等级保护 2.0 测评指导书

目录

一、 安全物理环境测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内	机房场地所在的建筑物要具有防震、防风和防雨等的能力	1) 核查是否有建筑物抗震设防审批文档 2) 核查是否有雨水渗漏的痕迹 3) 核查是否有可灵活开启的窗户， 若有窗户， 是否做了封闭、上锁等防护措施 4) 核查屋顶、 墙体、门窗和地面等是否有破损开裂的情况	1) 机房具有验收文档 2) 天花板、窗台下无水渗漏的现象 3) 机房无窗户， 有窗户且做了防护措施 4) 现场观测屋顶、 墙体、门窗和地面等无开裂的情况
	b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施,	机房场地要避免设置在建筑物的顶层或地下室。如果因为某些原因无法避免时，设置在建筑物顶层或地下室的机房需要加强防水和防潮措施	1) 核查机房是否在顶层或地下室 2) 若是，核查机房是否采取了防水和防潮措施	1) 非建筑物顶层或地下室 2) 在顶层或地下室的， 做了严格的防水防潮措施

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	为防止非授权人员进入机房，需要安装电子门禁系统对机房及机房内区域的出入人员实施访问控制，避免由于非授权人员的擅自进入，造成系统运行中断、设备丢失或损坏、数据被窃取或篡改，并可利用系统实现对人员进入情况的记录	1) 核查出入口是否配置电子门禁系统 2) 核查电子门禁系统是否开启并正常运行 3) 核查电子门禁系统是否可以鉴别、记录进入的人员信息	1) 机房出入口是配备电子门禁 2) 电子门禁系统工作正常，可对进出人员进行鉴别
防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识	对于安放在机房内用于保障系统正常运行的设备或主要部件需要进行固定，并设置明显的不易除去的标记用于识别	1) 核查机房内设备或主要部件是否固定 2) 核查机房内设备或主要部件上是否设置了明显且不易除去的标记	1) 机房内设备均放置在机柜或机架，并已固定 2) 设备或主要部件均设置了不易除去的标识、标志，如使用粘贴方式则不能有翘起
	b) 应将通信线缆铺设在隐蔽安全处	机房内通信线缆需要铺设在隐蔽安全处，防止线缆受损	核查机房内通信线缆是否铺设在隐蔽安全处	机房通信线缆铺设在线槽或桥架里
	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	机房需要安装防盗报警系统，或在安装视频监控系统的同时安排专人进行值守，防止盗窃和恶意破坏行为的发生	1) 核查是否配置防盗报警系统或专人值守的视频监控系统 2) 核查防盗报警系统或视频监控系统是否开启并正常运行	1) 机房内配置了防盗报警系统或专人值守的视频监控系统 2） 现场观测时监控系统正常工作
防雷击	a) 应将各类机柜、设施和设备等通过接地系统安全接地	在机房内对机柜、各类设施和设备采取接地措施，防止雷击对电子设备产生 损害	核查机房内机柜、设施和设备等是否进行接地处理，通常黄绿色相间的电线为接地用线	机房内所有机柜、设施和设备等均已采取了接地的控制措施

	b) 应采取 措施 防止 感应雷，例如设置防雷保安器或过压保护装置等	在机房内安装防雷保安器或过压保护等装置 ，防止感应雷对电子设备产生损害	1) 核查机房内是否设置防感应雷措施 2) 核查防雷装置是否通过验收或国家有关部门的技术检测	1) 机房内设置了防感应雷措施，如设置了防雷感应器、 防浪涌插座等 2) 防雷装置通过了国家有关部门的技术检测
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	机房内需要设置火灾自动消防系统， 可在发生火灾时进行自动检测、报警和灭火， 如采用自动气体消防系统、自动喷淋消防系统等	1）核查机房内是否设置火灾自动消防系统 2) 核查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火 3) 核查火灾自动消防系统是否通过验收或国家有关部门的技术检测	1) 机房内设置火灾自动消防系统 2) 现场观测时火灾自动消防系统工作正常
	b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料	机房内需要采用具有耐火等级的建筑材料，防止火灾的发生和火势蔓延	核查机房验收文档是否明确所用建筑材料的耐火等级	机房所有材料为耐火材料， 如使用墙体、 防火玻璃等， 但使用金属栅栏的不能算符合
	c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施	机房内需要进行区域划分并设置隔离防火措施，防止水灾发生后火势蔓延	1) 核查是否进行了区域划分 2) 核查各区域间是否采取了防火隔离措施	1) 机房进行了区域划分， 如过渡区、主机房 2) 区域间部署了防火隔离装置
防 水 和防潮	a）应采取措施防止雨水通过机房窗户、 屋顶和墙壁渗透	机房内需要采取防渗漏措施，防止窗户、屋顶和墙壁存在水渗透情况	核查窗户、屋顶和墙壁是否采取了防渗漏的措施	机房采取了防雨水渗透的措施，如封锁了窗户并采取了防水、屋顶和墙壁均采取了防雨水渗透的措施

	b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透	机房内需要采取防结露和排水措施，防止水蒸气结露和地面产生积水	1) 核查是否采取了防止水蒸气结露的措施 2) 核查是否采取了排水措施，防止地面产生积水	1) 机房内配备了专用的精密空调来防止水蒸气结露的控制措施 2) 机房内部署了漏水检测装置，可以对漏水进行监控报警
	c) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警	机房内需要布设对水敏感的检测装置，对渗水、漏水情况进行检测和报警	1) 核查是否安装了对水敏感的检测装置 2) 核查防水检测和报警装置是否开启并正常运行	1) 机房内部署了漏水检测装置，如漏水检测绳等 2) 检测和报警工作正常
防静电	a) 应采用防静电地板或地面并采用必要的接地防静电措施	机房内需要安装防静电地板或在地面采取必要的接地措施，防止静电的产生	1) 核查是否安装了防静电地板 2) 核查是否采用了防静电接地措施	1) 机房部署了防静电地板 2) 机房采用了接地的防静电措施
	b) 应采取措施防上静电的产生，例如采用静电消除器、佩戴防静电手环等。	机房内需要配备静电消除器 E 佩戴防静电手环等消除静电的设备。	核查机房内是否配备了静电消除设备。	机房配备了防静电设备
湿温度控制	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	机房内需要安装温、湿度自动调节装置，如空调、除湿机、通风机等，使机房内温、湿度的变化在适宜设备运行所允许的范围之内。通常机房内适宜的温度范围是 18~27℃，空气湿度范围是 35~75%	1) 核查机房内是否配备了专用空调 2) 核查机房内温湿度是否在设备运行所允许的范围之内	1) 机房内配备了专用的精密空调 2) 机房内温湿度设置在 20-25, 湿度为：40%-60%
电力供应	a) 应在机房供电线路上配置稳压器和过电压防护设备	机房供电线路上需要安装电流稳压器和电压过载保护装置，防止电力波动对电子设备造成损害	核查供电线路上是否配置了稳压器和过电压防护设备	1) 机房的计算机系统供电线路上设置了稳压器和过电压防护设备

				2) 现场观测时稳压器和过电压防护设备可正常工作
	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	机房供电需要配备不间断电源 (UPS)或备用供电系统，如备用发电机或使用第三方提供的备用供电服务，防止电力中断对设备运转和系统运行造成损害	1) 核查是否配备不间断电源(UPS)等备用供电系统 2) 核查不间断电源 (UPS)等备用供电系统的运行切换记录和检修维护记录	1) 机房配备了 UPS 后备电源系统 2)UPS 能够满足短期断电时的供电要求
	c) 应设置冗余或并行的电力电缆线路为计算机系统供电	机房供电需要使用冗余或并行的电力电缆线路，防止电力中断对设备运转和系统运行造成损害	核查是否设置了冗余或并行的电力电缆线路为计算机系统供电	为机房配备了冗余的供电线路，如市电双路接入
电磁防护	a) 电源线和通信线缆应隔离铺设，避免互相干扰	机房内电源线和通信线缆需要隔离铺设在不同的管道或桥架内,防止电磁辐射和干扰对设备运转和系统运行产生的影响	核查机房内电源线缆和通信线缆是否隔离铺设	机房内电源线缆和通信线缆隔离铺设，如通过线槽或桥架进行了隔离
	b) 应对关键设备实施电磁屏蔽	机房内关键设备需要安放在电磁屏蔽机柜内或电磁屏蔽区域内,防止电磁辐 射和干扰对设备运转和系统运行产生的影响	核查机房内是否为关键设备配备了电磁屏蔽装置	为关键设备采取了电磁屏蔽措施，如配备了屏蔽机柜或屏蔽机房，关键设备 如加密机

二、安全通信网络测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据

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	为了保证主要网络设备具备足够处理能力，应定期检查设备资源占用情况，确保设备的业务处理能力具备冗余空间。	1) 应访谈网络管理员业务高峰时期为何时，核查边界设备和主要网络设备的处理能力是否满足业务高峰期需要，询问采用何种手段对主要网络设备的运行状态进行监控。 以华为交换机为例，输入命令"display cpu -usage" , "display memory-usage" 查看相关配置。一般来说，在业务高峰期主要网络设备的CPU内存最大使用率不宜超过 70%，也可以通过综合网管系统查看主要网络设备的 CPU、内存的使用情况 2) 应访谈或核查是否因设备处理能力不足而出现过宕机情况，可核查综合网管系统告警日志或设备运行时间等，或者访谈是否因设备处理能力不足而进行设备升级。 以华为设备为例，输入命令 "display version ”，查看设备在线时长，如设备在线时间在近期有重启可询问原因 3) 应核查设备在一段时间内的性能峰值，结合设备自身的承载性能，分析是否能够满足业务处理能力	1) 设备 CPU和内存使用率峰值不大于 70%，通过命令核查相关使用情况： <Huawei>display cpu-usage CPU Usage Stat ， Cycle: 60 (Second) CPU Usage :3% Max: 45%. CPU Usage Stat. Time: 2?18 -05-26 16: 58:16 CPU utilization for five seconds: 15%: one minute:15%: five minutes: 15% <Huawei>display memory-usage CPU utilization for five seconds: 15%: one minute: 15%: five minutes: 15% System Total Memory Is: 75312648 bytes Total Memory Used Is: 45037704 bytes Memory Using Percentage Is: 59% 2) 未出现宕机情况，网管平台未出现宕机告警日志，设备运行时间较长 ： <Huawei>display version Huawei Versatile Routing Platform Software VRP (R) software, Version 5. 130 (AR1200 V200ROO3C0O Copyright (C) 2011-2012 HUAWEI TECH Co., LTD Huawei AR1220 Router uptime is 0 week, 0 day, 0 hour, 1 minute MPU 0(Master) : uptime is 0 week,0 day, 0 hour, I minute 3) 业务高峰流量不超过设备处理能力的 70%

	b) 应保证网络各个部分的带宽满足业务高峰期需要	为了保证业务服务的连续性，应保证网络各个部分的带宽满足业务高峰期需要。如果存在带宽无法满足业务高峰期需要的情况，则需要在主要网络设备上进行带宽配置，保证关键业务应用的带宽需求	1) 应访谈管理员高峰时段的流量使用情况，是否部署流量控制设备对关键业务系统的流量带宽进行控制，或在相关设备上启用 QoS配置，对网络各个部分进行带宽分配，从而保证业务高峰期业务服务的连续性 2) 应该查综合网管系统在业务商峰时段的带宽占用情况，分析是否满足业务需求。如果无法满足业务高蜂期需要，则需要在主要网络设备上进行带宽配置 3) 测试验证网络各个部分的带宽是否满足业务高峰期需求	1) 在各个关键节点部署流量监控系统， 能够监测网络中的实时流量，部署流量控制设备，在关键节点设备品置 QoS策略，对关健业务系统的流量带宽进行控制 2) 节点设备配置了流量监管和流量整形策略 ； 流量监管配置 ： class-map ：class-1 bandwidth percent 50 bandwidth 5000 (kbps ） max threshold 64 (packets) class-map ：class-2 bandwidth percent 15 bandwidth 1500 (kbps) max threshold 64 (packets) 流量整形配置 ： traffic classifier c1 operator or if-match acl 3002 traffic behavior b1 remark local-precedence af3 traffic policy p1 classifier c1 behavior b1 interface gigabitethernet 3/0/0 traffic-policy p1 inbound 3) 各通信链路高峰流量均不大其带宽的 70%

	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地址	根据实际情况和区域安全防护要求，应在主要网络设备上进行 VLAN划分。 VLAN 是一种通过将局域网内的设备逻辑地而不是物理 地划分成不同子网从而实现虚拟工作组的新技术。不同 VLAN内的报文在传输时是相互隔离的 , 即一个 VLAN 内的用户不能和其它 VLAN 内的用户直接通信，如果不同 VLAN要进行通信， 则需要通过路由器或三层交换机等三层设备实现	应访谈网络管理员，是否依据部门的工作职能、等级保护对象的重要程度和应用系统的级别等实际情况和区域安全防护要求划分了不同的 VLAN, 并核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。 以 Cisco IOS 为例，输入命令“ show vlan brief ”， 查看相关配置	划分不同的网络区域， 按照方便管理和控制的原则为各网络区域分配地址，不同网络区域之间应采取边界防护措施： 10 server active 20 user active 30 test active 99 management active
	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	为了保证等级保护对象的安全，应避免将重要网段部署在网络边界处且直接连接外部等级保护对象，防止来自外部等级保护对象的攻击。同时，应在重要网段和其它网段之间配置安全策略进行访问控制	1) 应核查网络拓扑图是否与实际网络运行环境一致 2) 应核查重要网络区域是否未部署在网络边界处；网络区域边界处是否部署了安全防护措施 3) 应核查重要网络区域与其他网络区域之间，例如应用系统区、数据库系统区等重要网络区域边界是否采取可靠的技术隔离手段，是否部署了网闸、防火墙和设备访问控制列表 (ACL) 等	1) 网络拓扑图与实际网络运行环境一致 2）重要网络区域未部署在网络边界处 3) 在重要网络区域与其他网络区域之间部署了网闸、 防火墙等安全设备实现了技术隔离

	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，保证系统的可用性	本要求虽然放在“安全通信网络”分类中，实际是要求整个网络架构设计需要冗余。为了避免网络设备或通信线路出现故障时引起系统中断，应采用冗余技术设计网络拓扑结构，以确保在通信线路或设备故障时提供备用方案，有效增强网络的可靠性	应核查系统的出口路由器、核心交换机、安全设备等关键设备是否有硬件冗余和通信线路冗余，保证系统的高可用性	采用 HSRP、VRRP等冗余技术设计网络架构，确保在通信线路或设备故障时网络不中断，有效增强网络的可靠性
通信传输	a) 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	为了防止数据在通信过程中被修改或破坏，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，这些数据包括鉴别数据、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	1) 应核查是否在数据传输过程中使用校验技术或密码技术来保证其完整性 2) 应测试验证设备或组件是否保证通信过程中数据的完整性。例如使用File ChecksumIntegrity Verifier、SigCheck 等工具对数据进行完整性校验	1) 对鉴别数据、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数据等采用校验技术或密码技术保证通信过程中数据的完整性； 2) File ChecksumIntegrity Verifier 计算数据的散列值，验证数据的完整性
	b) 应采用密码技术保证通信过程中数据的保密性	根据实际情况和安全防护要求，为了防止信息被窃听，应采取技术手段对通信过程中的敏感信息字段或整个报文加密，可采用对称加密、非对称加密等方式实现数据的保密性	1) 应核查是否在通信过程中采取保密措施，具体采用哪些技术措施 2) 应测试验证在通信过程中是否对敏感信息字段或整个报文进行加密，可使用 Sniffer、Wireshark 等测试工具通过流量镜像等方式抓取网络中的数据，验证数据是否加密	1) 对鉴别数据、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数据等采用密码技术保证通信过程中数据的保密性 2)Sniffer. Wireshak 可以监视到信息的传送，但是显示的是加密报文

可信验证	可基于可信根对通信设备的系统引导程序、系统程序、 重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	通信设备可能包括交换机、路由器或其他通信设备等，通过设备的启动过程和运行过程中对预装软件 （包括系统引导程序、系统程序、相关应用程序和重要配置参数 ）的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1) 应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证 2) 应核查是否在应用程序的关键执行环节进行动态可信验证 3) 应测试验证当检测到设备的可信性受到破坏后是否进行报警 4) 应测试验证结果是否以审计记录的形式送至安全管理中心 (2.3)	1) 通信设备、 交换机、路由器或其他通信设备具有可信根芯片或硬件 2) 启动过程基于可信根对系统引导程序、系统程序，重要配置参数和关键应用程序等进行可信验证度量 3) 在检测到其可信性受到破坏后进行报警， 并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结果记录 (2.3)

