的接入设备对内部重要网络的访问进行限制，降低攻击者利用无线网络入侵内部重要网络。
11	6.3.2.1	重要网络区域边界访问控制措施缺失或配置不当	建议对重要网络区域与其他网络区域之间的边界进行梳理，明确访问地址、端口、协议等信息，并通过访问控制设备，合理配置相关控制策略，确保控制措施有效。
12	6.3.3.1	外部网络攻击防御措施缺失	建议在关键网络节点（如互联网边界处）合理部署具备攻击行为检测、防止或限制功能的安全防护设备（如入侵防御设备、WEB应用防火墙、抗DDoS攻击等设备），或采用云防、流量清洗等外部抗攻击服务；相关安全防护设备应及时升级策略库/规则库。

序号	编号	对应判例	整改建议
13	6.3.3.2	内部网络攻击防御措施缺失	建议在关键网络节点处进行严格的访问控制措施，并部署相关的防护设备，检测、防止或限制从内部发起的网络攻击行为（包括其他内部网络区域对核心服务器区的攻击行为、服务器之间的攻击行为、内部网络向互联网目标发起攻击等）。对于服务器之间的内部攻击行为，建议合理划分网络区域，加强不同服务器之间的访问控制，部署主机入侵防范产品，或通过部署流量探针的方式，检测异常攻击流量。
14	6.3.3.3	网络行为分析措施缺失	建议在网络关键节点部署沙箱、抗APT系统或协议分析系统，对网络访问行为进行分析，实现对新型攻击行为的检测报警。
15	6.4.1.1	存在空口令、弱口令、通用口令或无身份鉴别措施	建议删除或修改账户通用口令，重命名默认账户，制定相关管理制度，规范口令的最小长度、复杂度与生命周期，并根据管理制度要求，合理配置账户口令复杂度和定期更换策略；此外，建议为不同设备配备不同的口令，避免一台设备口令被破解影响所有设备安全。
16	6.4.1.2	鉴别信息明文传输	建议尽可能避免通过网络环境对网络设备、安全设备、操作系统、数据库等进行远程管理。如确有需要，则建议采取措施或使用加密机制（如VPN加密通道、开启SSH、HTTPS协议等），防止鉴别信息在网络传输过程中被窃听。
17	6.4.1.3	未采用两种或两种以上组合身份鉴别技术	建议核心设备、操作系统等增加除用户名/口令以外的身份鉴别技术，如基于密码技术的动态口令/令牌等鉴别方式，使用多种鉴别技术进行身份鉴别，增强身份鉴别的安全力度；对于使用堡垒机或统一身份认证机制实现多种身份鉴别的场景，建议通过地址绑定等技术措施，确保设备只能通过该机制进行身份认证，无旁路现象存在。
18	6.4.2.1	未重命名默认账户名且未修改默认口令	建议网络设备、安全设备、主机设备（包括操作系统、数据库等）等重命名或删除默认管理员账户，修改默认密码，使其具备一定的安全强度，增强账户安全性。
19	6.4.2.2	访问控制策略存在缺陷或不完善，存在越权访问可能	建议根据系统用户及其所需的访问权限，设计系统访问控制策略，并依据该策略为系统用户分配与其角色或职责相匹配的访问权限，避免垂直越权和平行越权行为的发生。对应用系统的重要页面、功能模块进行重新进行身份、权限鉴别，确保应用系统不存在访问控制失效情况。
20	6.4.3.1	开启多余的系统服务、默认共享和高危端口	建议网络设备、安全设备、主机设备等关闭不必要的服务和端口，降低安全隐患。
21	6.4.3.2	存在可被利用的高危安全漏洞	建议在充分测试的情况下，及时对设备进行补丁更新，修补已知的高风险安全漏洞；此外，还应定期对设备进行漏洞扫描，及时处理发现的风险漏洞，提高设备稳定性与安全性。
22	6.4.3.3	数据有效性检验功能缺失或不完善	建议修改应用系统代码，对输入数据的格式、长度、特殊字符进行校验和必要的过滤，提高应用系统的安全性，防止相关漏洞的出现。
23	6.4.4.1	恶意代码防范措施缺失	建议在关键网络节点及主机操作系统上均部署恶意代码检测和清除产品，开启恶意代码检测和清除功能，并及时更新恶意代码库。网络层与主机层恶意代码防范产品宜形成异构模式，有效检测及清除可能出现的恶意代码攻击。

