ICS xx. xxx
L xx

团 体 标 准

T/ISEAA 001-2019

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

（征求意见稿）

2XXX-XX-XX 发布　　200X-XX-XX 实施

中关村信息安全测评联盟 发布

目　次

前　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能力，规范测评机构对系统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了等保测评行业指引性文件——《网络安全等级保护测评高风险判定指引》（简称“判定指引”），旨在推动等保测评工作中风险判断更加标准化，规范化。从而规范等级保护测评过程，提升等级保护测评活动的质量。

本指引是依据 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》有关条款，对测评过程中发现的安全性问题如何进行高风险判断的指引性文件。指引内容包括对应要求、判例内容、适用范围、补偿措施、整改建议等要素。

需要指出的是，本指引无法涵盖所有高风险案例，测评机构须结合实际情况，对安全问题所引发的风险等级做出客观判断。

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由中关村信息安全测评联盟提出并归口。

本标准起草单位：

本标准主要起草人：

网络安全等级保护测评高风险判定指引

1　范围

本指引适用于网络安全等级保护测评活动、安全检查等工作。信息系统建设单位亦可参考本指引描述的案例编制系统安全需求。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 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

《中华人民共和国网络安全法》

3　术语和定义

3.1　可用性要求较高的系统

指出现短时故障无法提供服务，可能对社会秩序、公共利益等造成严重损害的系统，即可用性级别大于等于99.9%，年度停机时间小于等于8.8小时的系统；一般包括但不限于银行、证券、非金融支付机构、互联网金融等交易类系统，提供公共服务的民生类系统、工业控制类系统等。

3.2　核心网络设备

指部署在核心网络节点的关键设备，一般包括但不限于核心交换机、核心路由器、核心边界防火墙等。

3.3　数据传输完整性要求较高的系统

指数据在传输过程中遭受恶意破坏或篡改，可能造成较大的财产损失，或造成严重破坏的系统，一般包括但不限于银行、证券、非金融支付机构、互联网金融等交易类系统等。

3.4　不可控网络环境

指互联网、公共网络环境、内部办公环境等无管控措施，可能存在恶意攻击、数据窃听等安全隐患的网络环境。

3.5　可被利用的漏洞

指可被攻击者用来进行网络攻击，可造成严重后果的漏洞，一般包括但不限于缓冲区溢出、提权漏洞、远程代码执行、严重逻辑缺陷、敏感数据泄露等。

4　安全物理环境

4.1　物理访问控制

4.1.1 机房出入口无控制措施

对应要求：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。

判例内容：机房出入口区域无任何访问控制措施，机房无电子或机械门锁，机房入口也无专人值守；办公或外来人员可随意进出机房，无任何管控、监控措施，存在较大安全隐患，可判高风险。

适用范围：所有系统。

满足条件（同时）：

a) 机房出入口区域无任何访问控制措施；

b) 机房无电子或机械门锁，机房入口也无专人值守；

c) 办公或外来人员可随意进出机房，无任何管控、监控措施。

补偿措施：如机房无电子门禁系统，但有其他防护措施，如机房出入配备24小时专人值守，采用摄像头实时监控等，可酌情降低风险等级。

整改建议：机房出入口配备电子门禁系统，通过电子门禁鉴别、记录进入的人员信息。

4.1.2 云计算基础设施物理位置不当

对应要求：应保证云计算基础设施位于中国境内。

判例内容：云计算基础设施（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，可判高风险。

适用范围：云计算平台。

满足条件：

云计算基础设施（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。

补偿措施：无。

整改建议：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应部署在中国境内。

4.2 防盗窃和防破坏

4.2.1 机房无防盗措施

对应要求：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。

判例内容：机房无防盗报警系统，也未设置有专人值守的视频监控系统，出现盗窃事件无法进行告警、追溯的，可判高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统所在机房；

b) 机房无防盗报警系统；

c) 未设置有专人值守的视频监控系统；

d) 机房环境不可控；

e) 如发生盗窃事件无法进行告警、追溯。

补偿措施：如果机房有专人24小时值守，并且能对进出人员进出物品进行登记的（如部分IDC机房有要求设备进出需登记），可酌情降低风险等级。

整改建议：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，确保机房环境的安全可控。

4.3 防火

4.3.1 机房无防火措施

对应要求：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。

判例内容：机房内无防火措施（既无自动灭火，也无手持灭火器/或手持灭火器药剂已过期），一旦发生火情，无任何消防处置措施，可判高风险；若机房未达到消防验收的，可判高风险。

适用范围：所有系统。

满足条件（任意条件）：

a) 机房内无任何防火措施（既无自动灭火，也无手持灭火器/或手持灭火器药剂已过期）。

b) 机房未达到消防验收要求。

补偿措施：无。

整改建议：建议机房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，相关消防设备如灭火器等应定期检查，确保防火措施有效，并通过机房消防验收。

4.4 温湿度控制

4.4.1 机房无温湿度控制措施

对应要求：应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

判例内容：机房无有效的温湿度控制措施，或温湿度长期高于或低于设备允许的温湿度范围，可能加速设备损害，提高设备的故障率，对设备的正常运行带来安全隐患，或可能引起火灾等安全隐患的，可判高风险。

适用范围：所有系统。

满足条件（同时）：

a) 机房无温湿度调节措施；

b) 机房温湿度长期处于设备运行的范围之外。

补偿措施：对于一些特殊自然条件或特殊用途的系统，可酌情降低风险等级。

整改建议：建议机房设置温、湿度自动调节设备，确保机房温、湿度的变化在设备运行所允许的范围之内。

4.5 电力供应

4.5.1 机房无短期备用电力供应措施

对应要求：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。

判例内容：对于可用性要求较高的系统，如银行、证券等交易类系统，提供公共服务的民生类系统、工控类系统等，机房未配备短期备用电力供应设备（如UPS）或配备的设备无法在短时间内满足断电情况下的正常运行要求的，可判高风险。

适用范围：对可用性要求较高的3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 系统可用性要求较高；

c) 无法提供短期备用电力供应或备用电力供应无法满足系统短期正常运行。

补偿措施：如机房配备多路供电，且供电方同时断电概率较低的情况下，可酌情降低风险等级。

整改建议：建议配备容量合理的后备电源，并定期对UPS进行巡检，确保在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。

4.5.2 机房无电力线路冗余措施

对应要求：应设置冗余或并行的电力电缆线路为计算机系统供电。

判例内容：机房未配备冗余或并行电力线路供电来自于同一变电站，可判高风险。

适用范围：对可用性要求较高的3级及以上系统。

满足条件（同时）：

a) 3级及以上系统；

b) 系统可用性要求较高；

c) 机房未配备冗余或并行电力线路供电来自于同一变电站。

补偿措施：如机房配备大容量UPS，且足够保障断电情况下，一定时间内系统可正常运行或保障数据存储完整的，可酌情降低风险等级。

整改建议：建议配备冗余或并行的电力线路，电力线路应来自于不同的变电站；对于可用性要求较高的系统（4级系统），建议变电站来自于不同的市电。

4.5.3 机房无应急供电措施

对应要求：应提供应急供电设施。

判例内容：系统所在的机房必须配备应急供电措施，如未配备，或应急供电措施无法使用，可判高风险。

适用范围：4级系统。

满足条件（同时）：

a) 4级系统；

b) 机房未配备应急供电措施，或应急供电措施不可用/无法满足系统正常允许需求。

补偿措施：如果系统采用多数据中心方式部署，且通过技术手段能够实现应用级灾备，一定程度上可降低单一机房发生故障所带来的可用性方面影响，可酌情降低风险等级。

整改建议：建议配备应急供电设施，如备用发电设备。

4.6 电磁防护

4.6.1 机房无电磁防护措施

对应要求：应对关键设备或关键区域实施电磁屏蔽。

判例内容：对于涉及大量核心数据的系统，如机房或关键设备所在的机柜未采取电磁屏蔽措施，可判高风险。

适用范围：对于数据防泄漏要求较高的4级系统。

满足条件（同时）：

a) 4级系统；

b) 系统存储数据敏感性较高，有较高的保密性需求；

c) 机房环境复杂，有电磁泄露的风险。

补偿措施：如该4级系统涉及的信息对保密性要求不高，或者机房环境相对可控，可酌情降低风险等级。

整改建议：建议机房或重要设备所在的机柜采用电磁屏蔽技术，且相关产品或技术获得相关检测认证资质的证明。

5 安全通信网络

5.1 网络架构

5.1.1 网络设备业务处理能力不足

对应要求：应保证网络设备的业务处理能力满足业务高峰期需要。

判例内容：对可用性要求较高的系统，网络设备的业务处理能力不足，高峰时可能导致设备宕机或服务中断，影响金融秩序或引发群体事件，若无任何技术应对措施，可判定为高风险。

