ICS 35.040
L 80

ISEAA

团　　体　　标　　准

T/ISEAA 001—2020

网络安全等级保护测评高风险判定指引

High risk assessment guidelines for classified protection evaluation of cyber security

2020-11-05 发布　　2020-12-01 实施

中关村信息安全测评联盟　　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》给出的规则起草。

本文件由中关村信息安全测评联盟提出并归口。

本文件起草单位：上海市信息安全测评认证中心、国家网络与信息系统安全产品质量监督检验中心、江苏金盾检测技术有限公司、江苏骏安信息测评认证有限公司、山东新潮信息技术有限公司、合肥天帷信息安全技术有限公司、深圳市网安计算机安全检测技术有限公司、杭州安信检测技术有限公司、成都安美勤信息技术股份有限公司、甘肃安信信息安全技术有限公司、教育信息安全等级保护测评中心、辽宁浪潮创新信息技术有限公司、银行卡检测中心、安徽祥盾信息科技有限公司。

本文件主要起草人：金铭彦、罗峥、张笑笑、刘静、徐御、陈清明、陆臻、陈妍、吴晓艳、何欣峰、许晓晨、张杰、武建双、牛建红、倪祥焕、何志鹏、严维兵、王永琦、范仲伟、武斌、杨凌珺、盛璐禕。

引　言

等级保护测评是推动和贯彻网络安全等级保护工作的重要环节之一。为了更好地提升全国等级保护测评机构的能力，规范测评机构对网络安全风险严重程度的判定规则，中关村信息安全测评联盟组织编写本等级保护测评行业指引性文件，旨在促进安全风险判定更加标准化、规范化，从而更好地规范等级保护测评活动，提升等级保护测评工作质量。

本文件依据 GB/T 22239—2019《信息安全技术　网络安全等级保护基本要求》中第二级及以上安全通用要求及云计算安全扩展要求中的基本原则，对测评过程中发现的安全性问题如何进行高风险判定给出指引。

本文件仅考虑一般系统场景，无法涵盖所有行业及特殊场景，实际测评活动中应根据安全问题所处的环境、面临的威胁、已采取的措施，并结合本文件内容做出客观、科学、合理的判定。

网络安全等级保护测评高风险判定指引

1 范围

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—1999 计算机信息系统 安全保护等级划分准则

GB/T 25069—2010 信息安全技术 术语

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

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—2014 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—1999、GB/T 25069—2010、GB/T 31168—2014 和 GB/T 22239—2019 界定的以及下列术语和定义适用于本文件。

3.1

高可用性系统

可用性大于或等于 99.9%，年度停机时间小于或等于 8.8 h 的系统，例如，银行、证券、非银行支付机构、互联网金融等交易类系统，提供公共服务的民生类系统，工业控制类系统，云计算平台等。

3.2

关键网络设备

部署在关键网络节点的重要网络设备，包括但不限于核心交换机、核心路由器等，一旦该设备遭受攻击或出现故障将影响整个系统网络。

3.3

不可控网络环境

互联网、公共网络环境、开放性办公网络等缺少网络安全管控措施，可能存在恶意攻击、数据窃听等安全隐患的网络环境。

3.4

可被利用的高危漏洞

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。

3.5

云管理平台

被云服务商或云服务客户用于对云计算资源进行管理的系统平台。

4 缩略语

下列缩略语适用于本文件。

ACL:访问控制列表(Access Control List)

CPU:中央处理单元(Central Processing Unit)

DDoS:拒绝服务(Distributed Denial of Service)

IP:互联网协议(Internet Protocol)

IPS:入侵防御系统(Intrusion Prevention System)

PIN:个人识别码(Personal Identification Number)

RTO:恢复时间目标(Recovery Time Objective)

SQL:结构化查询语言(Structured Query language)

UPS:不间断电源(Uninterruptible Power Supply)

USB:通用串行总线(Universal Serial Bus)

UTM:统一威胁管理(Unified Threat Management)

VPN:虚拟专用网络(Virtual Private Network)

5 概述

5.1 判例概述

本文件中每条判例由标准要求、适用范围、判例场景和补偿因素构成。其中,标准要求表述该条判例对应的 GB/T 22239—2019 中的具体要求(以第三级要求为例);适用范围表述该条判例适用的定级对象等级或特性;判例场景描述该条判例具体的场景及要素,当出现多个场景时,将通过标注“所有”或“任意”来明确表示是符合所有场景还是任意场景即判为高风险;补偿因素则给出可进行综合风险分析,从而酌情判定风险等级的场景及分析因素。

为方便测评人员使用以及为定级对象提出合理的整改建议,本文件在附录中给出每条判例与 GB/T 22239—2019 中第三级安全要求的对应关系以及整改建议,供测评人员参考,具体参见附录 A 和附录 B。

5.2 判定原则

在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,给出应判为高风险的场景:

——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,且没有等效或补偿措施;

——存在可被利用，且能造成严重后果的安全漏洞；

——通过综合风险分析，对业务信息安全和系统服务安全可能产生重大隐患的安全问题。

5.3 场景释义

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，本文件仅针对一般应用系统场景，给出应判为高风险的场景及补偿因素，供现场测评人员在进行风险分析时参考。

对于金融、电力、制造业等特定行业的系统，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。现场测评人员可根据本文件的内容，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场景及补偿因素，或虽然不在本文件明确的适用范围内，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 高风险判例

6.1 安全物理环境

6.1.1 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：二级及以上系统。

c) 判例场景：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）、无专人值守等。

d) 补偿因素：机房所在位置处于受控区域，非授权人员无法随意进出机房，可根据实际措施效果，酌情判定风险等级。

6.1.2 机房防盗措施缺失

本判例包括以下内容：

a) 标准要求：应设置机房防盗报警系统或设置有专人值守的视频监控系统。

b) 适用范围：三级及以上系统。

c) 判例场景（所有）：

1) 机房或机房所在区域无防盗报警系统，无法对盗窃事件进行告警、追溯；

2) 未设置有专人值守的视频监控系统。

d) 补偿因素：机房出入口或机房所在区域有其他控制措施，例如机房出入口设有专人值守，机房所在位置处于受控区域等，非授权人员无法进入该区域，可根据实际措施效果，酌情判定风险等级。

6.1.3 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：二级及以上系统。

c) 判例场景（任意）：

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，手提式灭火器等灭火设施，消

防设备未进行年检或已失效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） 补偿因素：机房安排专人值守或设置了专人值守的视频监控系统，并且机房附近有符合国家消防标准的灭火设备，一旦发生火灾，能及时进行灭火，可根据实际措施效果，酌情判定风险等级。

6.1.4 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：二级及以上系统。

c） 判例场景（任意）：

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） 机房现有备用电力供应无法满足定级对象短期正常运行。

d） 补偿因素：对于机房配备多路供电的情况，可从供电方同时断电发生概率等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.1.5 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：高可用性的四级系统。

c） 判例场景（任意）：

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） 应急供电措施不可用或无法满足定级对象正常运行需求。

d） 补偿因素：

1） 对于机房配备多路供电的情况，可从供电方同时断电发生概率等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

2） 对于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，能降低单一机房发生电力故障所带来的可用性方面影响的情况，可从影响程度、RTO 等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.1.6 云计算基础设施物理位置不当