三、安全区域边界测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
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接口进行通信	为了保障数据通过受控边界，应明确网络边界设备，并明确边界设备物理端口，网络外连链路仅能通过指定的设备端口进行数据通信	1) 应核查网络拓扑图与实际的网络链路是否一致，是否明确了网络边界，且明确边界设备端口。 2) 应核查路由配置信息及边界设备配置信息，确认是否指定物理端口进行跨越边界的网络通信。 以 Cisco I0S 为例，输入命令“ router#show running - config ”，查看相关配置。 3) 应采用其他技术手段核查是否不存在其他未受控端口进行跨越边界的网络通信，例如检测无线访问情况，可使用无线嗅探器、无线入侵检测 / 防御系统、手持式无线信号检测系统等相关工具进行检测	1) 查看网络拓扑图，并比对实际的网络链路，确认网络边界设备及链路接入端口无误 2) 通过相关命令显示设备端口、Vlan 信息 interface IP-Address 0K? Method Status Protocol FastEehernet0/0 192.168.11.1 YES manual up up FastEehernet0/1 192.168.12.1 YES manual up up Vlan1 unassigned YES manual down down (administratively) 显示路由信息 IP route 0.0.0.0 0.0.0.0.192.168.12

				3) 通过网络管理系统的自动拓扑发现功能，监控是否存在非授权的网络出口链路；通过无线嗅探器排查无线网络的使用情况，确认无非授权 WiFi
	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	设备的“非授权接入”可能会破坏原有的边界设计策略，可以采用技术手段和管理措施对“非授权接入”行为进行检查。技术手段包括部署内网安全管理系统，关闭网络设备未使用的端口，绑定 IP/MAC 地址等	1) 应访谈网络管理员，询问采用何种技术手段或管理措施对非授权设备私自联到内部网络的行为进行管控，并在网络管理员的配合下验证其有效性 2) 应核查所有路由器和交换机等设备闲置端口是否均已关闭。 以 Cisco I0S 为例，输入命令 "show ip interfaces brief ” 3) 如通过部署内网安全管理系统实现系统准入，应检查各终端设备是否统一进行了部署，是否存在不可控特殊权限接入设备 4）如果采用了 IP/MAC 地址绑定的方式进行准入控制，应核查接入层网络设备是否配置了 IP/MAC 地址绑定等措施 以 Cisco I0S 为例，输入命令 "show ip arp ”	1) 非使用的端口均已关闭，查看设备配置中是否存在如下类似配置： Interface FastEthernet0/1 shutdown 2) 网络中部署的终端管理系统已启用，且各终端设备均已有效部署，无特权设备 3)IP/MAC 地址绑定结果，查看设备配置中是否存在如下类似配置： arp 10.10.10.1 0000.e268.9890 arpa

	c) 应能够对内部用户非授权连到外部网络的行为进行检查或限制	内网用户设备上的外部连接端口的“非授权外联“行为也可能破坏原有的过界设计策略，可以通成内网安全管理系统的非授权外联管控功能或者防非法外联系统实现“非授权外联”行为的控制，由于内网安全管理系统可实现包括非授权外连管控在内的众多的管理功能，建议c采用该项措施。通过对用户非授权建立网络连接访问非可信网络的行为进行管控，从而减少安全风险的引入	1) 应核查是否采用内网安全管理系统或其它技术手段，对内部用户非授权连接到外部网络的行为进行限制或检查 2) 应核查是否限制终端设备相关端口的使用，如禁用双网卡、USB接口、Modem、无线网络等，防止内部用户非授权外连行为	1) 网络中部署有终端安全管理系统，或非授权外联管控系统 2) 网络中各类型终端设备均已正确部署了终端安全管理系统或外联管控系统，并启用了相关策略，如禁止更改网络配置，禁用双网卡、USB接口．、Mode、无线网络等
	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	为了防止未经授权的无线网络接入行为，无线网络应单独组网并通过无线接入网关等受控的边界防护设备接入到内部有线网络。同时，应部署无线网络管控措施，对分非授权无线网络进行检测、屏蔽	1) 应访谈网络管理员是否有授权的无线网络，是否单独组网后接入到有线网络 2) 应核查无线网络部署方式，是否部署无线接入网关，无线网络控制器等设备。应检查该类型设备配置是否合理，如无线网络设备信道使用是否合理，用户口令是否具备足够强度、是否使用WPA2加密方式等 3) 应核查网络中是否部署了对非授权无线设备管控措施，能够对非授权无线设备进行检查、屏蔽。如使用无线嗅探器、无线入侵检测/防御系统、手持式无线信号检测系统等相关工具进行检测、限制	1) 授权的无限网络通过无线接入网管，并通过防火墙等访问控制设备接入到有限网络。无线网络使用了1信道，防止设备间互相干扰；使用WPA2进行加密；且用户密码具备复杂度要求，如：口令长度8位以上，由数字、字母、大小写及特殊字符组成 2) 通过无线嗅探器未发现非授权无线设备

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	应在网络边界或区域之间部署网闸， 防火墙、 路由器、 交换机和无线接入网关等提供访问控制功能的设备或相关组件，想据访问控制策略设置有效的访问控制规则，访问控制规测采用白名单机制	1) 应核查在网络边界或区域之间是否部署访问控制设备，是否启用访问控制策略 2) 应核查设备的访问控制策略是否为白名单机制，仅允许授权的用户访问网络资源，禁止其他所有的网络访问行为 3) 应该检查配置的访问控制策略是否实际应用到相应的接口的进或出方向。 以 Cisco I0S 为例， 输入命令""Show running-config" ,检查配置文件中访问控制策略	设备访问控制策略具体如下： access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 192.168.3.10 eq 3389 access-list 100 permit tcp 192.168.1.0 0.0.0. 255 host 192.168.3.11 eq 3389 access-list 100 deny ip any any interface Gigabi tEthernet1/1 ip access-group 100 in
	b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化	根据实际业务需求配置访问控制策略，仅开放业务必须的端口， 禁止配置全通策略，保证边界访问控制设备安全策略的有效性。不同访问控制策略之间的逻辑关系应合理，访问控制策略之间不存在相互冲突，重叠或包含的情况 ；同时， 应保障访问控制规则数量最小化。	1) 应访谈安全管理员访问控制策略配置情况，核查相关安全设备的访问控制策略与业务及管理需求的一致性，结合策略命中数分析策略是否有效 2) 应检查访问控制策略中是否已禁止了全通策略或端口、地址限制范围过大的策略。 3) 应核查设备的不同访问控制策略之间的逻辑关系是否合理。 以 Cisco IOS 为例， 输入命令 ”show running-config “ ,检查配置文件中访问控制列表配置项	1) 访问控制需求与策略保持一致 2) 应合理配置访问控制策略的优先级，如 access-list 100 permit tcp 192.168 0.0.0.0.255.255 host 192.168.3.10 access-list 100 deny tcp 192. 168.1.0 0.0. 0.255 host 192.168.3.10 上述访问控制策略排列顺序不合理 ，第二条策略应在前面 ，否则不能被命中 3) 应禁用全通策略，如 access-list 100 permit tcp any host any eq any 4) 应合并相互包含的策略，如 ： access-list 100 permit tcp 192.168.0.0.0.255.255 host 192.168.3.10 access-list 100 permit tcp 192.168.1.0.0.255.255 host

				192.168.3.10 第二条策略不起作用，可直接删除
	c) 应对源地址、目的地址，源端口、 目的端口和协议等进行检查，以允许 / 拒绝数数据包进出	应对网络中网闸、 防火墙、 路由器、交换机和无线接入网关等提供访问控制功能的设备或相关组件进行检查，访问控制策略应明确源地址、 目的地址 ， 源端口、 目的端口和协议，以允许 / 拒绝数据包进出	应核查设备中访问控制策略是否明确设定了源地址、目的地址、源端口、目的端只和协议等相关配置参数。 以 Ciso IOS 为例 拒绝所有从 172.16.4.0 到 172.16.3.0 的 ftp 通信流量通过 F0/0 接口， 输入命令： ”show running-config “ , 检查配置文件中访问控制列表配置项	检查配置文件中是否存在类似如下配置项： access-list 101 deny tcp 172.16.4.0.0.0.255 172.16.3.0.0.0.255 eq 21 access-list 101 permit ip any any interface fastetnernet0/0 ip access-group101 out
	d) 应能根据会话状态信息为进出数据流提供明确的允许 / 拒绝访问的能力	防火墙能够根据数据包的源地址、目标地址、 协议类型、 源端口、 目标端口等对数据包进行控制，而且能够记录通过防火墙的连接状态，直接对包里的数据进行处理。防火墙还应具有完备的状态检测表来追踪连接会话状态，并结合前后数据包的关系进行综合判断，然后决定是否允许该数据包通过，通过连接状态进行更迅速更安全地过滤	应核查状态检测防火墙访问控制策略中是否明确设定了源地址、 目的地址、 源端口、目的端口和协议 以 Cisco IOS 为例，输入命令 ： show running0-config.	检查配置文件中应当存在类似如下配置项 ： access-list 101 permit tcp 192.168.2.0.0.0.255 host 192.168.3.100 eq 21 access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 192.168.3.10 eq 80 access-list 101 deny ip any any
	e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制	在网络边界采用下 - 代防火墙或相关安全组件 ，实现基于应用协议和应用内容的访问控制	1) 应核查在关键网络节点处是否部署访问控制设备 2) 应检查访问控制设备是否配置了相关策略，对应用协议、 应用内容进行访问控制，并对策略有效性进行测试	防火墙配置应用访问控制策略，从应用协议、应用内容进行访问控制，对 QQ 聊天工具、优酷视频以及各、 Web服务、 FTP 服务等进行管控

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	要维护系统安全，必须进行主动监视，以检查是否发生了入侵和攻击。监视入侵和安全事件既包括被动任务也也包括主动任务。很多入侵都是在发生攻击之后，通过检查日志文件才检测到的。这种攻击之后的检测通常被称为被动入侵检测；只有通过检查日志文件，攻击才得以根据日志信息进行复查和再现。其他入侵尝试可以在攻击发生的同时检测到，这种方法称为“主动入侵检测，它会查找已知的攻击模式或命令，并阻止这些命令的执行。 完整的入侵防范应首先实现对事件的特征分析功能，以发现潜在的攻击行为，应能发现目前主流的各种攻击行为，如端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。 目前对入侵防范的实现主要是通过在网络边界部署包含入侵防范功能的安全设备，如抗 APT 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统、入侵检测系统	1) 应核查相关系统或设备是否能够检测从外部发起的网络攻击行为 2) 应核查相关系统或设备的规则库版本是否已经更新到最新版本 3) 应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点 4) 应测试验证相关系统或设备的安全策略是否有效	1) 相关系统或设备有检测到外部发起攻击行为的信息； 2) 相关系统或设备的规则库进行了更新，更新时间与测评时间较为接近 3) 配置信息、安全策略中制定的规则覆盖系统关键节点的 IP 地址等 4) 监测到的攻击日志信息与安全第略相符

		(IDS)，入侵防御系统 (IPS)、包含入侵防范模块的多功能安全网关(UTM)等。 为了有效检测，防止或限制从外部发起的网络攻击行为，应在网络边界、核心等关键网络节点处部署 IPS等系统，或在防火墙、UTM启用入侵防护功能		

	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政击行为	为了有效检测、防止或限制从内部发起的网络攻击行为，应在网络边界、核心等关键网络节点处部署 IPS 等系统， 或在防火墙、 UTM启用入侵防护功能	1) 应核查相关系统或设备是否能够检测到从内部发起的网络攻击行为 2) 应核查相关系统或设备的规则库版本是否已经更新到最新版本 3) 应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点 4) 应测试验证相关系统或设备的安全策略是否有效	1) 相关系统或设备有检测到外部发起攻击行为的信息 ； 2) 相关系统或设备的规则库进行了更新， 更新时间与测评时间较为接近 3) 配置信息、 安全策略中制定的规则覆盖系统关键节点的 IP 地址等 4) 监测到的攻击日志信息与安全策略相符的
	c) 应在关键网络节点处检测、防止或限制从内部发起的网络政击行为	为了有效检测、防止或限制从内部发起的网络功击行为，应在网络边界、核心等关键网络节点处部署 IPS 等系统，或在防火墙， UTM 启用入侵防护功能	1) 应核查相关系统或设备是否能够检测到从内部发起的网络攻击行为 2) 应核查相关系统或设备的规则库版本是否已经更新到最新版本 3) 应核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点 4) 应测试验证相关系统或设备的安全策略是否有效	1) 相关系统或设备有检测到内部发起攻击行为的信息 2) 相关系统或设备的规则库进行了更新， 更新时间与测评时间较为接近 3) 配置信息、 安全策略中制定的规则覆盖系统关键节点的 IP 地址等 4) 监测到的攻击日志信息与安全策略相符
	d) 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	部署网络回溯系统或抗 APT 攻击系统等实现对新型网络攻击行为进行检测和分析	1) 应核查是否部署回溯系统或抗 APT攻击系统，实现对新型网络攻击行为进行检测和分析 2) 应核查相关系统或设备的的规则库版本是否已经更新到最新版本 3) 应测试验证是否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析	1) 系统内部署网络回溯系统或抗 APT攻击系统， 系统内包含对新型网络攻击的检测和分析功能 2) 网络回溯系统或抗 APT攻击系统的规则库进行了更新， 更新时间与测评时间较为接近 3) 经测试验证系统可对网络行为进行分析，且能够对未知新型网络攻击检测和分析

	e) 当检测到攻击行为时，记录攻击源 P、攻击类型、攻击目标、 攻击时间，在发生严重入侵事件时应提供报警。	为了保证系统受到攻击时能够及时准确的记录攻击行为并进行安全应急响应，当检测到攻击行为时， 应对攻击源 IP、 攻击类型、 攻击目标和攻击时间等信息进行日志记录。通过这些日志记录，可以对攻击行为进行审计分析。当发生严重入侵事件时， 应能够及时向有关人员报警，报警方式包括短信、邮件等。	1) 访谈网络管理员和查看网络拓扑结构，查看在网络边界处是否部署了包含入侵防范功能的设备。如果部署了相应设备，则检查设备的日志记录 ，查看是否记录了攻击源 IP、攻击类型、攻击目的和攻击时间等信息，查看设备采用何种方式进行报警 2) 应测试验证相关系统或设备的报警策略是否有效	1) 相关具有入侵防范功能的设备日志记录了攻击源 IP、攻击类型、攻击目标、 攻击时间等信息 2) 设备的报警功能已开启且处于正常使用状态
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新	计算机病毒、木马和蠕虫的泛滥使得防范恶意代码的破坏显得尤为重要。恶意代码是指怀有恶意目的可执行程序。目前恶意代码主要都是通过网页、邮件等网络载体进行传播。因此在网络边界处部署防恶意代码产品进行恶意代码防范是最为直接和高效的办法。 防恶意代码产品目前生要包括防病毒网关，包含防病毒模块的多功能安全网关等产品。其至少应具备的功能包括 ：对恶意代码的分析检查能力，对恶意代码的清除或阻断能力，以及发现恶意代码后记录日志和审计，并包含对恶意代码特征库的升级和检测系统的更新能力。 恶意代码具有特征变化快的特点。	1) 应访谈网络管理员和检查网络拓结构，查看在网络边界处是否部署了防恶意代码产品。如果部署了相关产品，则查看是否启用了恶意代码检测并查看白志记录中是否有相关阻断信息 2) 应访谈网络管理员，是否对防恶意代码产品的特征库进升级及具体的升级方式，并登录相应的防恶意代码产品，核查其特征库升级情况，当前是否为最新版本 3) 应测试验证相关系统或设备的安全策略是否有效	1) 在网络边界处及部署防恶意代码产品或组件，防恶意代码的功能正常开启且具有对恶意代码检测和清除的功能 2) 防恶意代码的特征库进行了开级， 且升级时间与测评时间较为接近