适用范围：对可用性要求较高的3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 系统可用性要求较高；

c) 核心网络设备性能无法满足高峰期需求，存在业务中断隐患，如业务高峰期，核心设备性能指标平均达到 80%以上。

补偿措施：针对设备宕机或服务中断制定了应急预案并落实执行，可酌情降低风险等级。

整改建议：建议更换性能满足业务高峰期需要的设备，并合理预计业务增长，制定合适的扩容计划。

5.1.2 网络区域划分不当

对应要求：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。

判例内容：应按照不同网络的功能、重要程度进行网络区域划分，如存在重要区域与非重要区域在同一子网或网段的，可判定为高风险。

适用范围：所有系统。

满足条件（任意条件）：

a) 承载业务系统的生产网络与办公网络在同一子网或网段。

b) 面向互联网提供服务的服务器区与内部网络区域在同一子网或网段。

c) 重要核心网络区域与非重要网络在同一子网或网段。

补偿措施：无。

整改建议：建议根据各工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网络区域，并做好各区域之间的访问控制措施。

5.1.3 互联网边界访问控制设备不可控

对应要求：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。

判例内容：互联网边界访问控制设备无管理权限，且无其他边界防护措施的，难以保证边界防护的有效性，也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，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 互联网边界访问控制设备无管理权限；

b) 无其他任何有效访问控制措施；

c) 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。

补偿措施：若互联网访问控制措施由云服务商提供或由集团公司统一管理等情况，可以根据“策略更改响应时间”、“策略有效性”等情况进行综合分析，酌情判断风险等级。

整改建议：建议部署自有的边界访问控制设备或租用有管理权限的边界访问控制设备，且对相关设备进行合理配置，确保互联网边界访问控制措施有效、可控。

5.1.4 互联网边界访问控制不当

对应要求：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。

判例内容：互联网出口无任何访问控制措施，或访问控制措施配置失效，存在较大安全隐患，可判定为高风险。

适用范围：所有系统。

满足条件（任意条件）：

a) 互联网出口无任何访问控制措施。

b) 互联网出口访问控制措施配置不当，存在较大安全隐患。

c) 互联网出口访问控制措施配置失效，无法起到相关控制功能。

补偿措施：边界访问控制设备不一定要是防火墙，只要是能实现相关的访问控制功能，形态为专用设备，且有相关功能能够提供相应的检测报告，可视为等效措施，判符合。如通过路由器、交换机或者带ACL功能的负载均衡器等设备实现，可根据系统重要程度，设备性能压力等因素，酌情判定风险等级。

整改建议：建议在互联网出口部署专用的访问控制设备，并合理配置相关控制策略，确保控制措施有效。

5.1.5 内部网络区域边界访问控制不当

对应要求：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。

判例内容：办公网与生产网之间无访问控制措施，办公环境任意网络接入均可对核心生产服务器和网络设备进行管理，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 办公网与生产网之间无访问控制措施；

b) 办公环境任意网络接入均可对核心生产服务器和网络设备进行管理。

补偿措施：边界访问控制设备不一定要是防火墙，只要是能实现相关的访问控制功能，形态为专用设备，且有相关功能能够提供相应的检测报告，可视为等效措施，判符合。如通过路由器、交换机或者带ACL功能的负载均衡器等设备实现，可根据系统重要程度，设备性能压力等因素，酌情判定风险等级。

整改建议：建议不同网络区域间应部署访问控制设备，并合理配置访问控制策略，确保控制措施有效。

5.1.6 关键线路和设备无冗余措施

对应要求：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。

判例内容：对可用性要求较高的系统，若网络链路为单链路，核心网络节点、核心网络设备或关键计算设备无冗余设计，一旦出现故障，可能导致业务中断，可判定为高风险。

适用范围：对可用性要求较高的3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 系统可用性要求较高；

c) 关键链路、核心网络设备或关键计算设备无任何无冗余措施，存在单点故障。

补偿措施：

a) 如系统采取多数据中心部署，或有应用级灾备环境，能在生产环境出现故障情况下提供服务的，可酌情降低风险等级。

b) 对于系统可用性要求不高的其他 3 级系统，如无冗余措施，可酌情降低风险等级。

c) 如核心安全设备采用并联方式部署，对安全防护能力有影响，但不会形成单点故障，也不会造成重大安全隐患的，可酌情降低风险等级。

整改建议：建议关键网络链路、核心网络设备、关键计算设备采用冗余设计和部署（如采用热备、负载均衡等部署方式），保证系统的高可用性。

5.1.7 云计算平台等级低于承载业务系统等级

对应要求：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。

判例内容：云计算平台承载高于其安全保护等级的业务应用系统，业务应用系统部署在低于其安全保护等级的云计算平台上，均可判定为高风险。

适用范围：对可用性要求较高的3级及以上系统。

满足条件（任意条件）：

a) 云计算平台承载高于其安全保护等级的业务应用系统。

b) 业务应用系统部署在低于其安全保护等级的云计算平台上。

c) 业务应用系统部署在未通过等级保护测评的云计算平台上。

整改建议：建议云租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。

5.2 通信传输

5.2.1 数据传输无完整性保护措施

对应要求：应采用密码技术保证通信过程中数据的完整性。

判例内容：对数据传输完整性要求较高的系统，数据在网络层传输无完整性保护措施，一旦数据遭到篡改，可能造成财产损失的，可判定为高风险。

适用范围：对数据传输完整性要求较高的3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 系统数据传输完整性要求较高；

c) 数据在网络层传输无任何完整性保护措施。

补偿措施：如应用层提供完整性校验等措施，或采用可信网络传输，可酌情降低风险等级。

整改建议：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。

5.2.2 敏感信息明文传输

对应要求：应采用密码技术保证通信过程中数据的保密性。

判例内容：口令、密钥等重要敏感信息在网络中明文传输，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 设备、主机、数据库、应用等口令、密钥等重要敏感信息在网络中明文传输；

c) 该网络管控措施不到位，存在口令被窃取并远程登录的风险。

补偿措施：

a) 如网络接入管控较好且网络环境为内网封闭可控环境，确保密码被窃取难度较大，或使用多因素等措施确保即使密码被窃取也无法进行管理，可酌情降低风险等级。

b) 如业务形态上必须使用远程 Internet 访问的相关设备，设备采用多因素认证，且严格限制管理地址的，可酌情降低风险等级。

整改建议：建议相关设备开启SSH或HTTPS协议或创建加密通道，通过这些加密方式传输敏感信息。

6 安全区域边界

6.1 边界防护

6.1.1 互联网边界访问控制设备不可控

对应要求：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。

判例内容参见章节5.1.4。

6.1.2 无违规内联检查措施

对应要求：应能够对非授权设备私自联到内部网络的行为进行检查或限制。

判例内容：非授权设备能够直接接入重要网络区域，如服务器区、管理网段等，且无任何告警、限制、阻断等措施的，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 物理、网络等环境不可控，存在非授权接入可能；

c) 可非授权接入网络重要区域，如服务器区、管理网段等；

d) 无任何控制措施，控制措施包括限制、检查、阻断等。

补偿措施：如接入的区域有严格的物理访问控制，采用静态IP地址分配，关闭不必要的接入端口，IP-MAC地址绑定等措施的，可酌情降低风险等级。

整改建议：建议部署能够对违规内联行为进行检查、定位和阻断的安全准入产品。

6.1.3 无违规外联检查措施

对应要求：应能够对内部用户非授权联到外部网络的行为进行检查或限制。

判例内容：重要核心管理终端、重要业务终端等关键设备，如无法对非授权联到外部网络的行为进行检查或限制，或内部人员可旁路、绕过边界访问控制设备私自外联互联网，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 物理、网络等环境不可控，存在非授权外联可能；

c) 重要核心管理终端、重要业务终端等关键设备存在私自外联互联网可能；

d) 无任何控制措施，控制措施包括限制、检查、阻断等。

补偿措施：如物理、网络等环境可控，非授权外联可能较小，相关设备上的USB接口、无线网卡等有管控措施，对网络异常进行监控及日志审查，可酌情降低风险等级。

整改建议：建议部署能够对违规外联行为进行检查、定位和阻断的安全管理产品。

6.1.4 无线网络无管控措施

对应要求：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。

判例内容：内部核心网络与无线网络互联，且之间无任何管控措施，一旦非授权接入无线网络即可访问内部核心网络区域，存在较大安全隐患，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 内部核心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；

c) 非授权接入无线网络将对内部核心网络带来较大安全隐患。

补偿措施：

a) 在特殊应用场景下，无线覆盖区域较小，且严格受控，仅有授权人员方可进入覆盖区域的，可酌情降低风险等级；

b) 对无线接入有严格的管控及身份认证措施，非授权接入可能较小，可根据管控措施的情况酌情降低风险等级。

整改建议：如无特殊需要，内部核心网络不应与无线网络互联；如因业务需要，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核心网络的访问进行限制，降低攻击者利用无线网络入侵内部核心网络。