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：二级及以上云计算平台。

c） 判例场景：云计算基础设施，例如云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软硬件等不在中国境内。

d） 补偿因素：无。

6.2 安全通信网络

6.2.1 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：高可用性的三级及以上系统。
c) 判例场景：核心交换机、核心路由器、边界防火墙等网络链路上的关键设备性能无法满足高峰期需求，可能导致服务质量严重下降或中断，例如性能指标平均达到80%以上。
d) 补偿因素：对于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，能降低单一机房发生设备故障所带来的可用性方面影响的情况，可从影响程度、RTO等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

注：80%仅为参考值，可根据设备类型、处理效果等情况综合判断；性能指标包括CPU、内存占用率，吞吐量等。

6.2.2 网络区域划分不当

本判例包括以下内容：
a) 标准要求：应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
b) 适用范围：二级及以上系统。
c) 判例场景：重要网络区域与非重要网络在同一子网或网段，例如承载业务系统的生产网络与员工日常办公网络，面向互联网提供服务的服务器区域与内部网络区域在同一子网或网段等。
d) 补偿因素：同一子网之间有技术手段实现访问控制，可根据实际措施效果，酌情判定风险等级。

6.2.3 网络边界访问控制设备不可控

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：二级及以上系统。
c) 判例场景(所有)：
   1) 网络边界访问控制设备无管理权限；
   2) 未采取其他任何有效的访问控制措施，例如服务器自带防火墙未配置访问控制策略等；
   3) 无法根据业务需要或所发生的安全事件及时调整访问控制策略。
d) 补偿因素：网络边界访问控制措施由云服务商提供或由集团公司统一管理，管理方能够根据系统的业务及安全需要及时调整访问控制策略，可从策略更改响应时间、策略有效性、执行效果等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.2.4 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：二级及以上系统。
c) 判例场景：在网络架构上，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)无访问控制设备实施访问控制措施，例如重要网络区域与互联网等外部非安全可控网络边界处、生产网络与员工日常办公网络之间、生产网络与无线网络接入区之间未部署访问控制设备实施访问控制措施等。
d) 补偿因素：无。

注：互联网边界访问控制设备包括但不限于防火墙、UTM等能实现相关访问控制功能的专用设备；对于内部边界访问控制，也可使用路由器、交换机或者带ACL功能的负载均衡器等设备实现。测评过程中应根据设备部署

位置、设备性能压力等因素综合进行分析，判断采用设备的合理性。

6.2.5 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：高可用性的三级及以上系统。

c) 判例场景：核心通信线路、关键网络设备和关键计算设备无冗余设计，一旦出现线路或设备故障，就可能导致服务中断。

d) 补偿因素：

1) 对于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，能降低生产环境设备故障所带来的可用性方面影响的情况，可从影响程度、RTO 等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

2) 对于关键计算设备采用虚拟化技术的情况，可从虚拟化环境的硬件冗余和虚拟化计算设备（如虚拟机、虚拟网络设备等）冗余等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.2.6 云计算平台等级低于承载业务系统等级

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：二级及以上系统。

c) 判例场景（任意）：

1) 云计算平台承载高于其安全保护等级（SxAxGx）的业务应用系统；

2) 业务应用系统部署在低于其安全保护等级（SxAxGx）的云计算平台上；

3) 业务应用系统部署在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的云计算平台上。

d) 补偿因素：无。

6.2.7 重要数据传输完整性保护措施缺失

本判例包括以下内容：

a) 标准要求：应采用校验技术或密码技术保证通信过程中数据的完整性。

b) 适用范围：三级及以上系统。

c) 判例场景：网络层或应用层无任何重要数据（如交易类数据、操作指令数据等）传输完整性保护措施，一旦数据遭到篡改，将对系统或个人造成重大影响。

d) 补偿因素：对于重要数据在可控网络中传输的情况，可从已采取的网络管控措施、遭受数据篡改的可能性等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.2.8 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通信过程中数据的保密性。

b) 适用范围：三级及以上系统。

c) 判例场景：鉴别信息、个人敏感信息或重要业务敏感信息等以明文方式在不可控网络环境中传输。

d) 补偿因素：

1) 使用多种身份鉴别技术、限定管理地址等措施，获得的鉴别信息无法直接登录应用系统或设备，可根据实际措施效果，酌情判定风险等级；

2) 可从被测对象的作用、重要程度以及信息泄露后对整个系统或个人产生的影响等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.3 安全区域边界

6.3.1 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：三级及以上系统。

c) 判例场景：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，或边界设备控制策略设置不当，一旦非授权接入无线网络即可访问内部重要资源。

d) 补偿因素：对于必须使用无线网络的场景，可从无线接入设备的管控和身份认证措施、非授权接入的可能性等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.3.2 重要网络区域边界访问控制配置不当

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：二级及以上系统。

c) 判例场景：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）访问控制设备配置不当或控制措施失效，存在较大安全隐患。例如办公网络任意网络终端均可访问核心生产服务器和网络设备；无线网络接入区终端可直接访问生产网络设备等。

d) 补偿因素：无。

6.3.3 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：二级及以上系统。

c) 判例场景（任意）：

1) 二级系统关键网络节点无任何网络攻击行为检测手段，例如未部署入侵检测系统；

2) 三级及以上系统关键网络节点对外部发起的攻击行为无任何防护手段，例如未部署 IPS 入侵防御设备、应用防火墙、反垃圾邮件、态势感知系统或抗 DDoS 设备等；

3) 网络攻击/防护检测措施的策略库、规则库半年及以上未更新，无法满足防护需求。

d) 补偿因素：主机设备部署入侵防范产品，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，酌情判定风险等级。

注 1：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。

注 2：所列举的防护设备仅为举例使用。测评过程中，应分析定级对象所面临的威胁、风险以及安全防护需求，并以此为依据检查是否合理配备了对应的防护设备。

6.3.4 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：三级及以上系统。

c) 判例场景(任意)：

1) 关键网络节点对内部发起的攻击行为无任何检测、防护手段，例如未部署入侵检测系统、IPS 入侵防御设备、态势感知系统等；

2) 网络攻击/防护检测措施的策略库、规则库半年及以上未更新，无法满足防护需求。

d) 补偿因素：

1) 对于主机设备部署入侵防范产品的情况，可从策略库、规则库更新情况，对攻击行为的防护能力等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

2) 对于重要网络区域与其他内部网络之间部署防火墙等访问控制设备，且对访问的目标地址、目标端口、源地址、源端口、访问协议等有严格限制的情况，可从现有措施能否对内部网络攻击起到限制作用等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

3) 对于与互联网完全物理隔离或强逻辑隔离的系统，可从网络、终端采取的管控，攻击源进入内部网络的可能性等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.3.5 恶意代码防范措施缺失

本判例包括以下内容：

a) 标准要求：应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的更新。

b) 适用范围：二级及以上系统。

c) 判例场景(所有)：

1) 主机层无恶意代码检测和清除措施，或恶意代码库一个月以上未更新；

2) 网络层无恶意代码检测和清除措施，或恶意代码库一个月以上未更新。

d) 补偿因素：

1) 对于使用 Linux、Unix、Solaris、CentOS、AIX、Mac 等非 Windows 操作系统的二级系统，主机和网络层均未部署恶意代码检测和清除产品，可从总体防御措施、恶意代码入侵的可能性等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