		因此对于恶意代码检测重要的特征库更新， 以及监测系统自身的更新，都非常重要。 产品应具备通过多种方式实现恶意代码特征库和检测系统更新的能力。如自动远程更新，手动选程更新， 手动本地更新等方		
	b) 应在关键网络节点处对垃圾邮件进行检测和防护并维护垃圾邮件防护机制的升级和更新	垃圾邮件是指电子邮件使用者事先未提出要求或同意接收的电子邮件，应部署相应设备或系统对垃圾邮件进行识别和处理，包括部署透明的防垃圾邮件网关。基于转发的防垃圾邮件系统、安装于邮件服务器的防垃圾邮件软件，以及与邮件服务器一体的防垃圾邮件的邮件服务器等，并保证规则库已经更新到最新	1) 应核查在关键网络节点处是否部署了防垃圾邮件设备或系统 2) 应核查防垃圾邮件产品运行是否正常，防垃投邮件规则库是否已经更新到最新。 3) 应测试验证相关系统或设备的安全策略是否有效	1）在网络关键节点处部署了防垃投邮件设备的产品或组件， 防垃级邮件设备的功能正常开启 2) 防垃报邮件防护机制的进行了升级和更新，且升级时间与测评时间较为接近 3) 测试结果显示系统或设备能够对垃圾邮件成功的阻断
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件进行审计	为了对重要用户行为和重要安全事件进行审计 ，需要在网络边界部署相关系统，启用重要网络节点日志功能，将系统日志信息输出至各种管理端口、内部缓存或者日志服务器	1) 核查是否部署了综合安全审计系统或类似功能的系统平台 2) 核查安全审计范围是否覆盖到每个用户并对重要的用户行为和重要安全事件进行了审计	1) 在网络边界处、 重要网络节点处部界了审计设备 2）审计的范围能够覆盖到每个用户， 且审计记录包合了重要的用户行为和重要安全事件

	b) 审计记录应包括事件的日期和时间、 用户、事件类型、事件是否成功及其他与审计相关的信息	审计记录包含内容是否全面将直接影响审计的有效性，网络边界处和重要网络节点的日志审计内容应记录事件的时间、 类型、用户、事件类型、事件是否成功等必要信息	核查审计记录信意是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。 -般来说，对于主流路由器和交换机设备，可以实现对系统错误、 网络和接口的变化、登录失败、 ACL 匹配等进行审计，审计内容向括了时间、类型、用户等相关信息。因此，只要这些路由器和交换机设备启用审计功能就能符合该项要求。但对于防火墙等安全设备来说，由于其访同控制策略命中日志需要手动启用，因此应重点核查其访问控制策命中日志是否启用	审计记录包含了事件的日期和时间、用户、事件类型、事件是否成功等信息
	c) 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	审计记录能够帮助管理人员及时发现系统运行状况和网络攻击行为，因此需要对审计记录实施技术上和管理上的保护， 防止未授权修改、 删除和破坏。可以设置专门的日志服务器来接收设备发送出的报警信息。非授权用户 (审计员除外) 无权删除本地和日志服务器上的审计记录	1) 核查是否采取了技术措施对审计记录进行保护 2) 核查审计记录的备份机制和备份策略是否合理	1) 审计系统开启了日志外发功能，日志转发至日志服务器 2) 审计记录存储超过 6 个月以上

	d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析	对于远程访问用户，应在相关设备上提供用户认证功能。通过配置用户、用户组，并结合访问控制规则可以实现对认证成功的用户允许访问受控资源。此外，还需对内部用户访问互联网的行为进行审计分析	核查是否对远程访问用户及互联风访问用户行为单独进行审计分析，并核查审计分析的记录是否包含了用于管理远程访同行为、访问互联网用户行为必要的信息	在网络边界处的审计系统对远程访问的用户行为进行了审计 ，审计系统对访问互联网的行为进行了单独的审计
可信验证	可甚于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	边界设备可能包括网闸、 防火墙、交换机、路由器或其他边界防护设备等，通过设备的启动过程和运行过程中对预装软件 （包括系统引导程序、系统程序、 相关应用程序和重要配置参数 ）的完整性验证或检测， 确保对系统引导程序、 系统程序、 重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1) 应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证 2) 应核查是否应用程序的关键执行环节进行动态可信验证 3) 应测试验证当检测到设备的可信性受到破坏后是否进行报警 4) 应测试验证结果是否以审计记录形式送至安全管理中心 (3.6)	1) 边界设备（网闸、防火墙、交换机、路由器或其他边界防护设备） 具有可信根芯片或硬件 2) 启动过程基于可信根对系统引导程序、 系统程序、 重要配置参数和关键应用程序等进行可信验证度量 3) 在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结果记录 (3.6)

四、安全计算环境测评指导书

4.1 网络设备测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据

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	一般来说，用户登录路由器的方式包话：利用控制台端口 (Console) 通过串口进行本地登录连接。利用辅助端口 (AUX) 通过 Modem进行远程拨号连接登录或者利用虚拟终端（VTY）通过TCP/IP网络进行TelnetT 登录等。无论是哪一种登录方式，都需要对用户身份进行鉴别，口令是路由器用来防止非受权访问的常用手段，是路由器本身安全的一部分，因此需要加强对路由器口令的管理，包括口令的设置和存储，最好的口令存储方法是保存在TACACS或 RADIUS认证服务器上。管理员应当依据需要为路由器相应的端口加上身份签别最基本的安全控制。 路由器不允许配置用户名相同的用户，同时要防止多人共用一个账户，实行分账户管理，每名管理员设置一个单独的账户，避免出现问题后不能及时进行追查。 为避免身份鉴别信息被冒用，可以通过采用今牌、 认证服务器等措施，加强身份鉴别信息的保护。如果仅仅基于口令的身份鉴别，应当保证	1) 应核查用户在登录时是否采用了身份签别措施 2) 应核查用户列表，测试用户身份标识是否具有唯一性 以华为路由器为例，输入“ display current-configuration" 命令 3) 应核查用户配置信息或访谈系统管理员，核查是否不存在空口令用户 4) 应核查用户鉴别信息是否具有复杂度要求并定期更换	1、 a、路由器使用口令鉴别机制对登录用户进行身份标识和鉴别 b、登录时提示输入用户名和口令 ：以错误口令或空口令登录时提示登录失败， 验证了登录控制功能的有效性 C、路由器中不存在密码为空的用户 2、 Cisco: 输入 show run 命令，存在如下类似用户列表配置 ： username admin privilege 15 password 0 xxxxxxxxx username audit privilege 10 password 0 xxxxxxxxx 或启用 AAA服务器进行身份认证 aaa new-model aaa authentication login default group tacacs+ local enable aaa authentication enable default group tacacs+ enable 华为/H3C: 输入 display current-configuration 命令，存在如下类似用户列表配置 ： local-user netadmin password irreversible-cipher xxxxxx 或启用 AAA服务器进行身份认证

		口令复杂度和定期更改的要求。 使用“service password-encryption"命令对存储在配置文件中的所有口令和类似数据进行加密，避免通过读取配置文件而获取口令的明文		hwtacacs scheme xxxxx primary authentication xxxxx primary authorization xxxxx primary accounting xxxxx key authentication cipher xxxxx key authorization cipher xxxxx key accounting cipher xxxxx 3、 Cisco：输入 show run 命令，存在如下类似配置： username admin privilege 15 password 0 xxxxxxxxx usermame audit privilege 10 password 0 xxxxxxxxx 华为/H3C：输入 diplay current-configuration 命令，查看是否存在如下类似配置： local-user netadmin password irreversible-cipherxxxxx 4、 口今组成：应由数字、字母、特殊字符组成 口今长度：应大于 8 位 口令更换周期：口今一般三个月换一次 H3C:输入 display password-control，查看是否存在如下配置：

				password-control aging 90 password-control length 8 password-control history 10 password-control composition type-number 3 type-length 4 H3C:输入 diplay password-control 命令, 查看是否存在如下配置 : password-control aging 90 password-control length 8 password-control history 10 password-control composition type-number 3 type length 4

	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	可以通过配置结束会话、限制管理员的最大登录失败次数、网络连接超时自动退出等多种措施实现登录失败处理功能。例如，可以利用“ exec-timeout" 命令 . 配置 VTY 的超时。避免一个空闲的任务一直占用 VTY, 从而避免恶意的攻击或远端系统的意外崩溃导致的资源独占。 设置管理员最大登录失败次数，一旦该管理员的登录失败次数超过设定数值， 系统将对其进行登录锁定，从而防止非法用户通过暴力破解的方式登录到路由器	1) 应核查是否配置并启用了登录失败处理功能 ：如果网络中部署堡垒主机，先核查堡垒主机是否具有登录失败处理功能， 如果没有部署堡垒主机， 则设置默认登录失败 3 次，退出登录界面 2) 应核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能 3) 应核查是否配置并启用了远程登录连接超时并自动退出功能 以华为路由器为例， 设置超时时间为 5 分钟，输入 "display current-configuration ”命令，在 VTY 下查看是否存在如下类似配置 ： line vty 0 4 access-list 101 in transport input ssh idle-timeout 5	1. 网络设备默认启用登录失败处理功能。 2. 堡垒机设置限制非法登录达到一定次数后实现账户锁定功能或 a、H3C:输入 display password-control 存在如下配置 ： password-control login-attempt 3 exceed locktime 360 b、 Cisco 华为路由器连续 d 登录 5 次锁定 10 分钟 3、堡垒机启用选程登录连接超时并自动退出功能 或 Ciso 路由器 : 输入 show run 命令，存在如下类似配置 ： exec-timcout 20 华为 /H3C 路由器： 输入 display current-configuration 命令 , 存在如下类似配置 idle-timeout 20

	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听	当对网络设备进行远程管理时，为避免口令传输过程中别窃取，不应当使用明文传送的 Telnet 服务，而应当采用 SSH ITTPS 等加密协议等方式进行交互式管理	应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听。如果网络中部署堡垒主机，先核查堡垒主机采用何种措施在进行远程登录时，防止鉴别信息在网络传输过程中被窃听， 如 SSH 等方式	Cisco ：输入 show run 命令， 存在如下类似配置 ： Router1#configure terminal Router1(config)#hostname Router1 Router1(config #ip domain name neoshi.net netRouterl(config)#crypto key generate rsa ..... How many bits in the modulus [512] :1024 Router1(config)#ip ssh time-out 120 Router1(config)#ip ssh authentcation-retries4 Router1(config)#line vty 04 Router1(config)#transport input sh 华为 H3C: 输入 diSplay curent-configuration 命令，存在如下类似配置 : local-user test password cipher 456%&ET service-type ssh level 3 ssh user test authentication type password User-interface vty 0 4 Protocol inbound ssh

	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	采用双因子鉴别是防止欺骗的有效方法，双因子鉴别不仅要求访问者知道一些鉴别信息，还需要访问者拥有鉴别特征， 例如采用令牌、 智能卡等	应核查系统是否采用口令、 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身份进行鉴别	除口令之外，采用了另外一种鉴别机制，此机制采用了密码技术， 如调用了密码机或采取 SM1- SM4 等算法
访问控制	a) 应对登录的用户分配账户和权限	为了确保交换机的安全，需要对登录的用户分配账户，并合理配置账户权限。 例如，相关管理人员具有与职位相对应的账户和权限	1) 应访谈网络管理员、 安全管理员、 系统管理员或核查用户账户和权限设置情况 2) 应核查是否已禁用或限制匿名、默认账户的访问权限	1、相关管理人员具有与职位相对应的账户和权限 2、网络设备中已禁用或限制匿名、默认账户的访问权限
	b) 应重命名或删除默认账户，修改默认账户的默伙口令	对于路由器的默认账户，由于他们的某些权限与实际要求可能存在差异，从而造成安全隐患， 因此这些默认账户应被禁用，并且应不存在默认账户 admin.huawei 及默认口令	1) 应核查是否已经重命名默认账户或默认账户已被删除 2) 应核查是否已修改默认账户的默认口令 登录交换机，使用交换机默认账户和默认口令进行登录测试， 看能否成功 ：思科：账户： cisco 、 Cisco，口令：cisco ; 华为：账户 admin. huawei， 口令：admin 、admin@huawei.com	1、使用默认账户和默认口令无法登录路由器 2、 Cisco 路由器不存在默认账户 cisco. Cisco 华为 H3C 交换机不存在默认账户 admin, huawei

	c) 应及时删除或停用多余的、 过期的账户，避免共享账户的存在	路由器中如果存在多余的、过期的账户，可能会被攻击者利用其进行非法操作的风险，因此应及时清理路由器中的账户，删除或停用多余的账户	1）应核查是否不存在多余的或过期的账户，管理员用户与账户之间是否一一对应 2) 应核查并测试多余的、过期的账户是否被删除或停用 思科 : 输入 show run 命令，查看每条如下类似命令所配置的用户名是否确实必要： username XXXXXXXX privilege xx password XXXXXXXX 华为/H3C: 输入 display current-configuration 命令，查看每条如下类似命令所配置的用户名是否确实必要： local-user xxxxx privilege level x	1、Ciso: 输入 show run 命令，查看每条如下类似命令所配置的用户名是否确实必要： username XXXXXXXX privilege xx password XXXXXXXX 华为/H3C: 输入 display current-configuration 命令，查看每条如下类似命令所配置的用户名是否确实必要： local-user xxxxx privilege level x 或 local-user xxxxx password privilege xxxxxxx service type xxxxx level x 2、网络管理员、安全管理员和系统管理员不同用户采用不同账户登录系统

	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限。 例如，进行角色划分， 分为网络管理员、安全管理员、 系统管理员三个角色，并设置对应的权限	1) 应核查是否进行角色划分，如划分为网络管理员， 安全管理员、 系统管理员等角色 2) 应核查访问控制策略，查看管理用户的权限是否已进行分离 3) 应核查管理用中权限是否为其工作任务所需的最小权	1、访谈管理员，进行角色划分，分为网络管理员， 安全管理员、 系统管理员三个角色，并设置对应的权限 2、Cisco 路由器：输 show run 命令，存在如下类似配置 ： username admin privilege 15 password 0 xxxxxxxx usermame audit privilege 10 password 0 xxxxxxxx username operator privilege 7 password 0xxxxxxxx 华为/H3C 交换机；输入 display current-configuration 命令，存在如下类似配置 ： local-user userl service-type telnet user privilede level 2 # local-user user2 service-type ftp user privilede level 3 3. 网络管理员、 安全管理员、 系统管理员对应的账户为其工作任务所需的最小权限

	d) 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	访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作，访问控制粒度要求主体为用户级或进程级， 客体为文件、 数据库表级	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	此项不适合， 条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户
	e) 访问控制的粒度应达到主体为用户级或进程级， 客体为文件、数据库表级	访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作、访问控制粒度要求主体为用户级或进程级， 客体为文件、 数据库表统，	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	此项不适合， 条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户
	f) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	敏感标记是强制访问控制的依据，主客体都有 ，它存在的形式无所谓，可能是整形的数字， 也可能是字母，总之它表示主客体的安全级别。敏感标记由安全管理员进行设置，通过对重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作，实现强制访问控制。	此项不适合	此项不适合

安全审计	a) 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	为了对网络设备的运行状况、网络流量、管理记录等进行检测和记录，需要启用系统日志功能。系统日志中的每个信息都被分配了一个严重级别，并伴随一些指示性问题或事件的描述信息。 交换机的系统日志信息通常输出至各种管理端口、内部缓存或者日志服务器，在缺省情况下，控制台端口上的日志功能处于启用状态	1）应核查是否开启了安全审计功能； 网络设备设置日志服务器 IP 地址，并使用 syslog 方式或者 SMP方式将日志发送到日志服务器 2) 应核查安全审计范围是否覆盖到每个用户 3) 应核查是否对重要的用户行为和重要安全事件进行审计	Cisco: 网络设备设置日志服务器， 并使用 syslog 方式或者 SMP方式将日志发送到日志服务器， 通过输入 'show run ”命令，存在如下类似配置： logging on logging trap debugging logging facility local6 logging x.x.x.x Service timestamps log datetime 华为 /H3C: 网络设备设置日志服务器，并使用 Syslog 方式或者 SNMP方式将日志发送到日志服务器， 通过输入”display current-configuration “命令，存在如下类似配置： Info-center enable Info-center loghost source vlan-interface 3 Info-center loghost 192.10.12.1 facility local 1 Info-center source default channel 2 log level warning Snmp-agent snmp-agent trap enable standard authentication

				snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
	b) 审计记录应包括事件的日期和时间，用户、事件类型， 事件是否成功及其他与审计相关的信息	对于交换机设备，日志审计内容需要记录时间、 类型、用户、事件类型、事件是否成功等相关信息	应核查审计记录信息是否包括事件的日期和时间、 用户、 事件类型、 事件是否成功及其他与审计相关的信息	日志信息中包含事件的日期和时间用户、事件类型、 事件是否成功及其他与审计相关的信息

	c) 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	审计记录能修帮助管理人员及时发现系统运行状况和网络攻击行为，因此需要对审计记录实施技术上和管理上的保护，历正未授权修改、删除和破坏	访谈审计记录的存储、备份和保护的措施，是否将交换机日志定时发送到日志服务器上等，并使用 syslog 方式或 SNMP方式将日志发送到日志服务器。 如果部署了日志服务器，登录日志服务器查看被测交换机的日志是否在收集的范围内	网络设备的日志信息定期转发至日志服务器，日志服务器上可查看到半年前的审计记录
	d) 应对审计进程进行保护，防止未经授权的中断	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容，非审计员的其他账户不能中断审计进程	应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护	非审计员的其他账户来不能中断审计进程
入侵防范	a) 应遵循最小安装的原则仅安装需要的组件和应用程序	遵循最小安装原则，仅安装需要的组件和应用程序，能够极大的降低遭受攻击的可能性。及时更新系统补丁，避免遭受由于系统漏洞带来的风险	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现

	b) 应关闭不需要的系统服务、默认共享和高危端口	关闭不需要的系统服务、 默认共享和高危端口，可以有效降低系统遭受攻击的可能性	1）应访谈系统管理员是否定期对系统服务进行梳理，关闭了非必要的系统服务和默认共享 2) 应核查是否不存在非必要的高危端口	Cisco: 输入 show run 命令。根据实际网络环境参考已经关闭不必要服务 : no service tcp-small-servers no service udp-smal-servers. no cdp run no cdp enable no ip finger no service finger no ip bootp server no ip source-route no ip proxy-arp no ip directed-broadcast no ip domain-lookup 华为/H3C: 输入 diplay current-configuration 命令，根据实际网络环境参考已经关闭不必要服务 , 例如： p http shutdown