6.2 访问控制

6.2.1 互联网边界访问控制配置不当

对应要求：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。

判例内容：与互联网互连的系统，边界处如无专用的访问控制设备或配置了全通策略，可判定为高风险。

适用范围：所有系统。

满足条件（任意条件）：

a) 互联网出口无任何访问控制措施。

b) 互联网出口访问控制措施配置不当，存在较大安全隐患。

c) 互联网出口访问控制措施配置失效，启用透明模式，无法起到相关控制功能。

补偿措施：边界访问控制设备不一定要是防火墙，只要是能实现相关的访问控制功能，形态为专用设备，且有相关功能能够提供相应的检测报告，可视为等效措施，判符合。如通过路由器、交换机或者带ACL功能的负载均衡器等设备实现，可根据系统重要程度，设备性能压力等因素，酌情判定风险等级。

整改建议：建议在互联网出口部署专用的访问控制设备，并合理配置相关控制策略，确保控制措施有效。

6.2.2 通信协议无转换或隔离措施

对应要求：应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。

判例内容：可控网络环境与不可控网络环境之间数据传输未采用通信协议转换或通信协议隔离等方式进行数据转换，可判定为高风险。

适用范围：4级系统。

满足条件（同时）：

a) 4 级系统；

b) 可控网络环境与不可控网络环境之间数据传输未进行数据格式或协议转化，也未采用通讯协议隔离措施。

补偿措施：如通过相关技术/安全专家论证，系统由于业务场景需要，无法通过通信协议转换或通信协议隔离等方式进行数据转换的，但有其他安全保障措施的，可酌情降低风险等级。

整改建议：建议数据在不同等级网络边界之间传输时，通过通信协议转换或通信协议隔离等方式进行数据交换。

6.3 入侵防范

6.3.1 无外部网络攻击防御措施

对应要求：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。

判例内容：关键网络节点（如互联网边界处）未采取任何防护措施，无法检测、阻止或限制互联网发起的攻击行为，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 关键网络节点（如互联网边界处）无任何入侵防护手段（如入侵防御设备、云防、WAF 等对外部网络发起的攻击行为进行检测、阻断或限制）。

补偿措施：无。

整改建议：建议在关键网络节点（如互联网边界处）合理部署可对攻击行为进行检测、阻断或限制的防护设备（如抗APT攻击系统、网络回溯系统、威胁情报检测系统、入侵防护系统等），或购买云防等外部抗攻击服务。

6.3.2 无内部网络攻击防御措施

对应要求：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。

判例内容：关键网络节点（如核心服务器区与其他内部网络区域边界处）未采取任何防护措施，无法检测、阻止或限制从内部发起的网络攻击行为，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 关键网络节点（如核心服务器区与其他内部网络区域边界处）无任何入侵防护手段（如入侵防御、防火墙等对内部网络发起的攻击行为进行检测、阻断或限制）。

补偿措施：如核心服务器区与其他内部网络之间部署了防火墙等访问控制设备，且访问控制措施较为严格，发生内部网络攻击可能性较小或有一定的检测、防止或限制能力，可酌情降低风险等级。

整改建议：建议在关键网络节点处（如核心服务器区与其他内部网络区域边界处）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。

6.4 恶意代码和垃圾邮件防范

6.4.1 无恶意代码防范措施

对应要求：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升级和更新。

判例内容：主机和网络层均无任何恶意代码检测和清除措施的，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 主机层无恶意代码检测和清除措施；

b) 网络层无恶意代码检测和清除措施。

补偿措施：

a) 如主机层部署恶意代码检测和清除产品，且恶意代码库保持更新，可酌情降低风险等级。

b) 如 2 级及以下系统，使用 Linux、Unix 系统，主机和网络层均未部署恶意代码检测和清除产品，可视总体防御措施酌情降低风险等级。

c) 对与外网完全物理隔离的系统，其网络环境、USB 介质等管控措施较好，可酌情降低风险等级。

整改建议：建议在关键网络节点处部署恶意代码检测和清除产品，且与主机层恶意代码防范产品形成异构模式，有效检测及清除可能出现的恶意代码攻击。

6.5 安全审计

6.5.1 无网络安全审计措施

对应要求：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。

判例内容：在网络边界、重要网络节点无任何安全审计措施，无法对重要的用户行为和重要安全事件进行日志审计，可判定为高风险。

适用范围：所有系统。

满足条件：

在网络边界、重要网络节点无法对重要的用户行为和重要安全事件进行日志审计。

补偿措施：无。

整改建议：建议在网络边界、重要网络节点，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。

7 安全计算环境

7.1 网络设备、安全设备、主机设备等

7.1.1 身份鉴别

7.1.1.1 设备存在弱口令

对应要求：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。

判例内容：网络设备、安全设备、操作系统、数据库等存在空口令或弱口令帐户，并可通过该弱口令帐户登录，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 存在空口令或弱口令帐户；

b) 可使用该弱口令帐户登录。

补偿措施：

a) 如采用双因素认证等管控手段，恶意用户使用该空/弱口令帐号无法直接登录相关设备，可酌情降低风险等级。

b) 如测评对象重要性较低，不会对整个信息系统安全性产生任何影响，可酌情降低风险等级。

整改建议：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，合理配置账户口令策略，提高口令质量。

7.1.1.2 设备鉴别信息无防窃取措施

对应要求：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。

判例内容：通过不可控网络环境远程管理的网络设备、安全设备、操作系统、数据库等，鉴别信息明文传输，容易被监听，造成数据泄漏，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 通过不可控网络环境远程进行管理；
b) 管理帐户口令以明文方式传输；
c) 使用截获的帐号可远程登录。

补偿措施：

a) 如整个远程管理过程中，只能使用加密传输通道进行鉴别信息传输的，可视为等效措施，判符合。
b) 如采用多因素身份认证、访问地址限定、仅允许内部可控网络进行访问的措施时，窃听到口令而无法直接进行远程登录的，可酌情降低风险等级。
c) 如通过其他技术管控手段（如准入控制、桌面管理、行为管理等），降低数据窃听隐患的，可酌情降低风险等级。
d) 在有管控措施的情况下，如果默认采用加密进行管理，但同时也开启非加密管理方式，可根据实际管理情况，酌情判断风险等级。
e) 可根据被测对象的作用以及重要程度，可根据实际情况，酌情判断风险等级。

整改建议：建议尽可能避免通过不可控网络对网络设备、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。

7.1.1.3 设备未实现双因素认证

对应要求：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。

判例内容：重要核心设备、操作系统等未采用两种或两种以上鉴别技术对用户身份进行鉴别。例如仅使用用户名/口令方式进行身份验证，削弱了管理员账户的安全性，无法避免账号的未授权窃取或违规使用，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；
b) 重要核心设备、操作系统等通过不可控网络环境远程进行管理；
c) 设备未启用两种或两种以上鉴别技术对用户身份进行鉴别；4 级系统多种鉴别技术中未用到密码技术或生物技术。

补偿措施：

a) 如设备通过本地登录方式（非网络方式）维护，本地物理环境可控，可酌情降低风险等级。
b) 采用两重用户名/口令认证措施（两重口令不同），例如身份认证服务器、堡垒机等手段，可酌情降低风险等级。
c) 如设备所在物理环境、网络环境安全可控，网络窃听、违规接入等隐患较小，口令策略和复杂度、长度符合要求的情况下，可酌情降低风险等级。
d) 可根据被测对象的作用以及重要程度，根据实际情况，酌情判断风险等级。

整改建议：建议重要核心设备、操作系统等增加除用户名/口令以外的身份鉴别技术，如密码/令牌、生物鉴别方式等，实现双因子身份鉴别，增强身份鉴别的安全力度。

7.1.2 访问控制

7.1.2.1 设备默认口令处理不当

对应要求：应重命名或删除默认账户，修改默认账户的默认口令。

判例内容：网络设备、安全设备、操作系统、数据库等默认账号的默认口令未修改，使用默认口令进行登录设备，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 未修改默认帐户的默认口令；

b) 可使用该默认口令账号登录。

补偿措施：无。

整改建议：建议网络设备、安全设备、操作系统、数据库等重命名或删除默认管理员账户，修改默认密码，使其具备一定的强度，增强账户安全性。

7.1.3 安全审计

7.1.3.1 设备未开启安全审计措施

对应要求：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。

判例内容：重要核心网络设备、安全设备、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，也无法对事件进行溯源，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统

b) 重要核心网络设备、安全设备、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；

c) 无其他技术手段对重要的用户行为和重要安全事件进行溯源。

补偿措施：

a) 如使用堡垒机或其他第三方审计工具进行日志审计，能有效记录用户行为和重要安全事件，可视为等效措施，判符合。

b) 如通过其他技术或管理手段能对事件进行溯源的，可酌情降低风险等级。

c) 如核查对象非重要核心设备，对整个信息系统影响有限的情况下，可酌情降低风险等级。

整改建议：建议在重要核心设备、安全设备、操作系统、数据库性能允许的前提下，开启用户操作类和安全事件类审计策略或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。