2) 与互联网完全物理隔离或强逻辑隔离的系统，其网络环境可控，并采取 USB 介质管控、部署主机防护软件、软件白名单等技术措施，能有效防范恶意代码进入被测主机或网络，可根据实际措施效果，酌情判定风险等级；

3) 主机设备采用可信基的防控技术，对设备运行环境进行有效度量，可根据实际措施效果，酌情判定风险等级。

6.3.6 网络安全审计措施缺失

本判例包括以下内容：

a) 标准要求：应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

b) 适用范围：二级及以上系统。

c) 判例场景(所有):

1) 在网络边界、关键网络节点无法对重要的用户行为进行日志审计;

2) 在网络边界、关键网络节点无法对重要安全事件进行日志审计。

d) 补偿因素:无。

注:网络安全审计指通过对网络边界或重要网络节点的流量数据进行分析,从而形成的网络安全审计数据。网络安全审计包括网络流量审计和网络安全事件审计,其中网络流量审计主要是通过对网络流量进行统计、关联分析、识别和筛选,实现对网络中特定重要行为的审计,例如对各种违规的访问协议及其流量的审计、对访问敏感数据的人员行为或系统行为的审计等;网络安全事件审计包括但不限于对网络入侵检测、网络入侵防御、防病毒产品等设备检测到的网络攻击行为、恶意代码传播行为的审计等。

6.4 安全计算环境

6.4.1 网络设备、安全设备和主机设备

6.4.1.1 设备存在弱口令或相同口令

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:二级及以上系统。

c) 判例场景(任意):

1) 网络设备、安全设备、主机设备(包括操作系统、数据库等)存在可登录的弱口令账户(包括空口令、无身份鉴别机制);

2) 大量设备管理员账户口令相同,单台设备口令被破解将导致大量设备被控制。

d) 补偿因素:对于因业务场景需要,使用无法设置口令或口令强度达不到要求的专用设备,可从设备登录方式、物理访问控制、访问权限、其他技术防护措施、相关管理制度落实等角度进行综合风险分析,根据分析结果,酌情判定风险等级。

6.4.1.2 设备鉴别信息防窃听措施缺失

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:二级及以上系统。

c) 判例场景(所有):

1) 网络设备、安全设备、主机设备(包括操作系统、数据库等)的鉴别信息以明文方式在不可控网络环境中传输;

2) 未采取多种身份鉴别技术、限定管理地址等技术措施,鉴别信息被截获后可成功登录设备。

d) 补偿因素:对于设备提供加密、非加密两种管理模式,且其非加密通道无法关闭的情况,可从日常运维使用等角度进行综合风险分析,根据分析结果,酌情判定风险等级。

6.4.1.3 设备未采用多种身份鉴别技术

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：三级及以上系统。

c) 判例场景(所有)：

1) 关键网络设备、关键安全设备、关键主机设备(操作系统)通过不可控网络环境进行远程管理；

2) 设备未采用两种或两种以上鉴别技术对用户身份进行鉴别。

d) 补偿因素：

1) 远程管理过程中，多次采用同一种鉴别技术进行身份鉴别，且每次鉴别信息不相同，例如两次口令认证措施(两次口令不同)，可根据实际措施效果，酌情判定风险等级；

2) 对于采取登录地址限制、绑定管理终端等其他技术手段减轻用户身份被滥用的威胁的情况，可从措施所起到的防护效果等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.1.4 设备默认口令未修改

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：二级及以上系统。

c) 判例场景：网络设备、安全设备、主机设备(包括操作系统、数据库等)默认口令未修改，使用默认口令可以登录设备。

d) 补偿因素：对于因业务场景需要，无法修改专用设备的默认口令的情况，可从设备登录方式、物理访问控制、访问权限、其他技术防护措施、相关管理制度落实等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.1.5 设备安全审计措施缺失

本判例包括以下内容：

a) 标准要求：应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

b) 适用范围：二级及以上系统。

c) 判例场景(所有)：

1) 关键网络设备、关键安全设备、关键主机设备(包括操作系统、数据库等)未开启任何审计功能，无法对重要的用户行为和重要安全事件进行审计；

2) 未采用堡垒机、第三方审计工具等技术手段或所采用的辅助审计措施存在漏记、旁路等缺陷，无法对重要的用户行为和重要安全事件进行溯源。

d) 补偿因素：无。

6.4.1.6 设备审计记录不满足保护要求

本判例包括以下内容：

a) 标准要求：应对审计记录进行保护，定期备份，避免其受到非预期的删除、修改或覆盖等。

b) 适用范围：二级及以上系统。

c) 判例场景(任意)：

1) 关键网络设备、关键安全设备、关键主机设备(包括操作系统、数据库等)的重要操作、安全事件日志可被非预期删除、修改或覆盖等；

2） 关键网络设备、关键安全设备、关键主机设备(包括操作系统、数据库等)的重要操作、安全事件日志的留存时间不满足法律法规规定的要求(不少于六个月)。

d） 补偿因素:对于被测对象上线运行时间不足六个月的情况,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综合风险分析,根据分析结果,酌情判定风险等级。

6.4.1.7 设备开启多余的服务、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:二级及以上系统。

c） 判例场景(所有):

1） 网络设备、安全设备、主机设备(操作系统)开启多余的系统服务、默认共享、高危端口;

2） 未采用地址访问限制、安全防护设备等技术手段,减少系统服务、默认共享、高危端口开启所带来的安全隐患。

d） 补偿因素:对于系统服务、默认共享、高危端口仅能通过可控网络环境访问的情况,可从现有网络防护措施、所面临的威胁情况等角度进行综合风险分析,根据分析结果,酌情判定风险等级。

6.4.1.8 设备管理终端限制措施缺失

本判例包括以下内容:

a） 标准要求:应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

b） 适用范围:二级及以上系统。

c） 判例场景:网络设备、安全设备、主机设备(包括操作系统、数据库等)通过不可控网络环境进行远程管理,未采取终端接入管控、网络地址范围限制等技术手段对管理终端进行限制。

d） 补偿因素:采取多种身份鉴别等技术措施,能够降低管理终端管控不完善所带来的安全风险,可根据实际措施效果,酌情判定风险等级。

6.4.1.9 互联网设备存在已知高危漏洞

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:二级及以上系统。

c） 判例场景(所有):

1） 网络设备、安全设备、主机设备(包括操作系统、数据库等)可通过互联网管理或访问(包括服务、管理模块等);

2） 该设备型号、版本存在外界披露的高危安全漏洞;

3） 未及时采取修补或其他有效防范措施。

d） 补偿因素:通过访问地址限制或其他有效防护措施,使该高危漏洞无法通过互联网被利用,可根据实际措施效果,酌情判定风险等级。

6.4.1.10 内网设备存在可被利用的高危漏洞

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：二级及以上系统。

c) 判例场景(所有)：

1) 网络设备、安全设备、主机设备(包括操作系统、数据库等)仅能通过内部网络管理或访问(包括服务、管理模块等)；

2) 通过验证测试或渗透测试确认设备存在缓冲区溢出、提权漏洞、远程代码执行等可能导致重大安全隐患的漏洞。

d) 补偿因素：对于经过充分测试评估，该设备无法进行漏洞修补的情况，可从物理、网络环境管控情况，发生攻击行为的可能性，现有防范措施等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.1.11 恶意代码防范措施缺失