	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	为了保证安全，需要对通过 VTY 访问网络设备的登录地址进行限制，避免未授权的访问，可以利用 ip access-class 限制访问 VTY 的 IP 地址范围。同时，由于 VTYs 的数目有一定的限制，当所有的 VTYs 用完，就不能再建立远程的网络连接了。这就有可能被利用进行 Dos（拒绝服务攻击）	应核查配置文件是否对终端接入范围进行限制。如果网络中部署堡垒主机应先核查堡垒机是否限制管理终端地址范围，同时核查网络设备上是否仅配置位垒机的远程管理地址，否则登录设备进行核查： Cisco 路由器和路由器：输入 show run 命令； 华为/H3C 路由器和路由器：输入 diplay current-configuration 命令	堡垒机限制终端接入范围。 或 Cisco 路由器存在加不类似配置： access permit 192.168.1.10 access-list 3 deny any log line vty 0 4 access-class 3 in 或 ip http auth local no access-list 10 access-list 10 permit 192.168.0.1 access-list 10 deny any ip http access-class 10 ip http server 华为/H3C: 检查配置信息中存在类似如下配置信息： acl number 2001 rule 10 permit source 10.1.100.0.0.0.255 user-interface vty 0 4 acl 2001 inbound authentication-mode scheme user privilege level 1

	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	本条款要求应用系统应对数据的有效性进行验证，主要验证那些通过人机接口（如程序的界面）输入或通过通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出错（如 SQL 注入攻击等），人而影响系统的正常使用甚至危害系统的安全	此项不适合，该项要求一般在应用层面上核查	此项不适合， 该项要求一般在应用层面上核查
	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	核查漏扫修补报告，管理员定期进行漏洞扫描。发现漏洞在经过充分测试评估后及时修补漏洞	1) 应进行漏洞扫描，核查是否不存在高风险漏洞 2) 应访谈系统管理员，核查是否在经过充分测试评估后及时修补漏洞	管理员定期进行漏洞扫描，发现漏洞，在经过充分测试评估后及时修补漏洞
	h) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警	要维护系统安全，必须进行主动监视，一般是在网络边界、核心等重要节点处部署 IDS. IPS 等系统，或在防火墙、 UTM房用入侵检测功能，以检查息是否发生了入侵和攻击	此项不适合，该项要求一般在入侵防护系统上实现	此项不适合， 该项要求一般在入侵防护系统上实现
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	无论是 Windows 主机还是 Linux 主机，都面临木马、蠕虫等病毒的破坏。因此一般的主机为防范病毒，均会安装反病毒软件，或者采用可信验证机制对系统程序、应用程序等进行可信执行验证	此项不适合，该项要求一般在服务器上实现	此项不适合， 该项要求一般在服务器上实现

可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	设备应作为通信设备或边界设备对待	1) 应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证 2) 应核查是否在应用程序的关键执行环节进行动态可信验证 3) 应测试验证当检测到设备的可信性受到破坏后是否进行报警 4) 应测试验证结果是否以审计记录的形式送至安全管理中心 参见 2.3 和 3.6 可信验证	1) 通信设备、交换机、路由器或其他通信设备、边界设备（网闸、防火墙、交换机、路由器或其他边界防护设备） 具有可信根芯片或硬件 2) 启动过程基于可信根对系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证度量 3) 在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结果记录 参见 2.3 和 3.6 可信验证

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	一般来说，用户登录交换机的方式包括：利用控制台端口（Console）通过串口进行本地登录连接。利用辅助端口（AUX）通过Modem进行远程拨号连接登录或者利用虚拟终端（VTY）通过TCP/IP网络进行TelnetT登录等。无论是哪一种登录方式，都需要对用户身份进行鉴别，口令是交换机用来防止非受权访问的常用手段，是交换机本身安全的一部分，因此需要加强对交换机口令的管理，包括口令的设置和存储，最好的口令存储方法是保存在TACACS或RADIUS认证服务器上。管理员应当依据需要为交换机相应的端口加上身份签别最基本的安全控制。 路由器不允许配置用户名相同的用户，同时要防止多人共用一个账户，实行分账户管理，每名管理员设置一个单独的账户，避免出现问题后不能及时进行追查。 为避免身份鉴别信息被冒用，可以通过采用令牌、认证服务器等措施，加强身份鉴别信息的保护。如果仅仅基于口令的身份鉴别，应当保证	1) 应核查用户在登录时是否采用了身份签别措施 2) 应核查用户列表，测试用户身份标识是否具有唯一性 以华为路由器为例，输入“display current-configuration"命令 3) 应核查用户配置信息或访谈系统管理员，核查是否不存在空口令用户 4) 应核查用户鉴别信息是否具有复杂度要求并定期更换	1、 a、交换机使用口令鉴别机制对登录用户进行身份标识和鉴别； b、登录时提示输入用户名和口令：以错误口令或空口令登录时提示登录失败，验证了登录控制功能的有效性 C、交换机中不存在密码为空的用户 2、 Cisco：输入show run命令，存在如下类似用户列表配置： username admin privilege 15 password 0 xxxxxxxxx username audit privilege 10 password 0 xxxxxxxxx 或启用AAA服务器进行身份认证 aaa new-model aaa authentication login default group tacacs+ local enable aaa authentication enable default group tacacs+ enable 华为/H3C：输入display current-configuration命令，存在如下类似用户列表配置： local-user netadmin password irreversible-cipher xxxxxx 或启用AAA服务器进行身份认证

		口令复杂度和定期更改的要求。 使用“service password-encryption"命令对存储在配置文件中的所有口令和类似数据进行加密，避免通过读取配置文件而获取口令的明文		hwtacacs scheme xxxxx primary authentication xxxxx primary authorization xxxxx primary accounting xxxxx key authentication cipher xxxxx key authorization cipher xxxxx key accounting cipher xxxxx 3、 Cisco：输入 show run 命令，存在如下类似配置： username admin privilege 15 password 0 xxxxxxxxx usermame audit privilege 10 password 0 xxxxxxxxx 华为/H3C：输入 diplay current-configuration 命令，查看是否存在如下类似配置： local-user netadmin password irreversible-cipherxxxxx 4、 口今组成：应由数字、字母、特殊字符组成 口今长度：应大于 8 位 口令更换周期：口今一般三个月换一次 H3C:输入 display password-control，查看是否存在如下配置：

				password-control aging 90 password-control length 8 password-control history 10 password-control composition type-number 3 type-length 4 H3C:输入 diplay password-control 命令, 查看是否存在如下配置 : password-control aging 90 password-control length 8 password-control history 10 password-control composition type-number 3 type length 4

	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	可以通过配置结束会话、限制管理员的最大登录失败次数、网络连接超时自动退出等多种措施实现登录失败处理功能。例如，可以利用“ exec-timeout" 命令 . 配置 VTY 的超时。避免一个空闲的任务一直占用 VTY, 从而避免恶意的攻击或远端系统的意外崩溃导致的资源独占。 设置管理员最大登录失败次数，一旦该管理员的登录失败次数超过设定数值， 系统将对其进行登录锁定, 从而防止非法用户通过暴力破解的方式登录到路由器	1) 应核查是否配置并启用了登录失败处理功能 ：如果网络中部署堡垒主机，先核查堡垒主机是否具有登录失败处理功能， 如果没有部署堡垒主机， 则设置默认登录失败 3 次，退出登录界面 2) 应核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能 3) 应核查是否配置并启用了远程登录连接超时并自动退出功能 以华为路由器为例， 设置超时时间为 5 分钟，输入 "display current-configuration ”命令，在 VTY 下查看是否存在如下类似配置 ： line vty 0 4 access-list 101 in transport input ssh idle-timeout 5	1. 网络设备默认启用登录失败处理功能。 2. 堡垒机设置限制非法登录达到一定次数后实现账户锁定功能或 a、H3C:输入 display password-control 存在如下配置 ： password-control login-attempt 3 exceed locktime 360 b、 Cisco 华为交换机连续 d 登录 5 次锁定 10 分钟 3、堡垒机启用选程登录连接超时并自动退出功能 或 Ciso 交换机 : 输入 show run 命令，存在如下类似配置 ： exec-timcout 20 华为 /H3C 交换机： 输入 display current-configuration 命令 , 存在如下类似配置 idle-timeout 20

	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听	当对网络设备进行远程管理时，为避免口令传输过程中别窃取，不应当使用明文传送的 Telnet 服务，而应当采用 SSH ITTPS 等加密协议等方式进行交互式管理	应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听。如果网络中部署堡垒主机，先核查堡垒主机采用何种措施在进行远程登录时，防止鉴别信息在网络传输过程中被窃听， 如 SSH 等方式	Cisco ：输入 show run 命令， 存在如下类似配置 ： Router1#configure terminal Router1(config)#hostname Router1 Router1(config #ip domain name neoshi.net netRouterl(config)#crypto key generate rsa ..... How many bits in the modulus [512] :1024 Router1(config)#ip ssh time-out 120 Router1(config)#ip ssh authentcation-retries4 Router1(config)#line vty 04 Router1(config)#transport input sh 华为 H3C: 输入 diSplay curent-configuration 命令，存在如下类似配置 : local-user test password cipher 456%&ET service-type ssh level 3 ssh user test authentication type password User-interface vty 0 4 Protocol inbound ssh

	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	采用双因子鉴别是防止欺骗的有效方法，双因子鉴别不仅要求访问者知道一些鉴别信息，还需要访问者拥有鉴别特征， 例如采用令牌、 智能卡等	应核查系统是否采用口令、 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身份进行鉴别	除口令之外，采用了另外一种鉴别机制，此机制采用了密码技术， 如调用了密码机或采取 SM1- SM4 等算法
访问控制	a) 应对登录的用户分配账户和权限	为了确保交换机的安全，需要对登录的用户分配账户，并合理配置账户权限。 例如，相关管理人员具有与职位相对应的账户和权限	1) 应访谈网络管理员、 安全管理员、 系统管理员或核查用户账户和权限设置情况 2) 应核查是否已禁用或限制匿名、默认账户的访问权限	1、相关管理人员具有与职位相对应的账户和权限 2、网络设备中已禁用或限制匿名、默认账户的访问权限
	b) 应重命名或删除默认账户，修改默认账户的默伙口令	对于交换机的默认账户，由于他们的某些权限与实际要求可能存在差异，从而造成安全隐患， 因此这些默认账户应被禁用，并且应不存在默认账户 admin.huawei 及默认口令	1) 应核查是否已经重命名默认账户或默认账户已被删除 2) 应核查是否已修改默认账户的默认口令 登录交换机，使用交换机默认账户和默认口令进行登录测试， 看能否成功 ：思科：账户： cisco 、 Cisco，口令：cisco ; 华为：账户 admin. huawei， 口令：admin 、admin@huawei.com	1、使用默认账户和默认口令无法登录交换机 2、 Cisco 路由器不存在默认账户 cisco. Cisco 华为 H3C 交换机不存在默认账户 admin, huawei

	c) 应及时删除或停用多余的、 过期的账户，避免共享账户的存在	交换机中如果存在多余的、过期的账户，可能会被攻击者利用其进行非法操作的风险，因此应及时清理交换机中的账户，删除或停用多余的账户	1）应核查是否不存在多余的或过期的账户，管理员用户与账户之间是否一一对应 2) 应核查并测试多余的、过期的账户是否被删除或停用 思科 : 输入 show run 命令，查看每条如下类似命令所配置的用户名是否确实必要： username XXXXXXXX privilege xx password XXXXXXXX 华为/H3C: 输入 display current-configuration 命令，查看每条如下类似命令所配置的用户名是否确实必要： local-user xxxxx privilege level x	1、Ciso: 输入 show run 命令，查看每条如下类似命令所配置的用户名是否确实必要： username XXXXXXXX privilege xx password XXXXXXXX 华为/H3C: 输入 display current-configuration 命令，查看每条如下类似命令所配置的用户名是否确实必要： local-user xxxxx privilege level x 或 local-user xxxxx password privilege xxxxxxx service type xxxxx level x 2、网络管理员、安全管理员和系统管理员不同用户采用不同账户登录系统

	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限。 例如，进行角色划分， 分为网络管理员、安全管理员、 系统管理员三个角色，并设置对应的权限	1) 应核查是否进行角色划分，如划分为网络管理员， 安全管理员、 系统管理员等角色 2) 应核查访问控制策略，查看管理用户的权限是否已进行分离 3) 应核查管理用中权限是否为其工作任务所需的最小权	1、访谈管理员，进行角色划分，分为网络管理员， 安全管理员、 系统管理员三个角色，并设置对应的权限 2、Cisco 路由器：输 show run 命令，存在如下类似配置 ： username admin privilege 15 password 0 xxxxxxxx usermame audit privilege 10 password 0 xxxxxxxx username operator privilege 7 password 0xxxxxxxx 华为/H3C 交换机；输入 display current-configuration 命令，存在如下类似配置 ： local-user userl service-type telnet user privilede level 2 # local-user user2 service-type ftp user privilede level 3 3. 网络管理员、 安全管理员、 系统管理员对应的账户为其工作任务所需的最小权限

	d) 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	访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作，访问控制粒度要求主体为用户级或进程级， 客体为文件、 数据库表级	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	此项不适合， 条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户
	e) 访问控制的粒度应达到主体为用户级或进程级， 客体为文件、数据库表级	访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作、访问控制粒度要求主体为用户级或进程级， 客体为文件、 数据库表统，	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	此项不适合， 条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户
	f) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	敏感标记是强制访问控制的依据，主客体都有 ，它存在的形式无所谓，可能是整形的数字， 也可能是字母，总之它表示主客体的安全级别。敏感标记由安全管理员进行设置，通过对重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作，实现强制访问控制。	此项不适合	此项不适合

安全审计	a) 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	为了对网络设备的运行状况、网络流量、管理记录等进行检测和记录，需要启用系统日志功能。系统日志中的每个信息都被分配了一个严重级别，并伴随一些指示性问题或事件的描述信息。 交换机的系统日志信息通常输出至各种管理端口、内部缓存或者日志服务器，在缺省情况下，控制台端口上的日志功能处于启用状态	1）应核查是否开启了安全审计功能； 网络设备设置日志服务器 IP 地址，并使用 syslog 方式或者 SMP方式将日志发送到日志服务器 2) 应核查安全审计范围是否覆盖到每个用户 3) 应核查是否对重要的用户行为和重要安全事件进行审计	Cisco: 网络设备设置日志服务器， 并使用 syslog 方式或者 SMP方式将日志发送到日志服务器， 通过输入 'show run ”命令，存在如下类似配置： logging on logging trap debugging logging facility local6 logging x.x.x.x Service timestamps log datetime 华为 /H3C: 网络设备设置日志服务器，并使用 Syslog 方式或者 SNMP方式将日志发送到日志服务器， 通过输入”display current-configuration “命令，存在如下类似配置： Info-center enable Info-center loghost source vlan-interface 3 Info-center loghost 192.10.12.1 facility local 1 Info-center source default channel 2 log level warning Snmp-agent snmp-agent trap enable standard authentication

				snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
	b) 审计记录应包括事件的日期和时间，用户、事件类型， 事件是否成功及其他与审计相关的信息	对于交换机设备，日志审计内容需要记录时间、 类型、用户、事件类型、事件是否成功等相关信息	应核查审计记录信息是否包括事件的日期和时间、 用户、 事件类型、 事件是否成功及其他与审计相关的信息	日志信息中包含事件的日期和时间用户、事件类型、 事件是否成功及其他与审计相关的信息

	c) 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	审计记录能修帮助管理人员及时发现系统运行状况和网络攻击行为，因此需要对审计记录实施技术上和管理上的保护，历正未授权修改、删除和破坏	访谈审计记录的存储、备份和保护的措施，是否将交换机日志定时发送到日志服务器上等，并使用 syslog 方式或 SNMP方式将日志发送到日志服务器。 如果部署了日志服务器，登录日志服务器查看被测交换机的日志是否在收集的范围内	网络设备的日志信息定期转发至日志服务器，日志服务器上可查看到半年前的审计记录
	d) 应对审计进程进行保护，防止未经授权的中断	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容，非审计员的其他账户不能中断审计进程	应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护	非审计员的其他账户来不能中断审计进程
入侵防范	a) 应遵循最小安装的原则仅安装需要的组件和应用程序	遵循最小安装原则，仅安装需要的组件和应用程序，能够极大的降低遭受攻击的可能性。及时更新系统补丁，避免遭受由于系统漏洞带来的风险	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现

	b) 应关闭不需要的系统服务、默认共享和高危端口	关闭不需要的系统服务、 默认共享和高危端口，可以有效降低系统遭受攻击的可能性	1）应访谈系统管理员是否定期对系统服务进行梳理，关闭了非必要的系统服务和默认共享 2) 应核查是否不存在非必要的高危端口	Cisco: 输入 show run 命令。根据实际网络环境参考已经关闭不必要服务 : no service tcp-small-servers no service udp-smal-servers. no cdp run no cdp enable no ip finger no service finger no ip bootp server no ip source-route no ip proxy-arp no ip directed-broadcast no ip domain-lookup 华为/H3C: 输入 diplay current-configuration 命令，根据实际网络环境参考已经关闭不必要服务 , 例如： p http shutdown