序号	编号	对应判例	整改建议
24	6.4.5.1	重要数据明文传输	建议采用密码技术保证重要数据在传输过程中的保密性，且相关密码技术符合国家密码管理部门的规定。
25	6.4.5.2	重要数据明文存储	建议采用密码技术保证重要数据在存储过程中的保密性，且相关密码技术符合国家密码管理部门的规定。
26	6.4.6.1	重要数据无本地备份措施	建议建立备份恢复机制，定期对重要数据进行备份以及恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复，此外，应对备份文件妥善保存，不要放在互联网网盘、开源代码平台等不可控环境中，避免重要信息泄露。
27	6.4.6.2	数据处理系统冗余措施缺失	建议对重要数据处理系统采用热冗余技术，提高系统的可用性。
28	6.4.6.3	无异地灾备措施	建议建立异地应用级灾备中心，通过技术手段实现业务应用的实时切换，提高系统的可用性。
29	6.4.7.1	违规采集和存储个人信息	建议根据国家、行业主管部门以及标准的相关规定（如《信息安全技术 个人信息安全规范》），明确向用户表明采集信息的内容、用途以及相关的安全责任，并在用户同意、授权的情况下采集、保存业务必需的用户个人信息。
30	6.4.7.2	违规访问和使用个人信息	建议根据国家、行业主管部门以及标准的相关规定（如《信息安全技术 个人信息安全规范》），通过技术和管理手段，防止未授权访问和非法使用用户个人信息。
31	6.5.1.1	远程管理路径安全防护措施不足	建议采用加密的方式传输管理数据，防止数据泄露。
32	6.5.1.2	审计记录存储时间不满足要求	部署日志服务器，统一收集各设备的审计数据，进行集中分析，并根据法律法规的要求留存日志。
33	6.6.1.1	管理制度缺失	建议按照等级保护的相关要求，建立包括总体方针、安全策略在内的各类与安全管理活动相关的管理制度。
34	6.7.1.1	未建立网络安全工作领导机构	建议成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权。
35	6.8.1.1	外部人员接入网络管理措施缺失	建议在外部人员管理制度中明确接入受控网络访问系统的申请审批流程，并对外部人员接入设备、可访问资源范围、账号回收、保密责任等内容做出明确规定，避免因管理缺失导致外部人员对受控网络、系统带来安全隐患。
36	6.9.1.1	违规采购和使用网络安全产品	建议依据国家有关规定，采购和使用网络安全产品，例如采购或使用获得销售许可证或通过相关机构的检测认证的网络安全产品。
37	6.9.2.1	外包软件开发代码审计措施缺失	建议对开发单位开发的核心系统进行源代码审查，检查是否存在后门和隐蔽信道。如没有技术手段进行源代码审查的，可聘请第三方专业机构对相关代码进行安全检测。
38	6.9.3.1	上线前未开展安全测试	建议在新系统上线前，对系统进行安全性评估，及时修补评估过程中发现的问题，确保系统安全上线。
39	6.9.4.1	未定期进行等级测评	第三级以上系统每年进行至少一次的等级测评，并对发现的系统安全问题及时整改。
40	6.9.4.2	选择的测评机构不符合国家相关要求	选择网络安全等级保护网(www.djbh.net)全国网络安全等级保护测评机构目录中的测评机构。