本判例包括以下内容：

a) 标准要求：应采用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。

b) 适用范围、判例场景和补偿因素参见 6.3.5。

6.4.2 应用系统

6.4.2.1 应用系统口令策略缺失

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：二级及以上系统。

c) 判例场景：应用系统无用户口令长度、复杂度校验机制，例如可设置 6 位以下，单个、相同、连续数字、字母或字符等易猜测的口令。

d) 补偿因素：

1) 应用系统采取多种身份鉴别、访问地址限制等技术措施，获得的口令无法直接登录应用系统，可根据实际措施效果，酌情判定风险等级；

2) 对于仅内网访问的内部管理系统，可从内网管控、人员管控、实际用户口令质量等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

3) 对于部分专用软件、老旧系统等无法添加口令复杂度校验功能的情况，可从登录管控措施、实际用户口令质量、口令更换频率等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

4) 对于特定应用场景中的口令，例如 PIN 码、电话银行系统查询口令等，可从行业要求、行业特点等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.2.2 应用系统存在弱口令

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：二级及以上系统。

c) 判例场景：通过渗透测试或使用常用口令尝试登录，发现应用系统中存在可被登录的空口令、弱口令账户。

d) 补偿因素：

1) 对于互联网前端系统的注册用户存在弱口令的情况，可从对单个用户、整个应用系统所可能造成的影响等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

2) 对于因业务场景需要，无身份鉴别功能或口令强度达不到要求的应用系统，可从登录方式、物理访问控制、访问权限、其他技术防护措施、相关管理制度落实等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.2.3 应用系统口令暴力破解防范机制缺失

本判例包括以下内容：

a) 标准要求：应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

b) 适用范围：二级及以上系统。

c) 判例场景：通过互联网登录的应用系统登录模块未提供有效的口令暴力破解防范机制。

d) 补偿因素：

1) 应用系统采取多种身份鉴别、访问地址限制等技术措施，获得口令无法直接登录应用系统，可根据实际措施效果，酌情判定风险等级；

2) 对于互联网前端系统的注册用户，可从登录后用户获得的业务功能、账户被盗后造成的影响程度等角度进行综合风险分析，根据分析结果，酌情判定风险等级；涉及资金交易、个人隐私、信息发布、重要业务操作等的前端系统，不宜降低风险等级；

3) 对于无法添加登录失败处理功能的应用系统，可从登录地址、登录终端限制等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.2.4 应用系统鉴别信息明文传输

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：二级及以上系统。

c) 判例场景：应用系统的用户鉴别信息以明文方式在不可控网络环境中传输。

d) 补偿因素：应用系统采取多种身份鉴别、访问地址限制等技术措施，获得口令无法直接登录应用系统，可根据实际措施效果，酌情判定风险等级。

6.4.2.5 应用系统未采用多种身份鉴别技术

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：三级及以上系统。

c) 判例场景：通过互联网登录的系统，在进行涉及大额资金交易、核心业务、关键指令等的重要操作前未使用两种或两种以上鉴别技术对用户身份进行鉴别。

d) 补偿因素：

1) 在身份鉴别过程中，多次采用同一种鉴别技术进行身份鉴别，且每次鉴别信息不相同，例如两次口令认证措施(两次口令不同)，可根据实际措施效果，酌情判定风险等级；

2) 在完成重要操作前的不同阶段使用不同的鉴别方式进行身份鉴别，可根据实际措施效果，

酌情判定风险等级；

3） 对于用户群体为互联网个人用户的情况，可从行业主管部门的要求、用户身份被滥用后对系统或个人造成的影响等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

4） 对于采取登录地址限制、绑定设备等其他技术手段减轻用户身份被滥用的威胁的情况，可从措施所起到的防护效果等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.2.6 应用系统默认口令未修改

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：二级及以上系统。

c） 判例场景：应用系统默认口令未修改，使用默认口令可以登录系统。

d） 补偿因素：对于因业务场景需要，无法修改应用系统的默认口令的情况，可从设备登录方式、物理访问控制、访问权限、其他技术防护措施、相关管理制度落实等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.2.7 应用系统访问控制机制存在缺陷

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：二级及以上系统。

c） 判例场景：应用系统访问控制策略存在缺陷，可越权访问系统功能模块或查看、操作其他用户的数据，例如存在非授权访问系统功能模块、平行权限漏洞、低权限用户越权访问高权限功能模块等。

d） 补偿因素：

1） 对于部署在可控网络环境的应用系统，可从现有的防护措施、用户行为监控等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

2） 可从非授权访问模块的重要程度、影响程度，越权访问的难度等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.2.8 应用系统安全审计措施缺失

本判例包括以下内容：

a） 标准要求：应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

b） 适用范围：二级及以上系统。

c） 判例场景（所有）：

1） 应用系统无任何日志审计功能，无法对重要的用户行为和重要安全事件进行审计；

2） 未采取其他审计措施或其他审计措施存在漏记、旁路等缺陷，无法对应用系统重要的用户行为和重要安全事件进行溯源。

d） 补偿因素：对于日志记录不全或有审计数据但无直观展示等情况，可从审计记录内容、事件追溯范围等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.2.9 应用系统审计记录不满足保护要求

本判例包括以下内容：

a) 标准要求：应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
b) 适用范围：二级及以上系统。
c) 判例场景（任意）：
   1) 应用系统业务操作类、安全类等重要日志可被恶意删除、修改或覆盖等；
   2) 应用系统业务操作类、安全类等重要日志的留存时间不满足法律法规规定的相关要求（不少于六个月）。
d) 补偿因素：
   1) 对于应用系统提供历史日志删除等功能的情况，可从历史日志时间范围、追溯时效和意义等角度进行综合风险分析，根据分析结果，酌情判定风险等级；
   2) 对于应用系统未正式上线或上线时间不足六个月等情况，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综合风险分析，根据分析结果，酌情判定风险等级。

6.4.2.10 应用系统数据有效性检验功能缺失

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：二级及以上系统。
c) 判例场景（所有）：
   1) 应用系统存在 SQL 注入、跨站脚本、上传漏洞等可能导致敏感数据泄露、网页篡改、服务器被入侵等安全事件的发生，造成严重后果的高危漏洞；
   2) 未采取 WEB 应用防火墙、云盾等技术防护手段对高危漏洞进行防范。
d) 补偿因素：对于不与互联网交互的内网系统，可从应用系统的重要程度、漏洞影响程度、漏洞利用难度、内部网络管控措施等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.2.11 应用系统存在可被利用的高危漏洞

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：二级及以上系统。
c) 判例场景（所有）：
   1) 应用系统所使用的环境、框架、组件或业务功能等存在可被利用的高危漏洞或严重逻辑缺陷，可能导致敏感数据泄露、网页篡改、服务器被入侵、绕过安全验证机制非授权访问等安全事件的发生；
   2) 未采取其他有效技术手段对高危漏洞或逻辑缺陷进行防范。
d) 补偿因素：对于不与互联网交互的内网系统，可从应用系统的重要程度、漏洞影响程度、漏洞利用难度、内部网络管控措施等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.3 数据安全