	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	为了保证安全，需要对通过 VTY 访问网络设备的登录地址进行限制，避免未授权的访问，可以利用 ip access-class 限制访问 VTY 的 IP 地址范围。同时，由于 VTYs 的数目有一定的限制，当所有的 VTYs 用完，就不能再建立远程的网络连接了。这就有可能被利用进行 Dos（拒绝服务攻击）	应核查配置文件是否对终端接入范围进行限制。如果网络中部署堡垒主机应先核查堡垒机是否限制管理终端地址范围，同时核查网络设备上是否仅配置位垒机的远程管理地址，否则登录设备进行核查： Cisco 路由器和路由器：输入 show run 命令； 华为/H3C 路由器和路由器：输入 diplay current-configuration 命令	堡垒机限制终端接入范围。 或 Cisco 交换机存在加不类似配置： access permit 192.168.1.10 access-list 3 deny any log line vty 0 4 access-class 3 in 或 ip http auth local no access-list 10 access-list 10 permit 192.168.0.1 access-list 10 deny any ip http access-class 10 ip http server 华为/H3C: 检查配置信息中存在类似如下配置信息： acl number 2001 rule 10 permit source 10.1.100.0.0.0.255 user-interface vty 0 4 acl 2001 inbound authentication-mode scheme user privilege level 1

	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	本条款要求应用系统应对数据的有效性进行验证，主要验证那些通过人机接口（如程序的界面）输入或通过通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出错（如 SQL 注入攻击等），人而影响系统的正常使用甚至危害系统的安全	此项不适合，该项要求一般在应用层面上核查	此项不适合， 该项要求一般在应用层面上核查
	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	核查漏扫修补报告，管理员定期进行漏洞扫描。发现漏洞在经过充分测试评估后及时修补漏洞	1) 应进行漏洞扫描，核查是否不存在高风险漏洞 2) 应访谈系统管理员，核查是否在经过充分测试评估后及时修补漏洞	管理员定期进行漏洞扫描，发现漏洞，在经过充分测试评估后及时修补漏洞
	h) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警	要维护系统安全，必须进行主动监视，一般是在网络边界、核心等重要节点处部署 IDS. IPS 等系统，或在防火墙、 UTM房用入侵检测功能，以检查息是否发生了入侵和攻击	此项不适合，该项要求一般在入侵防护系统上实现	此项不适合， 该项要求一般在入侵防护系统上实现
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	无论是 Windows 主机还是 Linux 主机，都面临木马、蠕虫等病毒的破坏。因此一般的主机为防范病毒，均会安装反病毒软件，或者采用可信验证机制对系统程序、应用程序等进行可信执行验证	此项不适合，该项要求一般在服务器上实现	此项不适合， 该项要求一般在服务器上实现

可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	设备应作为通信设备或边界设备对待	1) 应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证 2) 应核查是否在应用程序的关键执行环节进行动态可信验证 3) 应测试验证当检测到设备的可信性受到破坏后是否进行报警 4) 应测试验证结果是否以审计记录的形式送至安全管理中心 参见 2.3 和 3.6 可信验证	1) 通信设备、交换机、路由器或其他通信设备、边界设备（网闸、防火墙、交换机、路由器或其他边界防护设备） 具有可信根芯片或硬件 2) 启动过程基于可信根对系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证度量 3) 在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结果记录 参见 2.3 和 3.6 可信验证

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	为了安全起见，防火墙器只有经过授权的合法用户才能访问，一般来说，用户登录防火墙的方式包话 ：通过浏览器以 WEB 方式登录，通过 Console 口以命令行方式登录， 通过 SSH方式登录。防火墙为了便于用户管理，还提供了图形界面管理工具便于用户对设备进行管理和维护。 无论是采用哪一种的呢公路方式，都需要对用户身份进行鉴别。 防火墙不允许配置用户名相同的用户，同时要防止多人共用一个账户，实行分账户管理，每名管理员设置一个单独的账户，避免出现问题后不能及时进行追查。 同时为避免身份鉴别信息被冒用，应当保证口令复杂度和定期更改的要求	1) 以天融信防火墙为例，核查用户在登录时是否来用里身份鉴别措施。 通过浏览器以 WEB方式登录 打开 IE 浏览器， 在地址输入框中输入网络卫士防火墙的 URL地址，如 https://192.168 83.240 。回车后进入网络卫士防火墙的登录界面，如下图所示，提示用户输入用户名和密码 输入用户名和密码后， 点击 ” 登录 “ 按钮，即可登录到网络卫士防火墙。 登录后，用户就可通过 WEB界面对网络卫士防火墙进行配置管理 通过 console 口以命令行方式登录 ： 通过 consol 口成功连接到防火墙后，超级终端界面会出现输入用户名的提示，如下图所示： 输入用户名， 然后回车后， 提示用户输入密码，如下图所示： 1）输入密码后，回车，即可登录到网络卫士防火墙。 登录后，用户就可使用命令行方式对网络卫士防火墙进行配置管理。 2) 应核查防火墙管理员账户列表，测试用户身份标识是否具有唯一性，核查是否存在多人共用账户的情况，核查是否存在空口令用户。	1) 防火墙使用口令鉴别机制对登录用户进行身份标识和鉴别 2) 用户身份标识具有唯一性， 不存在多人共用账户的情况，不存在空口令用户 3) 口令长度 8 位以上， 由数字、 大小写字母和特殊字符中的两种以上组成， 口令每季度至少更改一次

			3) 应询问管理员对身份鉴别所采取的具体措施，确认口令长度是否 8 位以上，是否由数字、 大小写字母和特殊字符中的两种以上组成，口令是否每季度至少更改一次	

	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	可以通过配置结束会话、限制管理员的最大登录失败次数、网络连接超时自动退出等多种措施实现登录失败处理功能。 例如，设置管理员最大登录失败次数，一旦该管理员的登录失败次数超过设定数值，系统将对其进行登录锁定，从而防止非法用户通过暴力破解的方式登录到防火墙	1) 应核查是否配置并启用了登录失败处理功能，核查是否配置并启用了限制非法登录达到一定次数后实现账户锁定功能 2) 应核查是否配置并启用了远程登录连接超时并自动退出功能	以天融信防火墙为例， 通过浏览器以 WEB 方式登录。 1) 配置并启用了登录失败处理功能， 配置并启用了限制非法登录达到一定次数后实现账户锁定功能。 在登录界面中输入防火墙管理员的用户名/口令后，点击“登录”按钮，进入管理界面。然后在左侧导航树中选择系统管理>>配置，激活“系统参数”页签，如下图所示。 选中“高级属性” 左侧的复选框， 可以查看到“最大登录失败次数” 的配置， 如下图所示。 2) 配置并启用了远程登录连接超时并自动退出功能。 在登录界面中输入防火墙管理员的用户名/口令后，点击“登录”按钮，进入管理界面。然后在左侧导航树中选择系统管理>配置，激活“系统参数” 页签， 如下图所示： 选中“高级属性” 左侧的复选框， 可以查看到“远程登录连接超时” 的配置， 如下图所示
	c) 当进行远程管理时，应采取必要措施、	为避免口令传输过程中别窃取，不应当使用明文传送的 Telnet 、HTTP	应询问系统管理员采用何种方式对防火墙进行远程管理 ，核查通过 WEB 界面	通过 WEB 界面进行远程管理时， 通过 SSL 协议进行加密处理

	防止鉴别信息在网络传输过程中被窃听	服务，而应当采用 SSH、ITTPS 等加密协议等方式进行交互式管理	管理是否都通过 SSL 协议进行加密处理	
	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	采用双因子鉴别是防止欺骗的有效方法，双因子鉴别不仅要求访问者知道一些鉴别信息，还需要访问者拥有鉴别特征，例如采用令牌、智能卡等．目前主流防火墙多采用“本地口令 +证书认证”的方式进行认证。“本地口令 +证书认证”认证时，用户既要通过防火墙内部认证服务器的口令认证，也要通过证书认证才能够成功登录防火墙	以天融信防火墙为例，通过浏览器以WEB方式登录。 1) 在登录界面中输入防火墙管理员的用户名口令后，点击“登录”按钮，进入管理界面。然后在左侧导航树中选择用户认证 >>用户管理 ，激活“用户管理”页签，如下图所示。 2）右侧显示用户列表信息，如下图所示： 3) 如果需要对用户进行两种或两种以上组合的鉴别技术，点击该用户条目右侧的“修改”图标，查看该用户的认证方式应该为“本地口令 +证书认证”或者“外部口令 +证书认证”。 例如，管理员希望对用户“doc”同时进行证书认证和外部服务器的口令认证，则点击用户“doc”条目右侧的“修改”图标后，用户属性的“认证方式”应该为“外部口令 +证书认证”，如下图所示。	以天融信防火墙为例，通过浏览器以 WEB 方式登录。 查看该用户的认证方式应该为“本地口令 +证书认证”或者“外部口令 +证书认证”。 例如，管理员希望对用户“doc”同时进行证书认证和外部服务器的口令认证，则点击用户“doc”条目右侧的“修改”图标后，用户属性的“认证方式”应该为“外部口令 +证书认证”，如下图所示

访问控制	a) 应对登录的用户分配账户和权限	为了确保防火墙的安全，需要对登录的用户分配账户，并合理配置账户权限	以天融信防火墙为例，在登录界面中输入防火墙管理员的用户名口令后，点击“登录”按钮，进入管理界面。 然后在左侧导航树中选择用户认证 >>用户管理，激活“用户管理”页签，右侧显示用户列表信息，如下图所示。 1) 应针对每一个用户账户，核查用户账启和权限设置情况是否合理，如账户管理员和配置管理员不应具有审计员权限。 2) 应核查是否已禁用或限制匿名、默认账户的访问权限	1、相关管理人员具有与职位相对应的账户和权限 2、禁用或限制匿名、默认账户的访问权限
	b) 应重命名或删除默认账户，修改默认账户的默伙口令	对于防火墙的默认账户，由于他们的某些权限与实际要求可能存在差异，从而造成安全隐患， 因此这些默认账户应被禁用	以天融信防火墙为例，在登录界面中输入防火墙管理员的用户名口令后，点击“登录”按钮，进入管理界面。 然后在左侧导航树中选择用户认证 >>用户管理，激活“用户管理”页签，右侧显示用户列表信息，如下图所示 1) 应核查是否重命名或删除这些默认账户 2) 应核查是否已修改默认账户的默伙口令	防火墙重命名或删除默认账户， 修改默认账户的默伙口令

	c) 应及时删除或停用多余的、 过期的账户，避免共享账户的存在	防火墙中如果存在多余的、过期的账户，可能会被攻击者利用其进行非法操作的风险，因此应及时清理路由器中的账户，删除或停用多余的账户	以天融信防火墙为例，在登录界面中输入防火墙管理员的用户名口令后，点击“ 登录 ” 按钮， 进入管理界面。 然后在左侧导航树中选择用户认证 >>用户管理 ，激活“ 用户管理 ”页签，右侧显示用户列表信息，如下图所示。 1) 应核查防火墙用户账户列表， 询问管理员各账户的具体用途，分析是否存在多余或过期账户，并核查管理员用户与账户之间是否一一对应。 2) 如果因为种种原因导致某些多余的、过期的账户无法被删除， 则应测试是否已经停用了这些多余的、过期的账户	防火墙用户账户列表不存在多余或过期账户，不存在共享用户
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限	以天融信防火墙为例，在登录界面中输入防火墙管理员的用户名口令后，点击“ 登录 ” 按钮， 进入管理界面。 然后在左侧导航树中选择用户认证 >>用户管理 ，激活“ 用户管理 ”页签，右侧显示用户列表信息，如下图所示 1) 应核查是否进行角色划分，系统中的账户分为系统管理员、安全管理员和审计管理员三类 ，其中， 安全管理员可以制定安全策略，系统管理员可以配置安全策略，审计管理员可以查看日志	1) 系统用户进行角色划分， 系统中的账户分为系统管理员、 安全管理员和审计管理员三类。 其中， 安全管理员可以制定安全策略， 系统管理员可以配置安全策略， 审计管理员可以查看日志 2) 管理用户的权限进行了分离， 并为其工作任务所费的最小权限， 如禁上对管理用户同时赋予配置管理员和审计管理员权限

			2) 应查看管理用户的权限是否已进行分离，是否为其工作任务所需的最小权限，如禁止对管理用户同时赋予配置管理员和审计管理员权限	
	d) 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	访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作，访问控制粒度要求主体为用户级或进程级， 客体为文件、 数据库表级	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	此项不适合， 条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户
	e) 访问控制的粒度应达到主体为用户级或进程级， 客体为文件、数据库表级	访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作、访问控制粒度要求主体为用户级或进程级， 客体为文件、 数据库表统	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	此项不适合， 条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户

	f) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	敏感标记是强制访问控制的依据，主客体都有 ，它存在的形式无所谓，可能是整形的数字， 也可能是字母，总之它表示主客体的安全级别。敏感标记由安全管理员进行设置，通过对重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作，实现强制访问控制	此项不适合，该项要求一般在服务器上实现	此项不适合， 该项要求一般在服务器上实现
安全审计	a) 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	为了对防火墙的运行状况、网络流量、管理记录等进行检测和记录， 需要启用系统日志功能。系统日志中的每个信息都被分配了一个严重级别，并伴随一些指示性问题或事件的描述信息。 防火墙的系统日志信息通常输出至各种管理端口、内部缓存或者日志服务器，在缺省情况下， 控制台端口上的日志功能处于启用状态	以天融信防火墙为例，在登录界面中输入防火墙管理员的用户名口令后，点击“ 登录 ” 按钮， 进入管理界面。 然后在左侧导航树中选择日志与报警 >> 日志设置 ，激活“ 用户管理 ”页签，右侧显示用户列表信息，如下图所示 在右侧显示 “ 日志设置 ” 页面， 设置正确的服务器地址、 端口、以及日志级别和日志类型等信息。 例如，如果希望记录 0-3 级的阻断策略日志，则“ 日志级别右侧的下拉框中应该设置为“ 3 ”，并且勾选了 “ 阻断策略 ” 的日志类型，如下图所示	防火墙设置正确的服务器地址、 端口、 以及日志级别和日志类型等信息

	b) 审计记录应包括事件的日期和时间，用户、事件类型， 事件是否成功及其他与审计相关的信息	对于防火墙来说，审计内容应包括时间、 类型、 用户、 事件类型、 事件是否成功等相关信息	以天融信防火墙为例，在登录界面中输入防火墙管理员的用户名口令后，点击“ 登录 ” 按钮， 进入管理界面。 然后在左侧导航树中选择日志与报警 >> 日志设置 ，激活“ 用户管理 ”页签，右侧显示用户列表信息，如下图所示。 登录日志服务器， 并选择管理策略》 日志收集源， 进入日志源配置界面， 查看所有日志收集源。确保日志源列表中包含了该防火墙的 IP 。 在日志服务器上，选择功能 >>日志查询并选择“ 审计域 ”页签。根据 IP 地址选择防火墙后，便可对该防火墙的日志进行核查，确认是否包括日期和时间、 用户、 事件类型、 事件是否成功等相关的信息	审计记录包括事件的日期和时间、 用户事件类型、事件是否成功及其他与审计相关的信息。

	c) 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	审计记录能修帮助管理人员及时发现系统运行状况和网络攻击行为，因此需要对审计记录实施技术上和管理上的保护，防止未授权修改、删除和破坏	以天融信防火墙为例，在登录界面中输入防火墙管理员的用户名口令后，点击“登录”按钮，进入管理界面。然后在左侧导航树中选择日志与报警 >> 日志设置，激活“用户管理”页签，右侧显示用户列表信息，如下图所示 登录日志服务器，并选择管理策略》日志收集源，进入日志源配置界面，查看所有日志收集源。确保日志源列表中包含了该防火墙的 IP。 收集到的日志数据会保存在日志系统的数据库中，通过对数据库进行备份操作，便可实现防火墙数据的备份和保护。 在日志服务器上，选择管理策略》》任务调度策略，然后在左侧“本地配置”分页中点击“任务调度策略”，确保存在类型为“备份数据库任务”的计划任务。这些任务会定时执行数据库的备份任务，进而达到备份防火墙日志信息的目的	防火墙日志信息定期转发至日志服务器，日志服务器上可查看到半年前的审计记录
	d) 应对审计进程进行保护，防止未经授权的中断	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容	应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护	非审计员的其他账户来不能中断审计进程，验证审计进程是否得到保护