7.1.4 入侵防范

7.1.4.1 设备开启高危服务端口

对应要求：应关闭不需要的系统服务、默认共享和高危端口。

判例内容：网络设备、安全设备、操作系统等存在多余系统服务/默认共享/高危端口，且存在可被利用的高危漏洞或重大安全隐患，可判定为高风险。

适用范围：所有系统。

满足条件：

操作系统上的多余系统服务/默认共享/高危端口存在可被利用的高风险漏洞或重大安全隐患。

补偿措施：如通过其他技术手段能降低漏洞影响，可酌情降低风险等级。

整改建议：建议网络设备、安全设备、操作系统等关闭不必要的服务和端口，减少后门等安全漏洞；根据自身应用需求，需要开启共享服务的，应合理设置相关配置，如设置账户权限等。

7.1.4.2 管理终端无管控措施

对应要求：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。

判例内容：通过不可控网络环境远程管理的网络设备、安全设备、操作系统、数据库等，未采取技术手段对管理终端进行限制，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；
b) 可通过不可控网络环境远程进行管理；
c) 未采取技术手段对管理终端进行管控（管控措施包括但不限于终端接入管控、网络地址范围限制、堡垒机等）。

补偿措施：如管理终端部署在运维区、可控网络或采用多种身份鉴别方式等技术措施，可降低终端管控不善所带来的安全风险的，可酌情降低风险等级。

整改建议：建议通过技术手段，对管理终端进行限制。

7.1.4.3 互联网设备未修补已知重大漏洞

对应要求：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。

判例内容：对于一些互联网直接能够访问到的网络设备、安全设备、操作系统、数据库等，如存在外界披露的重大漏洞，未及时修补更新，无需考虑是否有POC攻击代码，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 该设备可通过互联网访问；
b) 该设备型号、版本存在外界披露的重大安全漏洞；
c) 未及时采取修补或其他有效防范措施。

补偿措施：

a) 如相关漏洞暴露在可控的网络环境，可酌情降低风险等级。
b) 如某网络设备的 WEB 管理界面存在高风险漏洞，而该 WEB 管理界面只能通过特定 IP 或特定可控环境下才可访问，可酌情降低风险等级。

整改建议：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，弥补严重安全漏洞。

7.1.4.4 内部设备存在可被利用高风险漏洞

对应要求：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。

判例内容：通过验证测试或渗透测试能够确认并利用的，可对网络设备、安全设备、操作系统、数据库等造成重大安全隐患的漏洞（包括但不限于缓冲区溢出、提权漏洞、远程代码执行、严重逻辑缺陷、敏感数据泄露等），可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 存在可被利用的高风险漏洞；

b) 通过验证测试或渗透测试确认该高风险漏洞可能对该设备造成重大安全隐患。

补偿措施：只有在相关设备所在的物理、网络、管理环境严格受控，发生攻击行为可能性较小的情况下，方可酌情降低风险等级；对于互联网可访问到的设备，原则上不宜降低其风险等级。

整改建议：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扫，及时处理发现的风险漏洞，提高设备稳定性与安全性。

7.1.5 恶意代码防范

7.1.5.1 Windows 操作系统无恶意代码防范措施

对应要求：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。

判例内容：Windows操作系统未安装防恶意代码软件，并进行统一管理，无法防止来自外部的恶意攻击或系统漏洞带来的危害，可判定为高风险。

适用范围：所有系统。

满足条件（任意条件）：

a) Windows 操作系统未安装杀毒软件。

b) Windows 操作系统安装的杀毒软件病毒库一月以上未更新。（可根据服务器部署环境、行业或系统特性缩短或延长病毒库更新周期）

补偿措施：

a) 如一个月以上未更新，但有完备的补丁更新/测试计划，且有历史计划执行记录的，可根据服务器部署环境、行业或系统特性酌情降低风险等级。

b) 可与网络安全部分中的入侵防范和访问控制措施相结合来综合评定风险，如网络层部署了恶意代码防范设备，可酌情降低风险等级。

c) 对与外网完全物理隔离的系统，其网络环境、USB 介质等管控措施较好，可酌情降低风险等级。

整改建议：建议操作系统统一部署防病毒软件，或采用集成性质防病毒服务器或虚拟化底层防病毒措施，并及时更新病毒库，抵挡外部恶意代码攻击。

7.2 应用系统及数据

7.2.1 身份鉴别

7.2.1.1 应用系统口令策略缺失

对应要求：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。

判例内容：应用系统无任何用户口令复杂度校验机制，校验机制包括口令的长度、复杂度等，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 应用系统无口令长度、复杂度校验机制；

b) 可设置 6 位以下，单个数字或连续数字或相同数字等易猜测的口令。

补偿措施：

a) 如应用系统采用多种身份鉴别认证技术的，即使有口令也无法直接登录应用系统的，可酌情降低风险等级。

b) 如应用系统仅为内部管理系统，只能内网访问，且访问人员相对可控，可酌情降低风险等级。

c) 如应用系统口令校验机制不完善，如只有部分校验机制，可根据实际情况，酌情降低风险等级。

d) 特定应用场景中的口令（如 PIN 码）可根据相关要求，酌情判断风险等级。

整改建议：建议应用系统对用户的账户口令长度、复杂度进行校验，如要求系统账户口令至少8位，由数字、字母或特殊字符中2种方式组成；对于如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。

7.2.1.2 应用系统存在弱口令

对应要求：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。

判例内容：应用系统存在易被猜测的常用/弱口令帐户，可判定为高风险。

适用范围：所有系统。

满足条件：

通过渗透测试或常用/弱口令尝试，发现应用系统中存在可被登录弱口令帐户。

补偿措施：如该弱口令帐号为前台自行注册，自行修改的普通用户帐户，被猜测登录后只会影响单个用户，而不会对整个应用系统造成安全影响的，可酌情降低风险等级。

整改建议：建议应用系统通过口令长度、复杂度校验、常用/弱口令库比对等方式，提高应用系统口令质量。

7.2.1.3 应用系统无登录失败处理机制

对应要求：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。

判例内容：可通过互联网登录的应用系统未提供任何登录失败处理措施，攻击者可进行口令猜测，可判定为高风险。

适用范围：3级及以上系统。

满足条件：

a) 3 级及以上系统；

b) 可通过互联网登录，且对帐号安全性要求较高，如帐户涉及金融、个人隐私信息、后台管理等；

c) 对连续登录失败无任何处理措施；

d) 攻击者可利用登录界面进行口令猜测。

补偿措施：

a) 如应用系统采用多种身份鉴别认证技术的，可酌情降低风险等级。

b) 仅通过内部网络访问的内部/后台管理系统，如访问人员相对可控，可酌情降低风险等级。

c) 如登录页面采用图像验证码等技术可在一定程度上提高自动化手段进行口令暴力破解难度的，可酌情降低风险等级。

d) 可根据登录帐户的重要程度、影响程度，可酌情判断风险等级。但如果登录帐户涉及到金融行业、个人隐私信息、信息发布、后台管理等，不宜降低风险等级。

整改建议：建议应用系统提供登录失败处理功能（如帐户锁定、多重认证等），防止攻击者进行口令暴力破解。

7.2.1.4 互联网可访问系统未实现双因素认证

对应要求：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。

判例内容：通过互联网方式访问，且涉及大额资金交易、核心业务等操作的系统，在进行重要操作前应采用两种或两种以上方式进行身份鉴别，如只采用一种验证方式进行鉴别，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 通过互联网方式访问的系统，在进行涉及大额资金交易、核心业务等重要操作前未启用两种或两种以上鉴别技术对用户身份进行鉴别；4 级系统多种鉴别技术中未用到密码技术或生物技术。