6.4.3.1 重要数据传输完整性保护措施缺失

本判例包括以下内容：
a) 标准要求：应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

b) 适用范围、判例场景和补偿因素参见 6.2.7。

6.4.3.2 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、判例场景和补偿因素参见 6.2.8。

6.4.3.3 重要数据存储保密性保护措施缺失

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：三级及以上系统。

c) 判例场景(所有)：

1) 鉴别信息、个人敏感信息、行业主管部门规定需加密存储的数据等以明文方式存储；

2) 未采取数据访问限制、部署数据库防火墙、使用数据防泄露产品等其他有效保护措施。

d) 补偿因素：无。

6.4.3.4 数据备份措施缺失

本判例包括以下内容：

a) 标准要求：应提供重要数据的本地数据备份与恢复功能。

b) 适用范围：二级及以上系统。

c) 判例场景(任意)：

1) 应用系统未提供任何重要数据备份措施，一旦遭受数据破坏，将无法进行数据恢复；

2) 重要数据、源代码等备份到互联网网盘、代码托管平台等不可控环境，可能造成重要信息泄露。

d) 补偿因素：对于采用多数据中心或冗余方式部署，重要数据存在多个副本的情况，可从技术实现效果、恢复效果等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.3.5 异地备份措施缺失

本判例包括以下内容：

a) 标准要求：应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

b) 适用范围：三级及以上系统。

c) 判例场景：数据容灾要求较高的定级对象，无异地数据灾备措施，或异地备份机制无法满足业务或行业主管部门要求。

d) 补偿因素：无。

6.4.3.6 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：三级及以上系统。

c) 判例场景：对于数据处理可用性要求较高的定级对象，处理重要数据的设备，例如服务器、数据

库等未采用热冗余技术，发生故障后可能导致系统停止运行。

d) 补偿因素：对于采取其他技术防范措施的情况，可从技术实现效果、恢复方式、RTO 等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.3.7 未建立异地灾难备份中心

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：四级系统。

c) 判例场景：容灾、可用性要求较高的系统，未设立异地应用级容灾中心，或异地应用级容灾中心无法实现业务切换。

d) 补偿因素：对于采取其他技术防范措施的情况，可从技术实现效果、恢复方式、RTO 等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.4.3.8 鉴别信息释放措施失效

本判例包括以下内容：

a) 标准要求：应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

b) 适用范围：二级及以上系统。

c) 判例场景(所有)：

1) 身份鉴别信息释放或清除机制存在缺陷，利用剩余鉴别信息，可非授权访问系统资源或进行操作；

2) 无其他技术措施，消除或降低非授权访问系统资源或进行操作所带来的影响。

d) 补偿因素：无。

6.4.3.9 敏感数据释放措施失效

本判例包括以下内容：

a) 标准要求：应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

b) 适用范围：三级及以上系统。

c) 判例场景：个人敏感信息、业务敏感信息等敏感数据释放或清除机制存在缺陷，可造成敏感数据泄露。

d) 补偿措施：无。

6.4.3.10 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：二级及以上系统。

c) 判例场景(任意)：

1) 在未授权情况下，采集、存储用户个人隐私信息；

2) 采集、保存法律法规、主管部门严令禁止采集、保存的用户隐私信息。

d) 补偿因素：无。

6.4.3.11 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：二级及以上系统。
c) 判例场景(任意)：
   1) 未按国家、行业主管部门以及标准的相关规定使用个人信息，例如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，非法买卖、泄露用户个人信息等情况；
   2) 个人信息可非授权访问，例如未严格控制个人信息查询以及导出权限等。
d) 补偿因素：无。

6.4.3.12 云服务客户数据和用户个人信息违规出境

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：二级及以上云计算平台。
c) 判例场景：云服务客户数据、用户个人信息等数据出境未遵循国家相关规定。
d) 补偿因素：无。

6.5 安全管理中心

6.5.1 运行监控措施缺失

本判例包括以下内容：
a) 标准要求：应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。
b) 适用范围：高可用性的三级及以上系统。
c) 判例场景：对网络链路、安全设备、网络设备和服务器等的运行状况无任何监控措施，发生故障后无法及时对故障进行定位和处理。
d) 补偿因素：无。

6.5.2 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：三级及以上系统。
c) 判例场景：关键网络设备、关键安全设备、关键主机设备(包括操作系统、数据库等)的重要操作、安全事件等审计记录的留存不满足法律法规规定的相关要求(不少于六个月)。
d) 补偿因素：对于被测对象上线运行时间不足六个月的情况，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综合风险分析，根据分析结果，酌情判定风险等级。

6.5.3 安全事件发现处置措施缺失

本判例包括以下内容：
a) 标准要求：应能对网络中发生的各类安全事件进行识别、报警和分析。
b) 适用范围：三级及以上系统。
c) 判例场景：无法对网络中发生的网络攻击、恶意代码传播等安全事件进行识别、报警和分析。

d) 补偿因素：对于与互联网完全物理隔离的系统，可从网络管控措施、介质管控措施、应急措施等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.6 安全管理制度和机构

6.6.1 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：二级及以上系统。

c) 判例场景：未建立任何与安全管理活动相关的管理制度或相关管理制度无法适用于当前定级对象。

d) 补偿因素：无。

6.6.2 未建立网络安全领导小组

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：三级及以上系统。

c) 判例场景：未成立指导和管理信息安全工作的委员会或领导小组，或其最高领导未由单位主管领导担任或授权。

d) 补偿因素：无。

6.7 安全管理人员

6.7.1 未开展安全意识和安全技能培训

本判例包括以下内容：

a) 标准要求：应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

b) 适用范围：二级及以上系统。

c) 判例场景：未定期组织开展与安全意识、安全技能相关的培训。

d) 补偿因素：无。

6.7.2 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，经批准后再由专人开设账户、分配权限，并登记备案。

b) 适用范围：二级及以上系统。

c) 判例场景(所有)：

1) 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；

2) 无法提供外部人员接入受控网络访问系统的申请、审批等相关记录证据。

d) 补偿因素：无。

6.8 安全建设管理

6.8.1 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的采购和使用符合国家有关规定。

b) 适用范围：三级及以上系统。

c) 判例场景：网络安全产品的采购和使用违反国家有关规定，“例如采购、使用的安全产品未获得销售许可证、未通过国家有关机构的安全检测等”。

d) 补偿因素：对于使用开源、自研的网络安全产品（非销售类安全产品）的情况，可从该网络安全产品的作用、功能、使用场景、国家及行业主管部门的要求等角度进行综合风险分析，充分考虑该网络安全产品未通过专业机构检测，一旦出现功能缺陷、安全漏洞等问题对定级对象带来的影响，根据分析结果，酌情判定风险等级。

6.8.2 外包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：三级及以上系统。

c) 判例场景（所有）：

1) 涉及国计民生的核心业务系统，被测单位未对开发单位开发的系统进行源代码安全审查；

2) 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) 补偿因素：

1) 定级对象建成时间较长，虽未进行源代码安全审查，但定期进行安全检测，并能够提供安全检测报告，且当前管理制度中明确规定外包开发代码审计，可根据实际措施效果，酌情判定风险等级；

2) 对于被测单位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的情况，可从已采取的技术防范措施等角度进行综合风险分析，根据分析结果，酌情判定风险等级；