入侵防范	a) 应遵循最小安装的原则仅安装需要的组件和应用程序	遵循最小安装原则，仅安装需要的组件和应用程序，能够极大的降低遭受攻击的可能性。及时更新系统补丁，避免遭受由于系统漏洞带来的风险	此项不适合，该项要求一般在服务器上实现	此项不适合， 该项要求一般在服务器上实现
	b) 应关闭不需要的系统服务、默认共享和高危端口	关闭不需要的系统服务、 默认共享和高危端口，可以有效降低系统遭受攻击的可能性	此项不适合，该项要求一般在服务器上实现	此项不适合， 该项要求一般在服务器上实现
	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	为了保证安全， 避免未授权的访问，需要对远程管理防火墙的登录地址进行限制， 可以是某一特定的 IP 地址，也可以来自某一子网、 地址范围或地址组	如果网络中部署堡垒机的，先核查堡垒机是否限制终端接入范围进行限制，如果没有，登录设备进行核查。以天融信防火墙为例，在登录界面中输入防火墙管理员的用户名密码后，点击“ 登录 ” 按钮， 进入管理界面。 然后在左侧导航树中选择系统管理》配置，然后激活 “ 开放服务 ” 页签， 如下图所示。 在右侧页面中，应该存在“ 服务名称 " 为“ webui ”, "ssh" 或"telnet' 的服务规则。例如，只允许管理员使用 IP 地址为“ 192. 168. 83.234" 的主机登录防火墙， 并且该主机连接在 area_eth0 区域，则应该配置的服务规则如下图所示 ： 图中， “ 控制地址 ” 一列显示为 "doc. server", 是已经配置完成的主机地址	堡垒机限制终端接入范围或在设备本地设置访问控制列表限制终端接入范围。

			资源名称，定义了主机地址“ 192. 168. 83. 234 ”。可以通过点击左侧导航树中选择资源管理 >>地址，然后激活“ 主机 ” 页签， 查看主机资源名称和实际地址的对应关系，如下围所示	
	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	本条款要求应用系统应对数据的有效性进行验证，主要验证那些通过人机接口（如程序的界面）输入或通过通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出错（如 SQL 注入攻击等），人而影响系统的正常使用甚至危害系统的安全	此项不适合，该项要求一般在应用层面上核查	此项不适合， 该项要求一般在应用层面上核查

	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	核查漏扫修补报告，管理员定期进行漏洞扫描。发现漏洞在经过充分测试评估后及时修补漏洞	1) 应进行漏洞扫描，核查是否不存在高风险漏洞 2) 应访谈系统管理员，核查是否在经过充分测试评估后及时修补漏洞	管理员定期进行漏洞扫描，发现漏洞，在经过充分测试评估后及时修补漏洞
	h) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警	要维护系统安全，必须进行主动监视，一般是在网络边界、核心等重要节点处部署 IDS. IPS 等系统，或在防火墙、UTM房用入侵检测功能，以检查息是否发生了入侵和攻击	1) 应核查防火墙是否有入侵检测功能，查看入侵检测功能是否正确启用 2) 应核查在发生严重入侵事件时是否提供报警，报警方式般包括短信、邮件等	1) 防火墙启用入侵检测功能 2) 在发生严重入侵事件时提供短信、邮件等方式报警
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	无论是 Windows 主机还是 Linux 主机，都面临木马、蠕虫等病毒的破坏。因此一般的主机为防范病毒，均会安装反病毒软件，或者采用可信验证机制对系统程序、应用程序等进行可信执行验证	此项不适合，该项要求一般在服务器上实现	此项不适合，该项要求一般在服务器上实现
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形	设备应作为通信设备或边界设备对待	1) 应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证 2) 应核查是否在应用程序的关键执行环节进行动态可信验证 3) 应测试验证当检测到设备的可信性受到破坏后是否进行报警 4) 应测试验证结果是否以审计记录的形式送至安全管理中心 参见 2.3 和 3.6 可信验证	1) 通信设备、交换机、路由器或其他通信设备、边界设备（网闸、防火墙、交换机、路由器或其他边界防护设备）具有可信根芯片或硬件 2) 启动过程基于可信根对系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证度量 3) 在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结

	成审计记录送至安全管理中心			果记录 参见 2.3 和 3.6 可信验证

4.2 Linux 测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据

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	Linux 系或統的用户鉴别过程与其他 UNIX 系統相同：系统管理员为用户建立一个账户并为其指定一个口令 ，用户使用指定的口今登录后重新配置自己的自已的口令，这样用户就具备一个私有口令。 etc/password 文件中记录用户的属性信息，包括用户名、密码、用户标识、组标识等信息。现在 Linux 系统中不再直接保存在 /etc/password 文件中，通常将 password 文件中的口令字段使用一个“ x ”来代替，将 /etc/shadow 作为真正的口令文件，用于保存包括个人口令在内的数据。当然， shadow 文件是不能被普通用户读取的，只有超级用户才有权读取。 Linux 中的 /etc/login.defs 是登录程序的配置文件，在这里我们可配置密码的最大过期天数，密码的最大长度约束等内容。如果 /etc/pam.d/system-auth 文件里有相同的选项，则以 /etc/pam.d/system-auth 里的设置为准，也就是说 /etc/pam.d/system-aut 的配置优先级高于 /etc/login.defs 。 Linux 系统具有调用 PAM的应用程度认	1) 访谈系统管理员系统用户是否已设置密码， 并查看登录过程中系统账户是否使用了密码进行验证登录。 2) 以有权限的账户身份登录操作系统后，使用命令 more 查看 /etc/shadow 文件，核查系统是否存在空口令账户 3) 使用命令 more 查看 /etc/login. defs 文件，查看是否设置密码长度和定期更换要求 #more /etc/login. defs 使用命令 more 查看 /etc/pam.d/system-auth 文件。查看密码长度和复杂度要求 4) 检查是否存在旁路或身份鉴别措施可绕过的安全风险	1) 登录需要密码 2) 不存在空口令账户 3) 得出类似反馈信息，如下 ： PASS MAX_DAYS90 #登录密码有效期 90 天 PASS MIN_DAYS 0 #登录密码最短修改时间，增加可以防止非法用户短期更改多次 PASS MIN_LEN 7 #登录密码最小长度 7 位 PASS WARN_AGE 7 #登录密码过期提前 7 天提示修改 4) 不存在绕过的安全风险

		证用户。登示服务、屏保等功能，其中一个重要的文件使是 etc/pam.d/system-auth(在 Kedhat Cent0s 和 Fedora 系上）。/etc/pam.d/system-auth 或 /etc/login.defs 中的配置优先级高于其他地方的配置。 另外，root 用户不受 pam 认证规则的限制，相关配置不会影响 root 用户的密码，root 用户可以随意设置密码的。login.defs 文件也是对 root 用户无效的。		

	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	Linux 系统具有调用 PAM的应用程度认证用户、 登录服务、 屏保等功能， 其中一 个 重 要 的 文 件 便 /etc/pam.d/system-auth ， Redhat5 以后版本使用 pam_tally2.so 模块控制用户密码认证失败的次数上限，可以实现登录次数、 超时时间， 解锁时间等。 着只是针对某个程序的认证规则，在 PAM目录 (/etc/pam d) 下形如 sshd、login 等等的对应各程序的认证规则文件中进行修改。若所有密码认证均应用规则， 可直接修改 system_auth 文件	1) 系统配置并启用了登录失败处理功能 2) 以 root 身份登录进入 Linux ，查看文件内容 ： # cat /ete/pam.d/system -auth 或根据 linux 版本不同在 common 文件中 3) 查 看 /etc/profile 中 的 TIMEOUT环境变量，是否配置超时锁定参数	得出类似反馈信息，如下 ： 1) 和 2) 查看登录失败处理功能相关参数， /etc/pam.d/system — auth 文件中存 在 "account required /lib/security/pam_tally.so deny=3 no_ magic root reset" ; 3) 记录在文件 /etc/profile 中设置了超时锁定参数，在 profile 下设置 TMOUT= 300s

	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听	Linux 提供了远程访问与管理的接口，以方便管理员进行管理操作，网络登录的方式也是多样的，例如可以使用 Telnet 登录，也可以使用 SSH登录。但是， Telnet 不安全。 I 因为其在教据传输过程中，账户与密码均明文传输，这是非常危险的。黑客通过一些网络对嗅探工是能够轻易地的窃取网络中明文传输的账户与密码，因此不建议通过 Telnet 协议对服务器进行远程管理。针对 Telnet 协议不安全这种情况，可以在远程登录时使用 SSH协议。其原理跟 Telnet 类似，只是其具有更高的安全性。 SSH是一个运行在传输控制层上的应用程序，与 Telnet 相比，它提供了强大的认证与加密功能，可以保证在远程连接过程中，其传输的数据是加密处理过的。因此保障了账户与口令的安全	访谈系统管理员， 进行远程管理的方式。 1) 以 root 身份登录进入 Linux 查看是否运行了 sshd 服务，service - status-all | grep sshd 查看相关的端口是否打开，netstat -an|grep 22 若未使用 SSH方式进行远程管理，则查看是否使用了 Telnet 方式进行远程管理 service - -status-all|grep running， 查看是否存在 Telnet 服务 2) 可使用 wireshark 等抓包工具，查看协议是否为加密 3) 本地化管理， N/A	1) 使用 SSH方式进行远程管理， 防止鉴别信息在传输过程中被窃听 ,Telnet 默认不符合 2) 通过抓包工具， 截获信息为密文， 无法读取，协议为加密 3) N/A 本地管理
	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	对于第三级及以上的操作系统要求采用口令、 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	访谈和核查系统管理员在登录操作系统的过程中使用了哪些身份鉴别方法， 是否采用了两种或两种以上组合的鉴别技术， 如口令教字证书 Ukey、令牌、 指纹等， 是否有一种鉴别方法在鉴别过程中使用了密码技术	除口令之外，采用了另外一种鉴别机制，此机制采用了密码技术， 如调用了密码机或采取 SM1-SM4等算法

访问控制	a) 应对登录的用户分配账户和权限	对于 Linux 中一些重要的文件，应检查 Linux 系统主要目录的权限设置情况，Linux 系统对文件的操作权限，包括 4 种：读(r,4) ；写 (w,2) ；执行 (x,1) ；空(一，0)，文件的权限分为属主 (拥有者)、属组、其它用户和用户组的权限	以有相应权限的身份登录进入 Linux，使用“ 1s-1 文件名”命令，查看重要文件和目录权限设置是否合理，如：# 1s -1 /etc/passwd #744。	重点查看以下文件和目录权限是否设置合理。 —rwx- - - - -: 数字表示为 700 -rwxr--r- -: 数字表示为 744 -rw-rw-r-x: 数字表示为 665 drwx-x 一 x: 数字表示为 711 drwr- - - - -: 数字表示为 700 配置文件权限值不能大于 644，对于可执行文件不能大于 755
	b) 应重命名或删除默认账户，修改默认账户的默认口令	Linux 操作系统本身安装后提供各种账号，如 adm lp sync shutdown halt mail uucp operator games gopher ftp 等，但这些账户使用时并不需要，有的帐号越多，就越容易受到攻击，应禁用或者删除这些用户。 root 作为重要的默认账户，一般要求禁止远程登录	1) 以有相应权限的身份登录进入 Linux，使用 more 查看 /etc/shadow 文件，查看文件中的用户，是否存在 adm、lp. sync 、shutdown 、halt. 、mail 、uucp 、operator, 、games.、gopher ftp 等默认的、无用的用户。 2) 查看 root 账户是否能够进行远程登录	1) 不存在默认无用的账户 2) 使用 more 查看 /etc/ssh/sshd_config 文件中的 "PermitRootLogin" 参数设置为“ no “ ，即：PermitRootLogin no, 即不许可 root 远程登录
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在	通常操作系统在运行一段时间后，因业务应用或管理员岗位的调整，出现一些多余的、过期的账户；另一方面，也会出现多个系统管理员或用户使用同一账户登录操作系统的情况，造成审计追踪时无法定位到自然人。如果存在多余的，过期的账户，可能会被攻击者利用其进行非法操作的风险，因	1) 应核查是否不存在多余或过期账户，如查看 games、news、ftp 、1p 等系统默认账户是否被禁用，特权账号 halt 、shutdown 是否被删除 2) 应访谈网络管理员、安全管理员、系统管理员不同用户是否采用不同账户登录系统	1) 禁用或删除不需要的系统默认账户，如 games、news、ftp 、1p 、halt 、shutdown 等 2) 各类管理员均使用自己分配的特定权限账户登录，不存在多余、过期账户

		此应及时清理系统中的账户，删除或停用多余的、 过期的账户， 同时避免共享账户的存在		
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限。 Linux 系统安装后，root 拥有所有权限， 使用 sudo 授予普通用户 root 级权限，在 sudoer.conf 中进行配置	1) 以有相应权限的身份登录进入 Linux， 使用 more 查看 /etc/passwd 文件中的非默认用户，询问各账户的权限， 是否实现管理用户的权限分离 2) 以有相应权限的身份登录进入 Linux， 使用 more 查看 /etc/sudo.conf 文件，核查 root 级用户的权限都授予哪些账户	1) 各用户均具备最小权限 , 不与其他用户权限交叉。 设备下可支持新建多用户角色功能 2) 管理员权限仅分配 root 用户
	d) 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	操作系统的访问控制策略应由授权主体（如安全管理员） 进行配置， 非授权主体不得更改访问控制策略。访问控制策略规定操作系统用户对操作系统资源（如文件和目录 ）具有哪些权限，能进行哪些操作、通过在操作系统中配置访问控制策略，实现对操作系统各用户权限的限制	1) 访谈系统管理员， 是否指定授权人对操作系统访问控制权限进行配置 2) 核查账户权限配置， 是否依据安全策略配置各账户的访问规则	1) 由专门的安全员负责对访问控制权限的授权工作 2) 各账户权限配置， 均是基于安全员的安全策略配置进行的访问控制

	e) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	明确提出访问控制的粒度要求，重点目录的访问控制的主体可能为某个用户或某个进程，应能够控制用户或进程对文件、数据库表等客体的访问	使用“ ls -1 文件名”命令，查看重要文件和目录权限设置是否合理，如:#ls -1/etc/passwd #744，应重点查看以下文件和目录权限是否被修改过	由管理用户进行用户访问权限分配进行设置，依据访问控制策略 ，对各类文件和数据库表级进行访问。 重要文件和目录权限均在合理范围内， 用户可根据对文件不同的权限进行操作
	f) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	敏感标记是由强认证为安全管理员进行设置的，通过对重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作， 实现强制访问控制。 安全增强型 Linux (Security Enhanced Linux) 简称 SELinux，是一个 Linux 内核模块，也是 Linux 的一个安全子系统。2.6 及以上版本的 Linux 内被都团经集成了 SELinux 模块，在使用 SELinux 的操作系统中， 决定一个资源是否能够被访问的因素除了用户的权限 (读、写、执行) 外，还需要判断每一类进程是否拥有对某一类资源的访问权限，这种权限管理机制的主体是进程，也称为强制访问控制 (MAC)。在 SELinux 中，主体等同于进程， 客体是主体访问的资源，可以是文件、目录、端口、设备等	1) 明确系统中是否有敏感信息 2) 在主体用户或进程划分级别并设置敏感标记， 在客体文件设置敏感标记 3) 应测试是否依据主体、 客体安全标记控制主体对客体访问的强制访问控制策略 4) 以有相应权限的身份登录进入 Linux， 使用 more 查看 /etc/selinux/config 文件中的 SELINUX参数的设定	1) 2) 3)4) linux 服务器默认关闭 SELinux 服务。 或采取第三方主机加固系统或对操作系统内核进行二次开发加固，并实际查看系统可视化界面。 SELINUX有三种工作模式，分别是 : enforcing: 强制模式。违反 SELinux 规则的行为将阻止并记录到日志中， 表示使用 SELinux 。 permissive: 宽容模式。违反 SELinux 规则的行为只会记录到日志中， 一般为调试用，表示使用 SELinux disabled: 关闭 SELinux，使用 SELinux