补偿措施：

a) 采用两重用户名/口令认证措施，且两重口令不可相同等情况，可酌情降低风险等级。

b) 如应用服务访问的网络环境安全可控，网络窃听、违规接入等隐患较小，口令策略和复杂度、长度符合要求的情况下，可酌情降低风险等级。

c) 在完成重要操作前的不同阶段两次或两次以上使用不同的方式进行身份鉴别，可根据实际情况，酌情降低风险等级。

d) 涉及到主管部门认可的业务形态，例如快捷支付、小额免密支付等，可酌情降低风险等级。

e) 可根据被测对象中用户的作用以及重要程度，在口令策略和复杂度、长度符合要求的情况下，可根据实际情况，酌情判断风险等级。

f) 系统用户群体为互联网用户，且冒名登录、操作不会对系统或个人造成重大恶劣影响或经济损失的，可酌情判断风险等级。

整改建议：建议应用系统增加除用户名/口令以外的身份鉴别技术，如密码/令牌、生物鉴别方式等，实现双因子身份鉴别，增强身份鉴别的安全力度。

7.2.2 访问控制

7.2.2.1 应用系统登录模块权限控制不当

对应要求：应对登录的用户分配账户和权限。

判例内容：应用系统访问控制功能存在缺失，无法按照设计策略控制用户对系统功能、数据的访问；可通过直接访问URL等方式，在不登录系统的情况下，非授权访问系统功能模块，可判定为高风险。

适用范围：所有系统。

满足条件：

可通过直接访问URL等方式，在不登录系统的情况下，非授权访问系统重要功能模块。

补偿措施：

a) 如应用系统部署在可控网络，有其他防护措施能限制、监控用户行为的，可酌情降低风险等级。

b) 可根据非授权访问模块的重要程度、越权访问的难度，酌情判断风险等级。

整改建议：建议完善访问控制措施，对系统重要页面、功能模块进行访问控制，确保应用系统不存在访问控制失效情况。

7.2.2.2 应用系统默认口令处理不当

对应要求：应重命名或删除默认账户，修改默认账户的默认口令。

判例内容：应用系统默认账号的默认口令未修改，可利用该默认口令登录系统，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 未修改默认帐户的默认口令；

b) 可使用该默认口令账号登录。

补偿措施：无。

整改建议：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。

7.2.2.3 应用系统访问控制存在缺陷

对应要求：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。

判例内容：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。如存在平行权限漏洞，低权限用户越权访问高权限功能模块等，可判定为高风险。

适用范围：所有系统。

满足条件：

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。如存在平行权限漏洞，低权限用户越权访问高权限功能模块等。

补偿措施：

a) 如应用系统部署在可控网络，有其他防护措施能限制、监控用户行为的，可酌情

降低风险等级。

b) 可根据非授权访问模块的重要程度、越权访问的难度，酌情判断风险等级。

整改建议：建议完善访问控制措施，对系统重要页面、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。

7.2.3 安全审计

7.2.3.1 应用系统无安全审计措施

对应要求：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。

判例内容：应用系统（包括前端系统和后台管理系统）无任何日志审计功能，无法对用户的重要行为进行审计，也无法对事件进行溯源，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统

b) 应用系统无任何日志审计功能，无法对用户的重要行为进行审计；

c) 无其他技术手段对重要的用户行为和重要安全事件进行溯源。

补偿措施：

a) 如有其他技术手段对重要的用户行为进行审计、溯源，可酌情降低风险等级。

b) 如审计记录不全或审计记录有记录，但无直观展示，可根据实际情况，酌情降低风险等级。

整改建议：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。

7.2.4 入侵防范

7.2.4.1 数据有效性检验功能存在缺陷

对应要求：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。

判例内容：由于校验机制缺失导致的应用系统存在如SQL注入、跨站脚本、上传漏洞等高风险漏洞，可判定为高风险。

适用范围：所有系统。

满足条件：

a) 应用系统存在如 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，造成严重后果的高风险漏洞；

b) 无其他技术手段对该漏洞进行防范。

补偿措施：

c) 如应用系统存在 SQL 注入、跨站脚本等高风险漏洞，但是系统部署了 WAF、云盾等应用防护产品，在防护体系下无法成功利用，可酌情降低风险等级。

d) 不与互联网交互的内网系统，可根据系统重要程度、漏洞危害情况等，酌情判断风险等级。

整改建议：建议通过修改代码的方式，对数据有效性进行校验，提交应用系统的安全性，防止相关漏洞的出现。

7.2.4.2 应用系统存在可被利用的高风险漏洞

对应要求：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。

判例内容：应用系统所使用的环境、框架、组件等存在可被利用的高风险漏洞，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，可能造成严重后果的，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 应用系统所使用的环境、框架、组件等存在可被利用的，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，造成严重后果的高风险漏洞；

b) 无其他有效技术手段对该漏洞进行防范。

补偿措施：

a) 如应用系统使用的环境、框架、组件等存在高风险漏洞，但是系统部署了 WAF、云盾等应用防护产品，在防护体系下无法成功利用，可酌情降低风险等级。

b) 不与互联网交互的内网系统，可通过分析内网环境对相关漏洞的影响、危害以及利用难度，酌情提高/降低风险等级。

整改建议：建议定期对应用系统进行漏洞扫描，对可能存在的已知漏洞，在重复测试评估后及时进行修补，降低安全隐患。

7.2.4.3 应用系统存在严重逻辑缺陷类漏洞

对应要求：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。

判例内容：如应用系统的业务功能（如密码找回功能等）存在高风险安全漏洞或严重逻辑缺陷，可能导致修改任意用户密码、绕过安全验证机制非授权访问等情况，可判定为高风险。

适用范围：所有系统。

满足条件：

通过测试，发现应用系统的业务功能（如密码找回功能等）存在高风险安全漏洞或严重逻辑缺陷，可能导致修改任意用户密码、绕过安全验证机制非授权访问等情况。

补偿措施：无。

整改建议：建议通过修改应用程序的方式对发现的高风险/严重逻辑缺陷进行修补，避免出现安全隐患。

7.2.5 数据完整性

7.2.5.1 数据传输无完整性保护措施

对应要求：应采用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。

判例内容参见章节“5.2.1”。

7.2.6 数据保密性

7.2.6.1 敏感信息明文传输

对应要求：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。

判例内容：用户鉴别信息、公民敏感信息数据或重要业务数据等以明文方式在不可控网络中传输，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 用户身份认证信息、个人敏感信息数据或重要业务数据等以明文方式在不可控网络中传输。

补偿措施：

a) 如使用网络加密的技术确保数据在加密通道中传输，可根据实际情况，视为等效措施，判为符合。

b) 如敏感信息在可控网络中传输，网络窃听等风险较低，可酌情降低风险等级。

整改建议：建议采用密码技术确保重要数据在传输过程中的保密性。

7.2.6.2 敏感信息无存储保密性保护

对应要求：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。

判例内容：用户身份认证信息、个人敏感信息数据、重要业务数据、行业主管部门定义的非明文存储类数据等以明文方式存储，且无其他有效保护措施，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 用户身份认证信息、个人敏感信息数据、重要业务数据、行业主管部门定义的非明文存储类数据等以明文方式存储；

b) 无其他有效数据保护措施。

补偿措施：如采取区域隔离、部署数据库防火墙、数据防泄露产品等安全防护措施的，可通过分析造成信息泄露的难度和影响程度，酌情降低风险等级。

整改建议：采用密码技术保证重要数据在存储过程中的保密性。

7.2.7 数据备份恢复

7.2.7.1 数据备份措施缺失

对应要求：应提供重要数据的本地数据备份与恢复功能。

判例内容：应用系统未提供任何数据备份措施，一旦遭受数据破坏，无法进行数据恢复的，可判定为高风险。

适用范围：所有系统。

满足条件：

应用系统未提供任何数据备份措施，一旦遭受数据破坏，无法进行数据恢复。

补偿措施：无。

整改建议：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。

7.2.7.2 异地备份措施缺失

对应要求：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。

判例内容：对系统、数据容灾要求较高的系统，如金融、医疗卫生、社会保障等行业系统，如无异地数据灾备措施，或异地备份机制无法满足业务需要，可判定为高风险。

适用范围：对系统、数据容灾要求较高的3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 对容灾要求较高的系统；

c) 系统无异地数据备份措施，或异地备份机制无法满足业务需要。

补偿措施：

a) 一般来说同城异地机房直接距离不低于为 30 公里，跨省市异地机房直线距离不低于 100 公里，如距离上不达标，可酌情降低风险等级。

b) 系统数据备份机制存在一定时间差，若被测单位评估可接受时间差内数据丢失，可酌情降低风险等级。

c) 可根据系统容灾要求及行业主管部门相关要求，根据实际情况酌情判断风险等级。

整改建议：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。

7.2.7.3 数据处理系统无冗余措施

对应要求：应提供重要数据处理系统的热冗余，保证系统的高可用性。

判例内容：对数据处理可用性要求较高系统（如金融行业系统、竞拍系统、大数据平台等），应采用热冗余技术提高系统的可用性，若核心处理节点（如服务器、DB等）存在单点故障，可判定为高风险。