3) 对于部分模块外包开发的情况，可从外包开发模块的用途、重要性等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.8.3 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：三级及以上系统。

c) 判例场景：系统上线前未开展任何安全性测试，或未对测试发现的高风险问题进行安全评估和整改。

d) 补偿因素：定级对象建成时间较长，上线前虽未进行安全性测试，但上线后定期开展安全检测，且检测未发现高危风险隐患，可根据实际措施效果，酌情判定风险等级。

注：安全测试内容包括但不限于等级保护测评、扫描渗透测试、安全功能验证、源代码安全审核等。

6.9 安全运维管理

6.9.1 运维工具管控措施缺失

本判例包括以下内容：

a) 标准要求：应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。

b) 适用范围：三级及以上系统。

c) 判例场景(任意)：

1) 运维工具(特别是未商业化的运维工具)使用前未进行有效性检查，例如病毒、漏洞扫描等；

2) 对运维工具接入网络未进行严格的控制和审批；

3) 运维工具使用结束后未要求删除可能临时存放的敏感数据。

d) 补偿因素：无。

6.9.2 设备外联管控措施缺失

本判例包括以下内容：

a) 标准要求：应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

b) 适用范围：三级及以上系统。

c) 判例场景(所有)：

1) 管理制度中无与外部连接的授权和审批流程，也未定期进行相关的巡检；

2) 无技术手段对违规上网及其他违反网络安全策略的行为进行有效控制、检查、阻断。

d) 补偿因素：无。

6.9.3 外来接入设备恶意代码检查措施缺失

本判例包括以下内容：

a) 标准要求：应加强所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。

b) 适用范围：二级及以上系统。

c) 判例场景(所有)：

1) 管理制度中未明确外来计算机或存储设备接入安全操作规程；

2) 外来计算机或存储设备接入网络前未进行恶意代码检查。

d) 补偿因素：无。

6.9.4 变更管理制度缺失

本判例包括以下内容：

a) 标准要求：应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

b) 适用范围：二级及以上系统。

c) 判例场景(所有)：

1) 缺少相关变更管理制度，或变更管理制度中缺少变更管理流程、变更内容分析与论证、变

更方案审批流程等相关内容；

2） 实际变更过程中无任何流程、人员、方案等审核环节及记录。

d） 补偿因素：无。

6.9.5 数据备份策略缺失

本判例包括以下内容：

a） 标准要求：应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

b） 适用范围：二级及以上系统。

c） 判例场景：无备份与恢复等相关的安全管理制度，或未按照相关策略落实数据备份和恢复措施。

d） 补偿因素：

1） 虽未建立相关数据备份与恢复制度，但实际工作中实施了数据备份及恢复测试，且能够提供相关证据，备份与恢复措施符合业务需要，可根据实际措施效果，酌情判定风险等级；

2） 对于定级对象还未正式上线的情况，可从已制定的备份恢复策略、计划采取的技术措施，例如环境、存储等是否满足所规定的备份恢复策略要求等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.9.6 重要事件应急预案缺失

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：二级及以上系统。

c） 判例场景（任意）：

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，一旦出现应急事件，无法合理有序地进行应急事件处置。

d） 补偿因素：无。

6.9.7 未对应急预案进行培训演练

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：三级及以上系统。

c） 判例场景：未定期（至少每年一次）对相关人员进行应急预案培训，未根据不同的应急预案进行演练，无法提供应急预案培训和演练记录。

d） 补偿因素：对于定级对象还未正式上线的情况，可从培训演练制度、相关培训计划等角度进行综合风险分析，根据分析结果，酌情判定风险等级。

6.9.8 云计算平台运维方式不当

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，在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：二级及以上云计算平台。

c） 判例场景（所有）：

1） 云计算平台的运维地点不在中国境内；

2） 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） 补偿因素：无。

附 录 A
（资料性附录）
GB/T 22239—2019 中第三级安全要求与本文件判例对应关系

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 中第三级安全要求的对应关系。

表 A.1 GB/T 22239—2019 中第三级安全要求与本文件判例对应关系

序号	层面	控制点	标准要求	对应条款号	本文件判例	适用范围
1	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	机房出入口访问控制措施缺失	二级及以上系统
2		防盗窃和防破坏	应设置机房防盗报警系统或设置有专人值守的视频监控系统	6.1.2	机房防盗措施缺失	三级及以上系统
3		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	6.1.3	机房防火措施缺失	二级及以上系统
4		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	6.1.4	机房短期备用电力供应措施缺失	二级及以上系统
5			应提供应急供电设施	6.1.5	机房应急供电措施缺失	高可用性的四级系统
6		基础设施位置	应保证云计算基础设施位于中国境内	6.1.6	云计算基础设施物理位置不当	二级及以上云计算平台
7	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	网络设备业务处理能力不足	高可用性的三级及以上系统
8			应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址	6.2.2	网络区域划分不当	二级及以上系统
9			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	6.2.3	网络边界访问控制设备不可控	二级及以上系统
10				6.2.4	重要网络区域边界访问控制措施缺失	二级及以上系统
11			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	6.2.5	关键线路和设备冗余措施缺失	高可用性的三级及以上系统
12			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	6.2.6	云计算平台等级低于承载业务系统等级	二级及以上系统
13		通信传输	应采用校验技术或密码技术保证通信过程中数据的完整性	6.2.7	重要数据传输完整性保护措施缺失	三级及以上系统
14			应采用密码技术保证通信过程中数据的保密性	6.2.8	重要数据明文传输	三级及以上系统

表 A.1 GB/T 22239—2019 中第三级安全要求与本文件判例对应关系（续）

序号	层面	控制点	标准要求	对应条款号	本文件判例	适用范围
15	安全区域边界	边界防护	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	无线网络管控措施缺失	三级及以上系统
16		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	重要网络区域边界访问控制配置不当	二级及以上系统
17		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	外部网络攻击防御措施缺失	二级及以上系统
18			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	6.3.4	内部网络攻击防御措施缺失	三级及以上系统
19		恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新	6.3.5	恶意代码防范措施缺失	二级及以上系统
20		安全审计	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	6.3.6	网络安全审计措施缺失	二级及以上系统
21	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	设备存在弱口令或相同口令	二级及以上系统
22				6.4.2.1	应用系统口令策略缺失	二级及以上系统
23				6.4.2.2	应用系统存在弱口令	二级及以上系统
24			应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施	6.4.2.3	应用系统口令暴力破解防范机制缺失	二级及以上系统
25			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	设备鉴别信息防窃听措施缺失	二级及以上系统
26				6.4.2.4	应用系统鉴别信息明文传输	二级及以上系统
27			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	6.4.1.3	设备未采用多种身份鉴别技术	三级及以上系统
28				6.4.2.5	应用系统未采用多种身份鉴别技术	三级及以上系统
29		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	6.4.1.4	设备默认口令未修改	二级及以上系统
30				6.4.2.6	应用系统默认口令未修改	二级及以上系统
31			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	6.4.2.7	应用系统访问控制机制存在缺陷	二级及以上系统