安全审计	a) 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	Redhat Enterprise Linux-3 update 2 以后都开始使用 LASU (Linux Aduit Subsystem) 来进行审计。且志系统可以记录系统的各种信息 , 如: 安全、调试、运行信息。 审计子系统专用来记录安全信息，用于对系统安全事件的追溯。如果审计子系统没有运行， Linux 内核就将安全审计信息传递给日志系统。 Linux 操作系统的 auditd 进程主要用来记录安全信息。用于对系统安全事件的追溯；而 rsyslog 进程用来记录系统中的各种信息，如硬件报警和软件日志。Linux 操作系统在安全审计配置文件 /etc/audit/audit.rules 中配置安全事件审计规则	1) 以 root 身份登录进入 Linux, 查看服务进程 2) 若运行了安全审计服务， 则查看安全审计的守护进程是否正常 # ps -ef|grep auditd 3) 若未开启系统安全审计功能， 则确认是否部署了第三方安全审计工具 4) 以 root 身份登录进入 Linux 查看安全事件配置 : #gerep “ @priv-ops" /etc/audit/filter.conf .... more/etc/audit/audit.rules	1) 开启审计进程内容如下 : [root@localhost april]# service auditd status auditd (pid 1656) is running... [root@localhost april]# service rsyslog statusr syslogd (pid 1681) is running... [root@localhost april]# 2)Linux 服务器默认开启守护进程 3)audit.rules 中记录对文件和底层调用的相关记录， 记录的安全事件较为全面
	b) 审计记录应包括事件的日期和时间， 用户、事件类型，事件是否成功及其他与审计相关的信息	详细的审计记录才能实现有效的审计，审计记录应该包括事件的日期、 时间、类型、主体标识、 客体标识和结果等。通过记录中的详细信息， 能够帮助管理员或其他相关检查人员准确的分析和定位事件。 Linux 用户空间审计系统由 auditd 、ausearch 和 aureport 等应用程序组成，其中 ausearch 是查找审计事件的工具，可以用来查看系统日志	以有相应权限的身份登录进入 Linux, 使用命令 "ausearch-ts today ”，其中， -ts 指定时间后的 log, 或命令 "tail -20 /var/log/audit/audit.log “ 查看审计日志	审计记录应包括事件的日期、 时间、类型、主体标识、客体标识和结果

	c) 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	非法用户进入系统后的第一件事情就是去清理系统日志和审计日志，而发现入侵的最简单最直接的方法就是去看系统记录和安全审计文件。因此，必须对审计记录进行安全保护，避免受到未预期的删除修改或覆盖等。	访谈审计记录的存储、备份和保护的措施，是否将操作系统日志定时发送到日志服务器上等，并使用 sylog 方式或 smp 方式将日志发送到日志服务器。 如果部署了日志服务器，登录日志服务器查看操作系统的日志是否在收集的范围内	操作系统日志定期备份，共定期将本地存储日志转发至日志服务器
	d) 应对审计进程进行保护，防止未经授权的中断	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容。 在 Linux 中,Auditd 是审计守护进程，syslogd 是日志守护进程，保护好审计进程，当事件发生时，能够及时记录事件发生的详细内容。	1) 访谈对审计进程监控和保护的措施 2) 测试使用非安全审计员中断审计进程，查看审计进程的访问权限是否设置合理。 3) 查看是否有第三方系统对被测操作系统的审计进程进行监控和保护	1）2）审计进程不可以非审计人员权限修改 3）部署有第三方审计工具，可实时记录审计日志，管理员不可对日志进行删除
入侵防范	a) 应遵循最小安装的原则仅安装需要的组件和应用程序	在安装 Linux 操件系统时，应试循最小化安装原则，即不需要的包不进行安装。安装的包越多，面临的风险起大，系统瘦身有利于提高系统的安全性。 在操作系统使用过程中，为了避象由于多余组件和应用程序带来的安全风险，通常遵循最小安装原则，仅安装需要的组件和应用程序	1) 访谈安装系统时是否遵循最小化安装原则，查看安装操作手册 2) 使用命令“ yum list installed" 查看操作系统中已安装的程序包，询问是否有目前不需要的组件和应用程序	1) 系统安装遵循最小化安装原则 2) 不存在业务所不需要的组件和应用程序

	b) 应关闭不需要的系统服务、默认共享和高危端口	Linux 默认安装时会开启许多不必要的系统服务，为了避免由于多余的系统服务带来安全风险，通常可以将其关闭。通过查看监听端口，能够直观地发现并对比系统所运行的服务和程序，关闭高危端口，是操作系统常用的安全加固方式	1) 以有相应权限的身份登录进入 L.inux，使用命令"service --status-all| grep running" 查看是否已经关闭危险的网络服务 2) 以有相应权限的身份登录进入 L.inux，使用命令"netstat -ntlp "查看并确认是否开放的端口都为业务需要端口，是否已经关闭非必需的端口，L.inux 不存在共享问题	1) 关闭了系统多余服务，危险服务和进程 2) 关闭了多余端口
	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	在 Linux 系统中存在 /etc/hosts.allowr 和 /etc/hosts.deny 两个文件，它们是 tcpd 服务器的配置文件，tcpd 服务器可以控制外部 IP 对本机服务的访问。其中 /etc/hosts.allow 控制可以访问本机的 IP 地址，/ete/hosts.deny 控制禁止访问本机的 IP，如果两个文件的配置有冲突，以 /etc/hosts. deny 为准	查看在 /etc/hosts.deny 中是否有“ ALL: ALL", 禁止所有的请求 : 在 /etc/hosts.allow 中, 是否有如下配置 (举例): sshd: 192.168.1.10/255. 255. 255. 0 2) 是否采用了从防火墙设置了对接入终端的限制	1) 使用 more 查看 /etc/hosts.allow 中是否有如下配置限制 IP 及其访问方式，如 (举例): ssbd; 192. 168. 1.10/255.255 255.0 2) 对终端接入方式，网络地址范围等条件进行限制。通过 RADUS、堡垒主机、安全城、防火墙等运维方式实现对终端入方式的限制
	d) 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	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击，应对系统进行漏洞扫描，及时发现系统中存在的已知漏洞，并在经过充分测试评估后更新系统补丁，避免遭受由系统漏洞带的风险	1) 查看甲方自查的洞扫报告或通过第三方检查的漏洞报告，有无高风险漏洞 2) 系统有无漏洞测试环境，补丁更新的机制和流程加何 ？	1 有运维团队定期进行漏洞扫描，发现安全风险，及时补修 2)3 ）更断补丁时间为最近，对补丁进行控制和管理

			3) 访谈补丁升级机制，查看补丁安装情况： #rpm -qa grep patch	
	e) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警	要维护真正安全的环境，只具备安全系统还远远不够。如果假设自己不会受到攻击，或认为防护措施已足以保护自己的安全，都是非常危险的。要维护系统安全，必须进行主动监视，以检查是否发生了入侵和攻击。 一般意义上，入侵威胁分为外部渗透、内部渗透和不法行为三种，入侵行为分为物理入侵、系统入侵和远程入侵三种。此项中，关注的操作系统所面对的入侵成胁可能包含了三种造成入侵威胁的入侵行为主要是系统入侵和远程入侵两种。系统入侵，指入侵者在拥有系统的一个低级账号权限下进行的破坏活动。通常，如果系统没有及时更新最近的补丁程序，那么拥有低级权限的用户就可能利用系统漏洞获取更高的管理特权。远程入侵，指入侵者通过网络渗透到一个系统中。这种情况下，入侵者通常不具备任何特殊权限，	1) 访谈并查看入侵检测的措施，如经常通过如下命令查看入侵的重要线索（试图 Telnet.FTP 等），涉及命令“ #more /var/log /secure|grep refused" 2) 查看是否启用了主机防火墙、TCP SYN保护机制等设置 3) 访谈系统管理员是否安装了主机入侵检测软件。查看已安装的主机入侵，检查系统的配置情况，是否具备报警功能。可执行命令：find / -namie <daemonname> -print 检查是否安装了主机入侵检测软件，如 Dragon Squire by Enterasys Networks ，ITA by Symantec. Hostsentry by Psionic Software.Logcheck by Psiomc Software. RealSecure-agent by ISS 4) 查看网络拓扑图，查看网络上	1）入侵的重要路径均 deny 2) 开启主机防火墙相关置 3) 安装有基于主机的 IDS 设备 4) 若主机未部署主机 IDS 设备。可在网络链路上查香是否是 IDS、IPS. 发生入侵事件时，记录报警措施等

		他们通过漏洞扫扫描端口扫描等技术发现攻击目标，再利用相关技术执行破坏活动	是否部署了网络入侵检测系统，如 IDS	
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	作为 Linux 系统，也面临着木马和蠕虫的破坏，可以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对恶意代码进行检测	1) 核查操作系统中安装了什么防病毒软件，访谈管理员病毒库是否经常更新，核查病毒库最新版本，更新日期是否超过一个星期 2) 核查操作系统是否实现了可信验证机制，能够对系统程序、应用程序和重要配置文件 / 参数进行可信执行验途	1) 部署有网络版防病毒软件，病毒库最新，支持防恶意代码的统 - 管理个 2) 部署有主动免疫可信验证机制，可对病责入侵进行及时阻断

可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	针对服务器设备，需要服务器在启动过程对预装软件 （包括系统引导程序、系统程序、相关应用程序和重要配置参数）进行完整性验证或检测，确保对系统引导程序、 系统程序、 重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1) 核查服务器的启动， 是否实现可信验证的检测过程， 查看对那些系统引导程序、 系统程序或重要配置参数进行可信验证 2) 修改其中的重要系统程序之一和应用程序之一， 核查是否能够检测到并进行报警 3) 是否将验证结果形成审计记录送至安全管理中心	l ）服务器具有可信根芯片或硬件 2) 启动过程基于可信根对系统引导程序、系统程序， 重要配置参数和关键应用程序等进行可信验证度量 3) 在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结果记录
数据备份恢复	应提供重要数据处理系统的热冗余，保证系统的高可用性	对于可用性要求较高的等级保护对象来说，仅仅进行数据备份是远远不够的，还必须进行系统备份。 重要数据处理系统要求采用热冗余 ，保证系统的高可用性	1) 访谈系统管理员哪些是重要数据处理系统， 重要数据处理系统是否有备份机制， 是否采用本地热备份站点备份或异地活动互援备份。 2) 核查设备列表， 重要数据处理系统是否采用热备服务器	1) 对重要数据， 如用户数据， 鉴别数据等定期进行备份， 通过磁带备份到本地 2) 对于重要设备， 采取热备、集群、 负载均衡等高可用方式

4.3 Windows 测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据

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	Linux 系或統的用户鉴别过程与其他 UNIX 系統相同：系统管理员为用户建立一个账户并为其指定一个口令，用户使用指定的口今登录后重新配置自己的自已的口令，这样用户就具备一个私有口令。etc/password 文件中记录用户的属性信息，包括用户名、密码、用户标识、组标识等信息。现在 Linux 系统中不再直接保存在 /etc/password 文件中，通常将 password 文件中的口令字段使用一个“x”来代替，将 /etc/shadow 作为真正的口令文件，用于保存包括个人口令在内的数据。当然，shadow 文件是不能被普通用户读取的，只有超级用户才有权读取。 Linux 中的 /etc/login.defs 是登录程序的配置文件，在这里我们可配置密码的最大过期天数，密码的最大长度约束等内容。如果 /etc/pam.d/system-auth 文件里有相同的选项，则以 /etc/pam.d/system-auth 里的设置为准，也就是说 /etc/pam.d/system-aut 的配置优先级高于 /etc/login.defs 。 Linux 系统具有调用 PAM的应用程度认	1) 访谈系统管理员系统用户是否已设置密码，并查看登录过程中系统账户是否使用了密码进行验证登录。 2) 以有权限的账户身份登录操作系统后，使用命令 more 查看 /etc/shadow 文件，核查系统是否存在空口令账户 3) 使用命令 more 查看 /etc/login. defs 文件，查看是否设置密码长度和定期更换要求 #more /etc/login. defs 使用命令 more 查看 /etc/pam.d/system-auth 文件。查看密码长度和复杂度要求 4) 检查是否存在旁路或身份鉴别措施可绕过的安全风险	1) 登录需要密码 2) 不存在空口令账户 3) 得出类似反馈信息，如下： PASS MAX_DAYS90 #登录密码有效期 90 天 PASS MIN_DAYS 0 #登录密码最短修改时间，增加可以防止非法用户短期更改多次 PASS MIN_LEN 7 #登录密码最小长度 7 位 PASS WARN_AGE 7 #登录密码过期提前 7 天提示修改 4) 不存在绕过的安全风险

		证用户。登示服务、屏保等功能，其中一个重要的文件使是 etc/pam.d/system-auth(在 Kedhat Cent0s 和 Fedora 系上）。/etc/pam.d/system-auth 或 /etc/login.defs 中的配置优先级高于其他地方的配置。 另外，root 用户不受 pam 认证规则的限制，相关配置不会影响 root 用户的密码，root 用户可以随意设置密码的。login.defs 文件也是对 root 用户无效的。		

	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	Linux 系统具有调用 PAM的应用程度认证用户、 登录服务、 屏保等功能， 其中一 个 重 要 的 文 件 便 /etc/pam.d/system-auth ， Redhat5 以后版本使用 pam_tally2.so 模块控制用户密码认证失败的次数上限，可以实现登录次数、 超时时间， 解锁时间等。 着只是针对某个程序的认证规则，在 PAM目录 (/etc/pam d) 下形如 sshd、login 等等的对应各程序的认证规则文件中进行修改。若所有密码认证均应用规则， 可直接修改 system_auth 文件	1) 系统配置并启用了登录失败处理功能 2) 以 root 身份登录进入 Linux ，查看文件内容 ： # cat /ete/pam.d/system -auth 或根据 linux 版本不同在 common 文件中 3) 查 看 /etc/profile 中 的 TIMEOUT环境变量，是否配置超时锁定参数	得出类似反馈信息，如下 ： 1) 和 2) 查看登录失败处理功能相关参数， /etc/pam.d/system — auth 文件中存 在 "account required /lib/security/pam_tally.so deny=3 no_ magic root reset" ; 3) 记录在文件 /etc/profile 中设置了超时锁定参数，在 profile 下设置 TMOUT= 300s

	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听	Linux 提供了远程访问与管理的接口，以方便管理员进行管理操作，网络登录的方式也是多样的，例如可以使用 Telnet 登录，也可以使用 SSH登录。但是， Telnet 不安全。 I 因为其在教据传输过程中，账户与密码均明文传输，这是非常危险的。黑客通过一些网络对嗅探工是能够轻易地的窃取网络中明文传输的账户与密码，因此不建议通过 Telnet 协议对服务器进行远程管理。针对 Telnet 协议不安全这种情况，可以在远程登录时使用 SSH协议。其原理跟 Telnet 类似，只是其具有更高的安全性。 SSH是一个运行在传输控制层上的应用程序，与 Telnet 相比，它提供了强大的认证与加密功能，可以保证在远程连接过程中，其传输的数据是加密处理过的。因此保障了账户与口令的安全	访谈系统管理员， 进行远程管理的方式。 1) 以 root 身份登录进入 Linux 查看是否运行了 sshd 服务，service - status-all | grep sshd 查看相关的端口是否打开，netstat -an|grep 22 若未使用 SSH方式进行远程管理，则查看是否使用了 Telnet 方式进行远程管理 service - -status-all|grep running， 查看是否存在 Telnet 服务 2) 可使用 wireshark 等抓包工具，查看协议是否为加密 3) 本地化管理， N/A	1) 使用 SSH方式进行远程管理， 防止鉴别信息在传输过程中被窃听 ,Telnet 默认不符合 2) 通过抓包工具， 截获信息为密文， 无法读取，协议为加密 3) N/A 本地管理
	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	对于第三级及以上的操作系统要求采用口令、 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	访谈和核查系统管理员在登录操作系统的过程中使用了哪些身份鉴别方法， 是否采用了两种或两种以上组合的鉴别技术， 如口令教字证书 Ukey、令牌、 指纹等， 是否有一种鉴别方法在鉴别过程中使用了密码技术	除口令之外，采用了另外一种鉴别机制，此机制采用了密码技术， 如调用了密码机或采取 SM1-SM4等算法

访问控制	a) 应对登录的用户分配账户和权限	对于 Linux 中一些重要的文件，应检查 Linux 系统主要目录的权限设置情况，Linux 系统对文件的操作权限，包括 4 种：读(r,4) ；写 (w,2) ；执行 (x,1) ；空(一，0)，文件的权限分为属主 (拥有者)、属组、其它用户和用户组的权限	以有相应权限的身份登录进入 Linux，使用“ 1s-1 文件名”命令，查看重要文件和目录权限设置是否合理，如：# 1s -1 /etc/passwd #744。	重点查看以下文件和目录权限是否设置合理。 —rwx- - - - -: 数字表示为 700 -rwxr--r- -: 数字表示为 744 -rw-rw-r-x: 数字表示为 665 drwx-x 一 x: 数字表示为 711 drwr- - - - -: 数字表示为 700 配置文件权限值不能大于 644，对于可执行文件不能大于 755
	b) 应重命名或删除默认账户，修改默认账户的默认口令	Linux 操作系统本身安装后提供各种账号，如 adm lp sync shutdown halt mail uucp operator games gopher ftp 等，但这些账户使用时并不需要，有的帐号越多，就越容易受到攻击，应禁用或者删除这些用户。 root 作为重要的默认账户，一般要求禁止远程登录	1) 以有相应权限的身份登录进入 Linux，使用 more 查看 /etc/shadow 文件，查看文件中的用户，是否存在 adm、lp. sync 、shutdown 、halt. 、mail 、uucp 、operator, 、games.、gopher ftp 等默认的、无用的用户。 2) 查看 root 账户是否能够进行远程登录	1) 不存在默认无用的账户 2) 使用 more 查看 /etc/ssh/sshd_config 文件中的 "PermitRootLogin" 参数设置为“ no “ ，即：PermitRootLogin no, 即不许可 root 远程登录
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在	通常操作系统在运行一段时间后，因业务应用或管理员岗位的调整，出现一些多余的、过期的账户；另一方面，也会出现多个系统管理员或用户使用同一账户登录操作系统的情况，造成审计追踪时无法定位到自然人。如果存在多余的，过期的账户，可能会被攻击者利用其进行非法操作的风险，因	1) 应核查是否不存在多余或过期账户，如查看 games、news、ftp 、1p 等系统默认账户是否被禁用，特权账号 halt 、shutdown 是否被删除 2) 应访谈网络管理员、安全管理员、系统管理员不同用户是否采用不同账户登录系统	1) 禁用或删除不需要的系统默认账户，如 games、news、ftp 、1p 、halt 、shutdown 等 2) 各类管理员均使用自己分配的特定权限账户登录，不存在多余、过期账户