适用范围：对数据处理可用性要求较高的3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 对数据处理可用性要求较高系统；

c) 处理重要数据的设备（如服务器、DB 等）未采用热冗余技术，发生故障可能导致系统停止运行。

补偿措施：如当前采取的恢复手段，能够确保被测单位评估的RTO在可接受范围内，可根据实际情况酌情降低风险等级。

整改建议：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。

7.2.7.4 未建立异地灾难备份中心

对应要求：应建立异地灾难备份中心，提供业务应用的实时切换。

判例内容：对容灾、可用性要求较高的系统，如金融行业系统，如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，可判定为高风险。

适用范围：对容灾、可用性要求较高的4级系统。

满足条件（同时）：

a) 4 级系统；

b) 对容灾、可用性要求较高的系统；

c) 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。

补偿措施：如当前采取的恢复手段，能够确保被测单位评估的RTO在可接受范围内，可根据实际情况酌情降低风险等级。

整改建议：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。

7.2.8 剩余信息保护

7.2.8.1 鉴别信息释放措施失效

对应要求：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。

判例内容：身份鉴别信息释放或清除机制存在缺陷，如在正常进行释放或清除身份鉴别信息操作后，仍可非授权访问系统资源或进行操作，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 身份鉴别信息释放或清除机制存在缺陷；

b) 利用剩余鉴别信息，可非授权访问系统资源或进行操作。

补偿措施：无。

整改建议：建议完善鉴别信息释放/清除机制，确保在执行释放/清除相关操作后，鉴别信息得到完全释放/清除。

7.2.8.2 敏感数据释放措施失效

对应要求：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。

判例内容：身份鉴别信息释放或清除机制存在缺陷，如在正常进行释放或清除身份鉴别信息操作后，仍可非授权访问系统资源或进行操作，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 敏感数据释放或清除机制存在缺陷；

c) 利用剩余信息，可非授权获得相关敏感数据。

补偿措施：如因特殊业务需要，需要在存储空间保留敏感数据，相关敏感数据进行了有效加密/脱敏处理的，且有必要的提示信息，可根据实际情况，酌情降低风险等级。

整改建议：建议完善敏感数据释放/清除机制，确保在执行释放/清除相关操作后，敏感数据得到完全释放/清除。

7.2.9 个人信息保护

7.2.9.1 违规采集、存储个人信息

对应要求：应仅采集和保存业务必需的用户个人信息。

判例内容：在采集和保存用户个人信息时，应通过正式渠道获得用户同意、授权，如在未授权情况下，采取、存储用户个人隐私信息，可判定为高风险。

适用范围：所有系统。

满足条件（任意条件）：

a) 在未授权情况下，采取、存储用户个人隐私信息，无论该信息是否是业务需要。

b) 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。

补偿措施：如在用户同意、授权的情况下，采集和保存业务非必需的用户个人信息，可根据实际情况，酌情判断风险等级。

整改建议：建议通过官方正式渠道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。

7.2.9.2 非授权访问、使用个人信息

对应要求：应禁止未授权访问和非法使用用户个人信息。

判例内容：未授权访问和非法使用个人信息，如在未授权情况下将用户信息提交给第三方处理，未脱敏的情况下用于其他业务用途，未严格控制个人信息查询以及导出权限，非法买卖、泄露用户个人信息等，可判定为高风险。

适用范围：所有系统。

满足条件（任意条件）：

a) 在未授权情况下将用户个人信息共享给其他公司、机构、个人（国家、法律规定的公安、司法机构除外）。

b) 未脱敏的情况下用于其他非核心业务系统或测试环境等。

c) 未严格控制个人信息查询以及导出权限。

d) 非法买卖、泄露用户个人信息。

补偿措施：如互联网系统在收集用户的个人敏感信息前，数据收集方明确数据的用途，可能涉及使用数据的单位、机构，权责清晰，并根据各自职责与用户签订个人信息保密协议和个人信息收集声明许可协议的，可根据实际情况酌情降低风险等级。

整改建议：建议通过官方正式渠道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，通过技术和管理手段，防止未授权访问和非法使用。

7.2.10 数据完整性和保密性

7.2.10.1 云服务客户数据、用户个人信息违规出境

对应要求：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。

判例内容：云服务客户数据、用户个人信息等境外存储，且未遵循国家相关规定，可判定为高风险。

适用范围：云计算平台。

满足条件（同时）：

a) 云服务客户数据、用户个人信息等境外存储；

b) 数据出境未遵循国家相关规定。

整改建议：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。

8 安全管理中心

8.1 集中管控

8.1.1 运行监控措施缺失

对应要求：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。

判例内容：对可用性要求较高的系统，若没有任何监测措施，发生故障时难以及时对故障进行定位和处理，可判定为高风险。

适用范围：可用性要求较高的3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 对可用性要求较高的系统；

c) 无任何监控措施，发生故障也无法及时对故障进行定位和处理。

补偿措施：无。

整改建议：建议对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。

8.1.2 日志存储时间不满足要求

对应要求：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。

判例内容：《中华人民共和国网络安全法》要求“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”；因此，如相关设备日志留存不满足法律法规相关要求，可判定为高风险。

适用范围： 3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 对网络运行状态、网络安全事件等日志的留存不满足法律法规规定的相关要求（不少于六个月）。

补偿措施：对于一些特殊行业或日志时效性短于6个月的，可根据实际情况，可酌情降低风险等级。

整改建议：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。

8.1.3 安全事件发现处置措施缺失

对应要求：应能对网络中发生的各类安全事件进行识别、报警和分析。

判例内容：未部署相关安全设备，识别网络中发生的安全事件，并对重要安全事件进行报警的，可判定为高风险。

适用范围： 3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 无法对网络中发生的安全事件（包括但不限于网络攻击事件、恶意代码传播事件等）进行识别、告警和分析。

补偿措施：无。

整改建议：建议部署相关专业防护设备，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，及时处置。

9 安全管理制度

9.1 管理制度

9.1.1 管理制度缺失

对应要求：应对安全管理活动中的各类管理内容建立安全管理制度。

判例内容：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被测系统的，可判定为高风险。

适用范围：所有系统。

满足条件（任意条件）：

a) 未建立任何与安全管理活动相关的管理制度。

b) 相关管理制度无法适用于当前被测系统。

补偿措施：无。

整改建议：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。

10 安全管理机构

10.1 岗位设置

10.1.1 未建立网络安全领导小组

对应要求：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。

判例内容：未成立指导和管理信息安全工作的委员会或领导小组，或其最高领导不是由单位主管领导担任或授权，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 未成立指导和管理信息安全工作的委员会或领导小组，或领导小组最高领导不是由单位主管领导担任或授权。

补偿措施：无。

整改建议：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。

11 安全建设管理

11.1 产品采购和使用

11.1.1 违规采购和使用网络安全产品

对应要求：应确保网络安全产品采购和使用符合国家的有关规定。

判例内容：网络关键设备和网络安全专用产品的使用违反国家有关规定，可判定为高风险。

适用范围：所有系统。

满足条件：

网络关键设备和网络安全专用产品的使用违反国家有关规定。

补偿措施：无。

整改建议：建议依据国家有关规定，采购和使用网络关键设备和网络安全专用产品。（《中华人民共和国网络安全法》第二十三条规定网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销

售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。）

11.1.2 违规采购和使用密码产品与服务

对应要求：应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。

判例内容：密码产品与服务的使用违反国家密码管理主管部门的要求，可判定为高风险。

适用范围：所有系统。

满足条件：

密码产品与服务的使用违反国家密码管理主管部门的要求。

补偿措施：无。

整改建议：建议依据国家密码管理主管部门的要求，使用密码产品与服务。

11.2 外包软件开发

11.2.1 外包开发代码审计措施缺失

对应要求：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。

判例内容：对于涉及金融、民生、基础设施等重要行业的业务核心系统由外包公司开发，上线前未对外包公司开发的系统进行源代码审查，外包商也无法提供相关安全检测证明，可判定为高风险。

适用范围：涉及金融、民生、基础设施等重要核心领域的3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；
b) 涉及金融、民生、基础设施等重要行业的业务核心系统；
c) 被测单位为对外包公司开发的系统进行源代码安全审查；
d) 外包公司也无法提供第三方安全检测证明。

补偿措施：

a) 开发公司可提供国家认可的第三方机构出具的源代码安全审查报告/证明，可视为等效措施，判符合。
b) 可根据系统的用途以及外包开发公司的开发功能的重要性，根据实际情况，酌情判断风险等级。
c) 如第三方可提供软件安全性测试证明（非源码审核），可视实际情况，酌情降低风险等级。
d) 如被测方通过合同等方式与外包开发公司明确安全责任或采取相关技术手段进行防控的，可视实际情况，酌情降低风险等级。
e) 如被测系统建成时间较长，但定期对系统进行安全检测，当前管理制度中明确规定外包开发代码审计的，可根据实际情况，酌情降低风险等级。