序号	编号	对应判例	整改建议
41	6.10.1.1	未制定重要事件应急预案	建议根据本系统实际情况，对重要事件制定有针对性的应急预案，明确重要事件的应急处理流程、系统恢复流程等内容。
42	6.10.1.2	未定期开展应急预案培训和演练	建议每年定期对相关人员进行应急预案培训与演练，并保留应急预案培训和演练记录，使参与应急的人员熟练掌握应急的整个过程。
43	7.1.1.1	云计算基础设施位于中国境外	建议将云计算基础设施部署于中国境内，依据《网络安全法》及其他相关法规政策规定履行网络安全保护责任，接受国家相关部门的监管。
44	7.2.1.1	云计算平台承载高于其安全保护等级的业务系统	建议云服务客户选择不低于其安全保护等级的云计算平台；云计算平台只承载不高于其安全保护等级的业务应用系统。
45	7.2.1.2	云计算平台虚拟网络隔离措施缺失	建议采用网络防火墙、虚拟私有网（VPC，Virtual Private Cloud）、安全组防火墙等措施对云计算平台上不同租户或业务系统的虚拟网络边界进行逻辑隔离，并配置严格的IP、端口、协议访问控制策略。
46	7.2.1.3	未单独划分独立的资源池	建议在云计算平台设计规划和建设过程中，根据所承载的业务系统的安全级别，预留必要的软硬件资源作为第四级系统区专用，或通过系统网络策略调整形成与其他区域事实上隔离的区域调整为第四级系统专用区，从而实现第四级系统与其他级别系统的隔离部署。
47	7.2.1.4	云计算平台未提供安全防护能力	建议云计算平台为云租户提供满足其业务安全防护需求的安全能力，如带宽动态扩容、IPV6接入、公网IP、域名解析等网络通信能力，区域隔离、流量检测、端口转发等边界防护能力，抗DDoS、流量清洗、抗APT、协议分析等入侵防范能力。并保证相关安全服务可即时生效、动态扩容、相关特征库、规则库等及时更新，所提供的最高等级防护应满足所能承载的最高安全需求的租户系统的需要。
48	7.3.1.1	虚拟化网络边界访问控制措施缺失	建议通过部署安全组、虚拟防火墙、划分VLAN等措施，对虚拟网络区域边界实施访问控制，确保仅明确允许的流量可以跨区域访问。
49	7.3.2.1	云计算平台网络攻击防御措施缺失	建议云计算平台部署必要的租户行为检测措施，如流量监测，行为审计、态势感知等，确保云计算平台提供给给租户的网络、计算和存储资源被合法使用。在发现云租户通过云计算平台发起网络攻击时，能对租户的攻击行为进行记录，如攻击类型，攻击时间、攻击流量等，并在必要的情况下对攻击行为进行阻断。
50	7.4.1.1	镜像和快照保护措施缺失	建议在存储及传输虚拟机镜像和快照文件时，通过密码技术进行加密，或通过访问控制措施对镜像和快照的访问权限予以限制，防止敏感资源被非授权访问。
51	7.4.2.1	云服务客户数据、个人信息违规出境	建议云计算平台的数据中心、存储用户数据的服务器、存储设备等均在中国境内。云服务客户数据、个人信息如需出境需遵循国家有关规定。
52	7.4.3.1	云服务客户未在本地保存业务数据的备份	建议云服务客户根据自身数据更新频率等特性，定期或实时将云计算平台中的数据在本地备份。
53	7.4.3.2	未提供云计算平台迁移技术手段	建议云服务客户在采购云服务时通过协议条款明确云服务商在协助自身业务和数据迁移过程的义务和责任，通过技术和协议共同保障云服务客户自主选择云服务的合法权益。