表 A.1 GB/T 22239—2019 中第三级安全要求与本文件判例对应关系（续）

序号	层面	控制点	标准要求	对应条款号	本文件判例	适用范围
32	安全计算环境	安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	6.4.1.5	设备安全审计措施缺失	二级及以上系统
33				6.4.2.8	应用系统安全审计措施缺失	二级及以上系统
34			应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	6.4.1.6	设备审计记录不满足保护要求	二级及以上系统
35				6.4.2.9	应用系统审计记录不满足保护要求	二级及以上系统
36		入侵防范	应关闭不需要的系统服务、默认共享和高危端口	6.4.1.7	设备开启多余的服务、高危端口	二级及以上系统
37			应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制	6.4.1.8	设备管理终端限制措施缺失	二级及以上系统
38			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	6.4.2.10	应用系统数据有效性检验功能缺失	二级及以上系统
39			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	6.4.1.9	互联网设备存在已知高危漏洞	二级及以上系统
40				6.4.1.10	内网设备存在可被利用的高危漏洞	二级及以上系统
41				6.4.2.11	应用系统存在可被利用的高危漏洞	二级及以上系统
42		恶意代码防范	应采用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	6.4.1.11	恶意代码防范措施缺失	二级及以上系统
43		数据完整性	应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	6.4.3.1	重要数据传输完整性保护措施缺失	三级及以上系统
44		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	6.4.3.2	重要数据明文传输	三级及以上系统
45			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	6.4.3.3	重要数据存储保密性保护措施缺失	三级及以上系统

表 A.1 GB/T 22239—2019 中第三级安全要求与本文件判例对应关系（续）

序号	层面	控制点	标准要求	对应条款号	本文件判例	适用范围
46	安全计算环境	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	6.4.3.4	数据备份措施缺失	二级及以上系统
47			应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地	6.4.3.5	异地备份措施缺失	三级及以上系统
48			应提供重要数据处理系统的热冗余，保证系统的高可用性	6.4.3.6	数据处理系统冗余措施缺失	三级及以上系统
49			应建立异地灾难备份中心，提供业务应用的实时切换	6.4.3.7	未建立异地灾难备份中心	四级系统
50		剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	6.4.3.8	鉴别信息释放措施失效	二级及以上系统
51			应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	6.4.3.9	敏感数据释放措施失效	三级及以上系统
52		个人信息保护	应仅采集和保存业务必需的用户个人信息	6.4.3.10	违规采集和存储个人信息	二级及以上系统
53			应禁止未授权访问和非法使用用户个人信息	6.4.3.11	违规访问和使用个人信息	二级及以上系统
54		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	6.4.3.12	云服务客户数据和用户个人信息违规出境	二级及以上云计算平台
55	安全管理中心	集中管控	应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测	6.5.1	运行监控措施缺失	高可用性的三级及以上系统
56			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	6.5.2	审计记录存储时间不满足要求	三级及以上系统
57			应能对网络中发生的各类安全事件进行识别、报警和分析	6.5.3	安全事件发现处置措施缺失	三级及以上系统
58	安全管理制度和机构	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	管理制度缺失	二级及以上系统
59		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	6.6.2	未建立网络安全领导小组	三级及以上系统

表 A.1 GB/T 22239—2019 中第三级安全要求与本文件判例对应关系（续）

序号	层面	控制点	标准要求	对应条款号	本文件判例	适用范围
60	安全管理人员	安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施	6.7.1	未开展安全意识和安全技能培训	二级及以上系统
61		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请，批准后由专人开设账户、分配权限，并登记备案	6.7.2	外部人员接入网络管理措施缺失	二级及以上系统
62	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	6.8.1	违规采购和使用网络安全产品	三级及以上系统
63		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	6.8.2	外包开发代码审计措施缺失	三级及以上系统
64		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	6.8.3	上线前未开展安全测试	三级及以上系统
65	安全运维管理	网络和系统安全管理	应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据	6.9.1	运维工具管控措施缺失	三级及以上系统
66			应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为	6.9.2	设备外联管控措施缺失	三级及以上系统
67		恶意代码防范管理	应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等	6.9.3	外来接入设备恶意代码检查措施缺失	二级及以上系统
68		变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施	6.9.4	变更管理制度缺失	二级及以上系统
69		备份与恢复管理	应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等	6.9.5	数据备份策略缺失	二级及以上系统
70		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	6.9.6	重要事件应急预案缺失	二级及以上系统
71			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	6.9.7	未对应急预案进行培训演练	三级及以上系统
72		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	6.9.8	云计算平台运维方式不当	二级及以上云计算平台

附 录 B
（资料性附录）
高风险判例整改建议

针对本文件提出的高风险场景，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。

表 B.1 高风险判例对应整改建议

序号	条款号	判例	整改建议
1	6.1.1	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	机房防盗措施缺失	建议机房部署防盗报警系统或设置有专人值守的视频监控系统，如发生盗窃事件可及时告警或进行追溯，为机房环境的安全可控提供保障
3	6.1.3	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
4	6.1.4	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
5	6.1.5	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
6	6.1.6	云计算基础设施物理位置不当	建议在中国境内部署云计算服务器、存储设备、网络设备、云管理平台、信息系统等运行业务和承载数据的软、硬件等云计算基础设施
7	6.2.1	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
8	6.2.2	网络区域划分不当	建议对网络环境进行合理规划，根据各工作职能、重要性和所涉及信息的重要程度等因素，划分不同网络区域，便于各网络区域之间落实访问控制策略
9	6.2.3	网络边界访问控制设备不可控	建议部署或租用自主控制的边界访问控制设备，且对相关设备进行合理配置，确保网络边界访问控制措施有效、可控
10	6.2.4	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
11	6.2.5	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
12	6.2.6	云计算平台等级低于承载业务系统等级	建议云服务客户选择已通过等级保护测评（测评报告在有效期之内，测评结论为中及以上），且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

表 B.1　高风险判例对应整改建议（续）

序号	条款号	判例	整改建议
13	6.2.7 6.4.3.1	重要数据传输完整性保护措施缺失	建议采用校验技术或密码技术保证通信过程中数据的完整性，相关密码技术符合国家密码管理部门的规定
14	6.2.8 6.4.3.2	重要数据明文传输	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部门的规定
15	6.3.1	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的可能性
16	6.3.2	重要网络区域边界访问控制配置不当	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
17	6.3.3	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 攻击设备等），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
18	6.3.4	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的攻击等）。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
19	6.3.5 6.4.1.11	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，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
20	6.3.6	网络安全审计措施缺失	建议在网络边界、关键网络节点处部署具备网络行为审计以及网络安全审计功能的设备（例如网络安全审计系统、网络流量分析设备、入侵防御设备、态势感知设备等），并保留相关审计数据，同时设备审计范围覆盖每个用户，能够对重要的用户行为和重要安全事件进行日志审计，便于对相关事件或行为进行追溯
21	6.4.1.1	设备存在弱口令或相同口令	建议删除或修改账户口令，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
22	6.4.1.2	设备鉴别信息防窃听措施缺失	建议尽可能避免通过不可控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