整改建议：建议对外包公司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。

11.3 测试验收

11.3.1 上线前未开展安全测试

对应要求：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。

判例内容：系统上线前未通过安全性测试，或未对相关高风险问题进行安全评估仍旧“带病”上线的，可判定为高风险。安全检查内容可以包括但不限于扫描渗透测试、安全功能验证、源代码安全审核。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 系统上线前未进行任何安全性测试，或未对相关高风险问题进行安全评估仍旧“带病”上线。

补偿措施：

a) 如被测系统建成时间较长，定期对系统进行安全检测，管理制度中相关的上线前安全测试要求，可根据实际情况，酌情降低风险等级。

b) 如系统安全性方面是按照技术协议中的约定在开发过程中进行控制，并能提供相关控制的证明，可根据实际情况，酌情降低风险等级。

c) 可视系统的重要程度，被测单位的技术实力，根据自检和第三方检测的情况，酌情判断风险等级。

整改建议：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，确保系统不“带病”上线。

12 安全运维管理

12.1 漏洞和风险管理

12.1.1 未对安全漏洞和隐患进行识别与修补

对应要求：应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

判例内容：未对发现的安全漏洞和隐患及时修补，会导致系统存在较大的安全隐患，黑客有可能利用安全漏洞对系统实施恶意攻击，如果安全漏洞和隐患能够构成高危风险，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 通过漏洞扫描，发现存在可被利用的高风险漏洞；

c) 未对相关漏洞进行评估或修补，对系统安全构成重大隐患。

补偿措施：如果安全漏洞修补可能会对系统的正常运行造成冲突，应对发现的安全漏洞和隐患进行评估，分析被利用的可能性，判断安全风险的等级，在可接受的范围内进行残余风险评估，明确风险等级，若无高危风险，可酌情降低风险。

整改建议：建议对发现的安全漏洞和隐患进行及时修补评估，对必须修补的安全漏洞和隐患进行加固测试，测试无误后，备份系统数据，再从生产环境进行修补，对于剩余安全漏洞和隐患进行残余风险分析，明确安全风险整改原则。

12.2 网络和系统安全管理

12.2.1 未将重要运维操作纳入变更管理制度

对应要求：应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。

判例内容：未对运维过程中改变连接、安装系统组件或调整配置参数进行变更审批，且未进行变更性测试，一旦安装系统组件或调整配置参数对系统造成影响，有可能导致系统无法正常访问，出现异常，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 未建立变更管理制度，对于重大变更性运维过程无审批流程；

c) 变更过程未保留相关操作日志及备份措施，出现问题无法进行恢复还原。

补偿措施：无。

整改建议：建议对需要作出变更性运维的动作进行审批，并对变更内容进行测试，在测试无误后，备份系统数据和参数配置，再从生产环境进行变更，并明确变更流程以及回退方案，变更完成后进行配置信息库更新。

12.2.2 未对运维工具进行管控

对应要求：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。

判例内容：未对各类运维工具（特别是未商业化的运维工具）进行有效性检查，未对运维工具的接入进行严格的控制和审批，运维工具中可能存在漏洞或后门，一旦被黑客利用有可能造成数据泄露，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 未对各类运维工具（特别是未商业化的运维工具）进行有效性检查，如病毒、漏洞扫描等；对运维工具的接入也未进行严格的控制和审批；操作结束后也未要求删除可能临时存放的敏感数据。

补偿措施：

a) 如使用官方正版商用化工具，或自行开发的，安全可供的运维工具，可根据实际情况，酌情降低风险等级。

b) 如对于运维工具的接入有严格的控制措施，且有审计系统对相关运维操作进行审计，可根据实际情况，酌情降低风险等级。

整改建议：如果必须使用运维工具，建议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。

12.2.3 未对运维外联进行管控

对应要求：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。

判例内容：运维类制度中未明确服务器及终端与外部连接的授权和批准，也未定期对相关违反网络安全策略的行为进行检查，存在违规外联的安全隐患，一旦内网服务器或终端违规外联，可能造成涉密信息（商密信息）的泄露，同时增加了感染病毒的可能性，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 管理制度上无关于外部连接的授权和审批流程，也未定期进行相关的巡检；

c) 无技术手段检查违规上网及其他网络安全策略的行为。

补偿措施：在网络部署了相关的准入控制设备，可有效控制、检查、阻断违规无线上网及其他违反网络安全策略行为的情况下，如未建立相关制度，未定期进行巡检，可酌情降低风险等级。

整改建议：建议制度上明确所有与外部连接的授权和批准制度，并定期对相关违反行为进行检查，可采取终端管理系统实现违规外联和违规接入，设置合理的安全策略，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。

12.3 恶意代码防范管理

12.3.1 未对外来接入设备进行恶意代码检查

对应要求：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。

判例内容：外来计算机或存储设备本身可能已被感染病毒或木马，未对其接入系统前进行恶意代码检查，可能导致系统感染病毒或木马，对信息系统造成极大的危害，可判定为高风险。

适用范围：所有系统。

满足条件（同时）：

a) 未在管理制度或安全培训手册中明确外来计算机或存储设备接入安全操作流程；

b) 外来计算机或存储设备接入系统前未进行恶意代码检查。

补偿措施：无。

整改建议：建议制定外来接入设备检查制度，对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，再检查无误后，经过审批，设备方可接入系统。

12.4 变更管理

12.4.1 未建立变更管理制度

对应要求：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。

判例内容：未明确变更管理流程，未对需要变更的内容进行分析与论证，未制定详细的变更方案，无法明确变更的需求与必要性；变更的同时也伴随着可能导致系统无法正常访问的风险，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 无变更管理制度，或变更管理制度中无变更管理流程、变更内容分析与论证、变更方案审批流程等相关内容。

补偿措施：无。

整改建议：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，然后在实施变更。

12.5 备份与恢复管理

12.5.1 未建立数据备份策略

对应要求：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。

判例内容：未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，无法实现重要数据的定期备份与恢复性测试，一旦系统出现故障，需要恢复数据，存在无数据可恢复的情况，或者备份的数据未经过恢复性测试，无法确保备份的数据可用，可判定为高危风险。此外，如有相关制度，但未实施，视为制度内容未落实，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 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。

补偿措施：

a) 未建立相关数据备份制度，但若已实施数据备份措施，且备份机制符合业务需要，可酌情降低风险等级。

b) 如系统还未正式上线，则可检查是否制定了相关的管理制度，目前的技术措施（如环境、存储等）是否可以满足制度中规定的备份恢复策略要求，可根据实际情况判断风险等级。

整改建议：建议制定备份与恢复相关的制度，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性测试，保证备份数据的高可用性与可恢复性。

12.6 应急预案管理

12.6.1 未制定应急预案

对应要求：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。

判例内容：未制定重要事件的应急预案，未明确重要事件的应急处理流程、系统恢复流程等内容，一旦出现应急事件，无法合理有序的进行应急事件处置过程，造成应急响应时间增长，导致系统不能在最短的事件内进行恢复，可判定为高风险。

适用范围：所有系统。

满足条件：

未制定重要事件的应急预案。

补偿措施：如制定了应急预演，但内容不全，可根据实际情况，酌情降低风险等级。

整改建议：建议制定重要事件的应急预案，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。

12.6.2 未对应急预案进行培训演练

对应要求：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。

判例内容：未定期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应急演练，无法提供应急预案培训和演练记录，可判定为高风险。

适用范围：3级及以上系统。

满足条件（同时）：

a) 3 级及以上系统；

b) 未定期对系统相关的人员进行应急预案培训；

c) 未进行过应急预案的演练。

补偿措施：如系统还未正式上线，可根据培训演练制度及相关培训计划，根据实际情况判断风险等级。

整改建议：建议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。

12.7 云计算环境管理

12.7.1 云计算平台运维方式不当

对应要求：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。

判例内容：云计算平台的运维地点不在中国境内，且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，可判定为高风险。

适用范围：云计算平台。

满足条件（同时）：

a) 云计算平台的运维地点不在中国境内；

b) 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。

整改建议：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应遵循国家相关规定。

附录A

（资料性附录）

基本要求与判例对应表

序号	层面	控制点	控制项	对应编号	对应案例	适用范围
1	安全物理环境	物理访问控制	a）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；	4.1.1	机房出入口无控制措施	所有系统
2			应保证云计算基础设施位于中国境内。（云计算安全扩展要求）	4.1.2	云计算基础设施物理位置不当	云计算平台
3		防盗窃和防破坏	c）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。	4.2.1	机房无防盗措施	3 级及以上系统
4		防火	a）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；	4.3.1	机房无防火措施	所有系统
5		温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。	4.4.1	机房无温湿度控制措施	所有系统
6		电力供应	b）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；	4.5.1	机房无短期备用电力供应措施	对可用性要求较高的 3 级及以上系统
7			c）应设置冗余或并行的电力电缆线路为计算机系统供电；	4.5.2	机房无电力线路冗余措施	对可用性要求较高的 3 级及以上系统
8			d）应提供应急供电设施。	4.5.3	机房无应急供电措施	4 级系统
9		电磁防护	b）应对关键设备或关键区域实施电磁屏蔽。	4.6.1	机房无电磁防护措施	对于数据防泄漏要求较高的 4 级系统
10	安全通信网络	网络架构	a）应保证网络设备的业务处理能力满足业务高峰期需要；	5.1.1	网络设备业务处理能力不足	对可用性要求较高的 3 级及以上系统