序号	编号	对应判例	整改建议
54	7.4.4.1	云服务客户删除业务应用数据时，云计算平台未删除所有副本	建议云计算平台通过技术手段保证所有副本的数据同步生成、同步更新、同步清除。云服务客户也可通过协议条款明确云服务商在服务终止时清除所有数据副本的责任和义务，通过技术和协共同保障云服务客户的数据安全。
55	7.5.1.1	云计算平台管理流量与云服务客户业务流量未分离	建议云计算平台使用带外管理方式，管理口禁止运行其他业务。
56	7.6.1.1	云服务客户选择服务商不合规	建议遵守网络安全等级保护及其它相关网络安全政策、标准和规范要求，云服务客户选择不低于其安全保护等级的云计算平台，且确保业务应用系统不部署在未进行等级保护定级备案、测评、报告时间超出有效期或测评结论为差的云计算平台上。
57	7.6.2.1	供应商的选择不符合国家有关规定	建议从国家有关部门公布的产品、服务采购推荐目录中选择供应商，确保所采购的产品具备相关功能、性能、安全检验证书，具备销售许可，确保所采购产品和服务的合规性。
58	7.7.1.1	云计算平台运维地点不位于中国境内，且运维操作未遵循国家相关规定	建议在中国境内对云计算平台进行远程运维管理，依据《网络安全法》及其他相关法规政策规定履行网络安全保护责任，接受国家相关部门的监管，对确需在境外地点实施运维管理的，应提前向国家相关部门做好申请和报备，获得批准后严格按照要求实施。
59	8.1.1.1	无线接入点过度覆盖	建议根据无线信号强度、范围和干扰设计接入位置、强度，或者使用法拉第笼、白噪音等方式进行无线信号屏蔽，避免无线信号过度覆盖，防止外部区域未授权访问移动互联网。
60	8.2.1.1	有线网络与无线网络边界防护缺失	建议有线网络与无线网络边界之间部署无线接入网关设备，对无线接入进行统一管理。
61	8.2.2.1	无线接入设备认证功能缺失	建议无线接入设备未开启接入认证功能，防止非授权无线接入设备接入移动互联网。
62	8.2.3.1	无线接入设备高风险功能开启	建议禁用SSID的默认广播，使用基于WPA2或 WPA3的身份认证和加密解决方案，禁用默认启用的WPS功能。
63	8.2.3.2	多个AP使用相同简单认证密钥	建议为不同AP分配对应的专属密钥，避免多个AP使用相同简单认证密钥。
64	8.2.3.3	无法检测到针对无线接入设备的网络攻击行为	建议在网络中部署入侵检测产品并覆盖针对无线接入设备的网络扫描、DDoS 攻击、密码破解、中间人攻击和欺骗攻击等行为，同时应确保规则库及时更新。
65	8.3.1.1	移动终端安装未经指定证书签名的应用软件	建议移动终端在应用软件安装和运行前通过密码技术或校验技术验证软件完整性，确保软件未被篡改。
66	8.3.1.2	移动终端安装有高风险恶意软件	建议移动终端采用白名单方式进行终端应用软件安装、运行控制。
67	8.4.1.1	未知渠道应用软件安装	建议使用可靠分发渠道获取移动终端应用软件，避免安装、运行来自第三方应用商店或其他未知渠道的应用软件，安装、运行前使用密码技术对软件证书签名进行验证。
68	8.4.1.2	安装使用未经安全评估的开源软件	建议从官方渠道获取稳定版本开源软件，使用开源代码和应用程序前，应进行安全评估检测。
69	9.1.1.1	感知节点设备所处物理环境对感知节点造成物理破坏	建议根据感知节点所处环境选择合适的安装位置，避免周围环境对设备造成物理破坏，影响设备正常工作。
70	9.2.1.1	非授权感知节点设备能够接入网络中	建议设置感知节点接入控制措施，防止未经授权的感知节点接入网关、传感器等设备接入网络。

序号	编号	对应判例	整改建议
71	9.3.1.1	非授权用户可对感知节点设备的软件应用进行配置或变更	建议为感知节点设备配置访问控制措施，限制不同用户的访问权限，确保用户权限最小化。
72	9.3.2.1	网关节点设备连接无身份鉴别措施	建议启用感知节点设备的身份鉴别功能，并设置身份鉴别信息的长度、复杂度和有效期。
73	10.1.1.1	室外控制设备防护缺失	建议室外控制设备放置于箱体或装置中，并确保箱体或装置具有透风、散热、防盗、防雨和防火能力。
74	10.2.1.1	工业控制系统网络隔离措施缺失	建议工业控制系统与企业其他系统之间划分单独的网络区域，数据交互采用单向隔离装置并配置有效的访问控制策略。
75	10.2.1.2	工业控制系统所在网络区域划分不当，访问控制措施缺失	建议根据工业控制系统的业务特点划分不同安全域，不同安全区域之间根据业务需求配置访问控制策略。
76	10.2.2.1	工业控制系统广域网传输控制指令防护措施缺失	建议工业控制系统通过广域网传输控制指令时采用密码技术进行身份鉴别，并对传输中的数据进行保护。
77	10.3.1.1	工业控制系统与企业其他系统之间未对通用网络服务进行限制	建议工业控制系统与企业其他系统之间部署访问控制设备，并对E-Mail、WEB、Telnet、Rlogin、FTP等通用网络服务进行限制。
78	10.3.2.1	无线设备管控措施缺失	建议部署安全审计、态势感知等安全手段，对非授权设备接入无线网络环境中或干扰控制系统的行为，进行识别和告警。
79	10.4.1.1	控制设备未更新	建议使用专用设备或软件定期对工业控制系统的控制设备进行更新。
80	10.4.1.2	控制设备上线前恶意代码检测措施缺失	建议工业控制系统的控制设备上线前对其进行安全检测，及时发现并修复设备固件中的恶意代码程序。
81	10.5.1.1	工业控制系统重要设备未开展安全检测	建议购买经过国家专业机构检测的重要控制设备。

参 考 文 献

[1] 《中华人民共和国网络安全法》，2016
[2] 《中华人民共和国密码法》，2019
[3] 《网络安全审查办法》,2022
[4] GB/T 20984—2024 信息安全技术 信息安全风险评估方法
[5] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[6] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[7] GB/T 35273—2020 信息安全技术 个人信息安全规范
[8] GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求