表 B.1　高风险判例对应整改建议（续）

序号	条款号	判例	整改建议
23	6.4.1.3	设备未采用多种身份鉴别技术	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或令牌等鉴别方式，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双因素认证的场景，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
24	6.4.1.4	设备默认口令未修改	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
25	6.4.1.5	设备安全审计措施缺失	建议在关键网络设备、关键安全设备、关键主机设备（包括操作系统、数据库等）、运维终端性能允许的前提下，开启用户操作类和安全事件类审计策略；若性能不允许，建议使用第三方日志审计工具，实现对相关设备操作与安全行为的全面审计记录，保证发生安全问题时能够及时溯源
26	6.4.1.6	设备审计记录不满足保护要求	建议对设备的重要操作、安全事件日志进行妥善保存，避免受到非预期的删除、修改或覆盖等，留存时间不少于六个月，符合法律法规的相关要求
27	6.4.1.7	设备开启多余的服务、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，减少安全隐患
28	6.4.1.8	设备管理终端限制措施缺失	建议通过地址限制、准入控制等技术手段，对管理终端进行管控和限制
29	6.4.1.9	互联网设备存在已知高危漏洞	建议订阅安全厂商漏洞推送或本地安装安全软件，及时了解漏洞动态，在充分测试评估的基础上，弥补高危安全漏洞
30	6.4.1.10	内网设备存在可被利用的高危漏洞	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
31	6.4.2.1	应用系统口令策略缺失	建议应用系统对用户口令长度、复杂度进行校验，如要求用户口令长度至少为 8 位，由数字、字母或特殊字符中的 2 种组成；对于 PIN 码等特殊用途的口令，应设置弱口令库，通过对比方式，提高用户口令质量
32	6.4.2.2	应用系统存在弱口令	建议应用系统通过口令长度、复杂度校验、常用或弱口令库比对等方式，提高应用系统口令质量
33	6.4.2.3	应用系统口令暴力破解防范机制缺失	建议应用系统提供登录失败处理功能（如账户或登录地址锁定等），防止攻击者进行口令暴力破解
34	6.4.2.4	应用系统鉴别信息明文传输	互联网可访问的应用系统，建议用户身份鉴别信息采用加密方式传输，防止鉴别信息在网络传输过程中被窃听

表 B.1　高风险判例对应整改建议（续）

序号	条款号	判例	整改建议
35	6.4.2.5	应用系统未采用多种身份鉴别技术	建议应用系统增加除用户名、口令以外的身份鉴别技术，如基于密码技术的动态口令或令牌、生物鉴别方式等，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
36	6.4.2.6	应用系统默认口令未修改	建议应用系统重命名或删除默认管理员账户，修改默认密码，使其具备一定的强度，增强账户安全性
37	6.4.2.7	应用系统访问控制机制存在缺陷	建议完善访问控制措施，对系统重要页面、功能模块重新进行身份鉴别、权限校验，确保应用系统不存在访问控制失效情况
38	6.4.2.8	应用系统安全审计措施缺失	建议应用系统完善审计模块，对重要用户操作、行为进行日志审计，审计范围不仅针对前端用户的操作、行为，也包括后台管理员的重要操作
39	6.4.2.9	应用系统审计记录不满足保护要求	建议对应用系统重要操作类、安全类等日志进行妥善保存，避免受到非预期的删除、修改或覆盖等，留存时间不少于六个月，符合法律法规的相关要求
40	6.4.2.10	应用系统数据有效性检验功能缺失	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
41	6.4.2.11	应用系统存在可被利用的高危漏洞	建议定期对应用系统进行漏洞扫描、渗透测试等技术检测，对可能存在的已知漏洞、逻辑漏洞，在充分测试评估后及时进行修补，减少安全隐患
42	6.4.3.3	重要数据存储保密性保护措施缺失	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
43	6.4.3.4	数据备份措施缺失	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
44	6.4.3.5	异地备份措施缺失	建议设置异地灾备机房，并利用通信网络将重要数据实时备份至备份场地；灾备机房的距离应满足行业主管部门的相关要求，例如金融行业应符合 JR/T 0071 的相关要求
45	6.4.3.6	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
46	6.4.3.7	未建立异地灾难备份中心	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
47	6.4.3.8	鉴别信息释放措施失效	建议完善鉴别信息释放或清除机制，确保在执行释放或清除相关操作后，鉴别信息得到完全释放或清除
48	6.4.3.9	敏感数据释放措施失效	建议完善敏感数据释放或清除机制，确保在执行释放或清除相关操作后，敏感数据得到完全释放或清除

表 B.1　高风险判例对应整改建议（续）

序号	条款号	判例	整改建议
49	6.4.3.10	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 GB/T 35273—2020),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
50	6.4.3.11	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 GB/T 35273—2020),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
51	6.4.3.12	云服务客户数据和用户个人信息违规出境	建议云服务客户数据、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
52	6.5.1	运行监控措施缺失	建议部署统一监控平台或运维监控软件对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测
53	6.5.2	审计记录存储时间不满足要求	建议部署日志服务器,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
54	6.5.3	安全事件发现处置措施缺失	建议根据系统场景需要,部署 IPS,应用防火墙、防毒墙(杀毒软件)、垃圾邮件网关、新型网络攻击防护等防护设备,对网络中发生的各类安全事件进行识别、报警和分析,确保相关安全事件得到及时发现和及时处置
55	6.6.1	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
56	6.6.2	未建立网络安全领导小组	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
57	6.7.1	未开展安全意识和安全技能培训	建议制定与安全意识、安全技能相关的教育培训计划,并按计划开展相关培训,增强员工整体安全意识及安全技能,有效支撑业务系统的安全稳定运行
58	6.7.2	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
59	6.8.1	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
60	6.8.2	外包开发代码审计措施缺失	建议对开放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
61	6.8.3	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

表 B.1　高风险判例对应整改建议（续）

序号	条款号	判例	整改建议
62	6.9.1	运维工具管控措施缺失	建议在管理制度及实际运维过程中加强运维工具的管控，明确运维工具经过审批及必要的安全检查后才能接入使用，使用完成后应对工具中的数据进行检查，删除敏感数据，避免敏感数据泄露；尽可能使用商业化的运维工具，严禁运维人员私自下载第三方未商业化的运维工具
63	6.9.2	设备外联管控措施缺失	建议在制度上明确所有与外部连接的授权和批准，并定期对外联行为进行检查，及时关闭不再使用的外部连接；在技术上采用终端管理系统等具有相关功能的安全产品实现违规外联和违规接入的有效控制措施，并合理设置安全策略，在出现违规外联和违规接入时能第一时间进行检测和阻断
64	6.9.3	外来接入设备恶意代码检查措施缺失	建议制定外来接入设备检查制度，任何外来计算机或存储设备接入系统前必须经过恶意代码检查，在通过检查并经过审批后，外来设备方可接入系统
65	6.9.4	变更管理制度缺失	建议系统的任何变更均需要管理流程，必须组织相关人员（业务部门人员与系统运维人员等）进行分析与论证，在确定必须变更后，制定详细的变更方案，在经过审批后，先对系统进行备份，再实施变更
66	6.9.5	数据备份策略缺失	建议制定备份与恢复的相关制度，明确数据备份策略和数据恢复策略，以及备份程序和恢复程序，实现重要数据的定期备份与恢复测试，保证备份数据的高可用性与可恢复性
67	6.9.6	重要事件应急预案缺失	建议根据系统实际情况，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，并对应急预案进行演练
68	6.9.7	未对应急预案进行培训演练	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
69	6.9.8	云计算平台运维方式不当	建议云计算平台在中国境内设置运维场所，如需从境外对境内云计算平台实施运维操作，则应遵循国家相关规定

参 考 文 献

[1] 中华人民共和国网络安全法
[2] 中华人民共和国密码法
[3] 网络安全审查办法
[4] GB/T 20984—2007 信息安全技术 信息安全风险评估规范
[5] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求