序号	层面	控制点	控制项	对应编号	对应案例	适用范围
11			c）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	5.1.2	网络区域划分不当	所有系统
12			d）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；	5.1.3	互联网边界访问控制设备不可控	所有系统
13			d）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；	5.1.4	互联网边界访问控制不当	所有系统
14			d）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；	5.1.5	内部网络区域边界访问控制不当	所有系统
15			e）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	5.1.6	关键线路和设备无冗余措施	对可用性要求较高的3级及以上系统
16			a）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；（云计算安全扩展要求）	5.1.7	云计算平台等级低于承载业务系统等级	所有系统
17		通信传输	a）应采用密码技术保证通信过程中数据的完整性；	5.2.1	数据传输无完整性保护措施	对数据传输完整性要求较高的3级及以上系统
18			b）应采用密码技术保证通信过程中数据的保密性；	5.2.2	敏感信息明文传输	3级及以上系统
19	安全区域边界	边界防护	a）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	6.1.1	互联网边界访问控制设备不可控	所有系统

序号	层面	控制点	控制项	对应编号	对应案例	适用范围
			接口进行通信；			
20			b）应能够对非授权设备私自联到内部网络的行为进行检查或限制；	6.1.2	无违规内联检查措施	3 级及以上系统
21			c）应能够对内部用户非授权联到外部网络的行为进行检查或限制；	6.1.3	无违规外联检查措施	3 级及以上系统
22			d）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；	6.1.4	无线网络无管控措施	3 级及以上系统
23		访问控制	a）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；	6.2.1	互联网边界访问控制配置不当	所有系统
24			e）应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。	6.2.2	通信协议无转换或隔离措施	4 级系统
25		入侵防范	a）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；	6.3.1	无外部网络攻击防御措施	3 级及以上系统
26			b）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；	6.3.2	无内部网络攻击防御措施	3 级及以上系统
27		恶意代码和垃圾邮件防范	a）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	6.4.1	无恶意代码防范措施	所有系统
28		安全审计	a）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	6.5.1	无网络安全审计措施	所有系统

序号	层面	控制点	控制项	对应编号	对应案例	适用范围
			件进行审计；			
29	安全计算环境	身份鉴别	a）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；	7.1.1.1	设备存在弱口令	所有系统
30				7.2.1.1	应用系统口令策略缺失	所有系统
31				7.2.1.2	应用系统存在弱口令	所有系统
32			b）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；	7.2.1.3	应用系统无登录失败处理机制	3 级及以上系统
33			c）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	7.1.1.2	设备鉴别信息无防窃取措施	所有系统
34			d）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。	7.1.1.3	设备未实现双因素认证	3 级及以上系统
35				7.2.1.4	互联网可访问系统未实现双因素认证	3 级及以上系统
36		访问控制	b）应重命名或删除默认账户，修改默认账户的默认口	7.1.2.1	设备默认口令处理不当	所有系统
37				7.2.2.2	应用系统默认口令处理不当	所有系统
38			a）应对登录的用户分配账户和权	7.2.2.1	应用系统登录模块权限控制不当	所有系统
39			e）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；	7.2.2.3	应用系统访问控制存在缺陷	所有系统
40		安全审计	a）应启用安全审计功能，审计覆盖到每	7.1.3.1	设备未开启安全审计措施	3 级及以上系统

序号	层面	控制点	控制项	对应编号	对应案例	适用范围
41			个用户，对重要的用户行为和重要安全事件进行审计；	7.2.3.1	应用系统无安全审计措施	3 级及以上系统
42		入侵防范	b）应关闭不需要的系统服务、默认共享和高危端口；	7.1.4.1	设备开启高危服务端口	所有系统
43			c）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；	7.1.4.2	管理终端无管控措施	3 级及以上系统
44			d）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；	7.2.4.1	数据有效性检验功能存在缺陷	所有系统
45			e）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；	7.1.4.3	互联网设备未修补已知重大漏洞	所有系统
46				7.1.4.4	内部设备存在可被利用高风险漏洞	所有系统
47				7.2.4.2	应用系统存在可被利用的高风险漏洞	所有系统
48				7.2.4.3	应用系统存在严重逻辑缺陷类漏洞	所有系统
49		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。	7.1.5.1	Windows 操作系统无恶意代码防范措施	所有系统
50		数据完整性	a）应采用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；	7.2.5.1	数据传输无完整性保护措施	对数据传输完整性要求较高的 3 级及以上系统

序号	层面	控制点	控制项	对应编号	对应案例	适用范围
51		数据保密性	a）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；	7.2.6.1	敏感信息明文传输	3 级及以上系统
52			b）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。	7.2.6.2	敏感信息无存储保密性保护	所有系统
53		数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；	7.2.7.1	数据备份措施缺失	所有系统
54			b）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；	7.2.7.2	异地备份措施缺失	对系统、数据容灾要求较高的 3 级及以上系统
55			c）应提供重要数据处理系统的热冗余，保证系统的高可用性	7.2.7.3	数据处理系统无冗余措施	对数据处理可用性要求较高的 3 级及以上系统
56			d）应建立异地灾难备份中心，提供业务应用的实时切换。	7.2.7.4	未建立异地灾难备份中心	对容灾、可用性要求较高的 4 级系统
57		剩余信息保护	a）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；	7.2.8.1	鉴别信息释放措施失效	所有系统
58			b）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。	7.2.8.2	敏感数据释放措施失效	3 级及以上系统
59		个人信息保护	a）应仅采集和保存业务必需的用户个人信息；	7.2.9.1	违规采集、存储个人信息	所有系统
60			b）应禁止未授权访问和非法使用用户个	7.2.9.2	非授权访问、使用个人信息	所有系统

序号	层面	控制点	控制项	对应编号	对应案例	适用范围
			人信。			
61		数据完整性和保密性	a）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；（云计算安全扩展要求）	7.2.10.1	云服务客户数据、用户个人信息违规出境	云计算平台
62	安全区域边界	集中管控	c）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；	8.1.1	运行监控措施缺失	可用性要求较高的3级及以上系统
63			d）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；	8.1.2	日志存储时间不满足要求	3级及以上系统
64			f）应能对网络中发生的各类安全事件进行识别、报警和分析；	8.1.3	安全事件发现处置措施缺失	3级及以上系统
65	安全管理制度	管理制度	a）应对安全管理活动中的各类管理内容建立安全管理制度；	9.1.1	管理制度缺失	所有系统
66	安全管理机构	岗位设置	a）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	10.1.1	未建立网络安全领导小组	3级及以上系统
67	安全建设管理	产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规	11.1.1	违规采购和使用网络安全产品	所有系统
68			b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；	11.1.2	违规采购和使用密码产品与服务	所有系统
69		外包软件开发	c）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。	11.2.1	外包开发代码审计措施缺失	涉及金融、民生、基础设施等重要核心领域的3级及以

序号	层面	控制点	控制项	对应编号	对应案例	适用范围
						上系统
70		测试验收	b）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。	11.3.1	上线前未开展安全测试	3 级及以上系统
71	安全运维管理	漏洞和风险管理	a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；	12.1.1	未对安全漏洞和隐患进行识别与修补	3 级及以上系统
72		网络和系统安全管理	g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；	12.2.1	未将重要运维操作纳入变更管理制度	3 级及以上系统
73			h）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；	12.2.2	未对运维工具进行管控	3 级及以上系统
74			j）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。	12.2.3	未对运维外联进行管控	3 级及以上系统

序号	层面	控制点	控制项	对应编号	对应案例	适用范围
75		恶意代码防范管理	a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；	12.3.1	未对外来接入设备进行恶意代码检查	3 级及以上系统
76		变更管理	a）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；	12.4.1	未建立变更管理制度	3 级及以上系统
77		备份与恢复管理	c）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。	12.5.1	未建立数据备份策略	3 级及以上系统
78		应急预案管理	b）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；	12.6.1	未制定应急预案	所有系统
79			c）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；	12.6.2	未对应急预案进行培训演练	3 级及以上系统
80		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。（云计算安全扩展要求）	12.7.1	云计算平台运维方式不当	云计算平台