		此应及时清理系统中的账户，删除或停用多余的、 过期的账户， 同时避免共享账户的存在		
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限。 Linux 系统安装后，root 拥有所有权限， 使用 sudo 授予普通用户 root 级权限，在 sudoer.conf 中进行配置	1) 以有相应权限的身份登录进入 Linux， 使用 more 查看 /etc/passwd 文件中的非默认用户，询问各账户的权限， 是否实现管理用户的权限分离 2) 以有相应权限的身份登录进入 Linux， 使用 more 查看 /etc/sudo.conf 文件，核查 root 级用户的权限都授予哪些账户	1) 各用户均具备最小权限 , 不与其他用户权限交叉。 设备下可支持新建多用户角色功能 2) 管理员权限仅分配 root 用户
	d) 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	操作系统的访问控制策略应由授权主体（如安全管理员） 进行配置， 非授权主体不得更改访问控制策略。访问控制策略规定操作系统用户对操作系统资源（如文件和目录 ）具有哪些权限，能进行哪些操作、通过在操作系统中配置访问控制策略，实现对操作系统各用户权限的限制	1) 访谈系统管理员， 是否指定授权人对操作系统访问控制权限进行配置 2) 核查账户权限配置， 是否依据安全策略配置各账户的访问规则	1) 由专门的安全员负责对访问控制权限的授权工作 2) 各账户权限配置， 均是基于安全员的安全策略配置进行的访问控制

	e) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	明确提出访问控制的粒度要求，重点目录的访问控制的主体可能为某个用户或某个进程，应能够控制用户或进程对文件、数据库表等客体的访问	使用“ ls -1 文件名”命令，查看重要文件和目录权限设置是否合理，如:#ls -1/etc/passwd #744，应重点查看以下文件和目录权限是否被修改过	由管理用户进行用户访问权限分配进行设置，依据访问控制策略 ，对各类文件和数据库表级进行访问。 重要文件和目录权限均在合理范围内， 用户可根据对文件不同的权限进行操作
	f) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	敏感标记是由强认证为安全管理员进行设置的，通过对重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作， 实现强制访问控制。 安全增强型 Linux (Security Enhanced Linux) 简称 SELinux，是一个 Linux 内核模块，也是 Linux 的一个安全子系统。2.6 及以上版本的 Linux 内被都团经集成了 SELinux 模块，在使用 SELinux 的操作系统中， 决定一个资源是否能够被访问的因素除了用户的权限 (读、写、执行) 外，还需要判断每一类进程是否拥有对某一类资源的访问权限，这种权限管理机制的主体是进程，也称为强制访问控制 (MAC)。在 SELinux 中，主体等同于进程， 客体是主体访问的资源，可以是文件、目录、端口、设备等	1) 明确系统中是否有敏感信息 2) 在主体用户或进程划分级别并设置敏感标记， 在客体文件设置敏感标记 3) 应测试是否依据主体、 客体安全标记控制主体对客体访问的强制访问控制策略 4) 以有相应权限的身份登录进入 Linux， 使用 more 查看 /etc/selinux/config 文件中的 SELINUX参数的设定	1) 2) 3)4) linux 服务器默认关闭 SELinux 服务。 或采取第三方主机加固系统或对操作系统内核进行二次开发加固，并实际查看系统可视化界面。 SELINUX有三种工作模式，分别是 : enforcing: 强制模式。违反 SELinux 规则的行为将阻止并记录到日志中， 表示使用 SELinux 。 permissive: 宽容模式。违反 SELinux 规则的行为只会记录到日志中， 一般为调试用，表示使用 SELinux disabled: 关闭 SELinux，使用 SELinux

安全审计	a) 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	Redhat Enterprise Linux-3 update 2 以后都开始使用 LASU (Linux Aduit Subsystem) 来进行审计。且志系统可以记录系统的各种信息 , 如: 安全、调试、运行信息。 审计子系统专用来记录安全信息，用于对系统安全事件的追溯。如果审计子系统没有运行， Linux 内核就将安全审计信息传递给日志系统。 Linux 操作系统的 auditd 进程主要用来记录安全信息。用于对系统安全事件的追溯；而 rsyslog 进程用来记录系统中的各种信息，如硬件报警和软件日志。Linux 操作系统在安全审计配置文件 /etc/audit/audit.rules 中配置安全事件审计规则	1) 以 root 身份登录进入 Linux, 查看服务进程 2) 若运行了安全审计服务， 则查看安全审计的守护进程是否正常 # ps -ef|grep auditd 3) 若未开启系统安全审计功能， 则确认是否部署了第三方安全审计工具 4) 以 root 身份登录进入 Linux 查看安全事件配置 : #gerep “ @priv-ops" /etc/audit/filter.conf .... more/etc/audit/audit.rules	1) 开启审计进程内容如下 : [root@localhost april]# service auditd status auditd (pid 1656) is running... [root@localhost april]# service rsyslog statusr syslogd (pid 1681) is running... [root@localhost april]# 2)Linux 服务器默认开启守护进程 3)audit.rules 中记录对文件和底层调用的相关记录， 记录的安全事件较为全面
	b) 审计记录应包括事件的日期和时间， 用户、事件类型，事件是否成功及其他与审计相关的信息	详细的审计记录才能实现有效的审计，审计记录应该包括事件的日期、 时间、类型、主体标识、 客体标识和结果等。通过记录中的详细信息， 能够帮助管理员或其他相关检查人员准确的分析和定位事件。 Linux 用户空间审计系统由 auditd 、ausearch 和 aureport 等应用程序组成，其中 ausearch 是查找审计事件的工具，可以用来查看系统日志	以有相应权限的身份登录进入 Linux, 使用命令 "ausearch-ts today ”，其中， -ts 指定时间后的 log, 或命令 "tail -20 /var/log/audit/audit.log “ 查看审计日志	审计记录应包括事件的日期、 时间、类型、主体标识、客体标识和结果

	c) 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	非法用户进入系统后的第一件事情就是去清理系统日志和审计日志，而发现入侵的最简单最直接的方法就是去看系统记录和安全审计文件。因此，必须对审计记录进行安全保护，避免受到未预期的删除修改或覆盖等。	访谈审计记录的存储、备份和保护的措施，是否将操作系统日志定时发送到日志服务器上等，并使用 sylog 方式或 smp 方式将日志发送到日志服务器。 如果部署了日志服务器，登录日志服务器查看操作系统的日志是否在收集的范围内	操作系统日志定期备份，共定期将本地存储日志转发至日志服务器
	d) 应对审计进程进行保护，防止未经授权的中断	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容。 在 Linux 中,Auditd 是审计守护进程，syslogd 是日志守护进程，保护好审计进程，当事件发生时，能够及时记录事件发生的详细内容。	1) 访谈对审计进程监控和保护的措施 2) 测试使用非安全审计员中断审计进程，查看审计进程的访问权限是否设置合理。 3) 查看是否有第三方系统对被测操作系统的审计进程进行监控和保护	1）2）审计进程不可以非审计人员权限修改 3）部署有第三方审计工具，可实时记录审计日志，管理员不可对日志进行删除
入侵防范	a) 应遵循最小安装的原则仅安装需要的组件和应用程序	在安装 Linux 操件系统时，应试循最小化安装原则，即不需要的包不进行安装。安装的包越多，面临的风险起大，系统瘦身有利于提高系统的安全性。 在操作系统使用过程中，为了避象由于多余组件和应用程序带来的安全风险，通常遵循最小安装原则，仅安装需要的组件和应用程序	1) 访谈安装系统时是否遵循最小化安装原则，查看安装操作手册 2) 使用命令“ yum list installed" 查看操作系统中已安装的程序包，询问是否有目前不需要的组件和应用程序	1) 系统安装遵循最小化安装原则 2) 不存在业务所不需要的组件和应用程序

	b) 应关闭不需要的系统服务、默认共享和高危端口	Linux 默认安装时会开启许多不必要的系统服务，为了避免由于多余的系统服务带来安全风险，通常可以将其关闭。通过查看监听端口，能够直观地发现并对比系统所运行的服务和程序，关闭高危端口，是操作系统常用的安全加固方式	1) 以有相应权限的身份登录进入 L.inux，使用命令"service --status-all| grep running" 查看是否已经关闭危险的网络服务 2) 以有相应权限的身份登录进入 L.inux，使用命令"netstat -ntlp "查看并确认是否开放的端口都为业务需要端口，是否已经关闭非必需的端口，L.inux 不存在共享问题	1) 关闭了系统多余服务，危险服务和进程 2) 关闭了多余端口
	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	在 Linux 系统中存在 /etc/hosts.allowr 和 /etc/hosts.deny 两个文件，它们是 tcpd 服务器的配置文件，tcpd 服务器可以控制外部 IP 对本机服务的访问。其中 /etc/hosts.allow 控制可以访问本机的 IP 地址，/ete/hosts.deny 控制禁止访问本机的 IP，如果两个文件的配置有冲突，以 /etc/hosts. deny 为准	查看在 /etc/hosts.deny 中是否有“ ALL: ALL", 禁止所有的请求 : 在 /etc/hosts.allow 中, 是否有如下配置 (举例): sshd: 192.168.1.10/255. 255. 255. 0 2) 是否采用了从防火墙设置了对接入终端的限制	1) 使用 more 查看 /etc/hosts.allow 中是否有如下配置限制 IP 及其访问方式，如 (举例): ssbd; 192. 168. 1.10/255.255 255.0 2) 对终端接入方式，网络地址范围等条件进行限制。通过 RADUS、堡垒主机、安全城、防火墙等运维方式实现对终端入方式的限制
	d) 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	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击，应对系统进行漏洞扫描，及时发现系统中存在的已知漏洞，并在经过充分测试评估后更新系统补丁，避免遭受由系统漏洞带的风险	1) 查看甲方自查的洞扫报告或通过第三方检查的漏洞报告，有无高风险漏洞 2) 系统有无漏洞测试环境，补丁更新的机制和流程加何 ？	1 有运维团队定期进行漏洞扫描，发现安全风险，及时补修 2)3 ）更断补丁时间为最近，对补丁进行控制和管理

			3) 访谈补丁升级机制， 查看补丁安装情况： #rpm -qa grep patch	
	e) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警	要维护真正安全的环境，只具备安全系统还远远不够。如果假设自己不会受到攻击，或认为防护措施已足以保护自己的安全， 都是非常危险的。 要维护系统安全， 必须进行主动监视， 以检查是否发生了入侵和攻击。 一般意义上，入侵威胁分为外部渗透、内部渗透和不法行为三种，入侵行为分为物理入侵、系统入侵和远程入侵三种。 此项中， 关注的操作系统所面对的入侵成胁可能包含了三种造成入侵威胁的入侵行为主要是系统入侵和远程入侵两种。 系统入侵， 指入侵者在拥有系统的一个低级账号权限下进行的破坏活动。 通常，如果系统没有及时更新最近的补丁程序，那么拥有低级权限的用户就可能利用系统漏洞获取更高的管理特权。 远程入侵， 指入侵者通过网络渗透到一个系统中。这种情况下，入侵者通常不具备任何特殊权限，	1) 访谈并查看入侵检测的措施， 如经常通过如下命令查看入侵的重要线索（试图 Telnet.FTP 等），涉及命令“ #more /var/log /secure|grep refused" 2) 查看是否启用了主机防火墙、TCP SYN保护机制等设置 3) 访谈系统管理员是否安装了主机入侵检测软件。 查看已安装的主机入侵， 检查系统的配置情况， 是否具备报警功能。可执行命令 : find / -namie <daemonname> -print 检查是否安装了主机入侵检测软件，如 Dragon Squire by Enterasys Networks ， ITA by Symantec. Hostsentry by Psionic Software.Logcheck by Psiomc Software. RealSecure-agent by ISS 4) 查看网络拓扑图，查看网络上	1）入侵的重要路径均 deny 2) 开启主机防火墙相关置 3) 安装有基于主机的 IDS 设备 4) 若主机未部署主机 IDS 设备。可在网络链路上查香是否是 IDS、IPS. 发生入侵事件时，记录报警措施等

		他们通过漏洞扫扫描端口扫描等技术发现攻击目标，再利用相关技术执行破坏活动	是否部署了网络入侵检测系统，如 IDS	
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	作为 Linux 系统，也面临着木马和蠕虫的破坏，可以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对恶意代码进行检测	1) 核查操作系统中安装了什么防病毒软件，访谈管理员病毒库是否经常更新，核查病毒库最新版本，更新日期是否超过一个星期 2) 核查操作系统是否实现了可信验证机制，能够对系统程序、应用程序和重要配置文件 / 参数进行可信执行验途	1) 部署有网络版防病毒软件，病毒库最新，支持防恶意代码的统 - 管理个 2) 部署有主动免疫可信验证机制，可对病责入侵进行及时阻断

可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	针对服务器设备，需要服务器在启动过程对预装软件 （包括系统引导程序、系统程序、相关应用程序和重要配置参数）进行完整性验证或检测，确保对系统引导程序、 系统程序、 重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1) 核查服务器的启动， 是否实现可信验证的检测过程， 查看对那些系统引导程序、 系统程序或重要配置参数进行可信验证 2) 修改其中的重要系统程序之一和应用程序之一， 核查是否能够检测到并进行报警 3) 是否将验证结果形成审计记录送至安全管理中心	l ）服务器具有可信根芯片或硬件 2) 启动过程基于可信根对系统引导程序、系统程序， 重要配置参数和关键应用程序等进行可信验证度量 3) 在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结果记录
数据备份恢复	应提供重要数据处理系统的热冗余，保证系统的高可用性	对于可用性要求较高的等级保护对象来说，仅仅进行数据备份是远远不够的，还必须进行系统备份。 重要数据处理系统要求采用热冗余 ，保证系统的高可用性	1) 访谈系统管理员哪些是重要数据处理系统， 重要数据处理系统是否有备份机制， 是否采用本地热备份站点备份或异地活动互援备份。 2) 核查设备列表， 重要数据处理系统是否采用热备服务器	1) 对重要数据， 如用户数据， 鉴别数据等定期进行备份， 通过磁带备份到本地 2) 对于重要设备， 采取热备、集群、 负载均衡等高可用方式

4.4 Oracle 测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据

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	应检查 Oracle 数据库的口令策略配置，查看其身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口今复杂（如规定字符应混有大，小写字母数字和特殊字符），口令定期更新，新旧口令的替换要求	1) 访谈数据库管理员系统用户是否已设置密码，并查看登录过程中系统账户是否使用了密码进行验证登录 2) 查看是否启用口令复杂度函数：select limit from dba_profiles where profile= ' DEFAULT' and resource_name=' PASSWORD_VERIFY_FUNCTION' 3) 检查 utlpwdmg.sql 中“ -- Check for the minimum length of the password “部分中“ length(password)<" 后的值 4) PASSWORD_LIFE_TIME（口令过期时限）	1) 需要登录密码 2)dba_profiles 策略中 PASSWORD_VERIFY_FUNCTION 的值不为 UNLLIMITED 3)utlpwdmg.sql 中“ -- Check for the minimum length of the password “部分中“ length(password)<" 后的值为 8 或以上 4）dba_profiles 策略中 PASSWORD_LIFE_TIME 不为 UNLIMITED
	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	应检查数据库系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值，对超过限制值的登录终止其鉴别会话或临时封闭帐号。查看是否设置网络登录连接超时，并自动退出	1) 查看是否启用登录失败限制策略，执行：select limit from dba_profiles where profile= ' DEFAULT' and resource name=' FAILED_LOGIN_ATTEMPTS 2) 查看是否启用登录失败锁定策略，执行：select limit from dba_profiles where profile= 'DEFAULT' and resource_ name= PASSWORD_LOCK_TIME" 3) 查看是否启用登录超时退出策略，执行： select limit from dba_profiles=	1)dba_pofiles 策略中 FAILED_LOGIN_ATTEMPTS 不为 UNLIMITED 2)dba_pofiles 策略中 PASSWORD_LOCK_TIME 不为 UNLIMITED 3)dba_pofiles 策略中 IDLE_ TIME 不为 UNLIMITED

			'DEFAULT and resource name= 'IDLE_ TIME'	
	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听	为了防止包括鉴别信息在内的敏感信息在网络传输过程中被窃听，应限制从远程管理数据，如果业务模式需要从远程进行管理，则应提供包括 SSH在内的方式对传输数据进行加密	1) 查看initsSID.ora (%ORACIE_HOME\db_1\NETWORK\ADMIN)中 REMOTE_0S _AUTHEN的赋值 2) 查看listene.ora (%ORACIE_HOME\db_1\NETWORK\ADMIN)文件中的 "LISTENER ” -"DESCRIPTION "-"ADDRESS_LIST"-"ADDRESS"-"PROTOCOL项目的赋值 3) 执行show parameter remote_login_passwordfile	1) 符合，且本项为 false, 则符合 (为true, 远程操作系统认证。 2) 应存在以下项目 : PROTOCOL=TCPS (实际为 TCP) 3) 结果 应为 NONE,远程 无法登录 , Exclusive (唯 一的数据库密码文件登录
	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	Oracle 不能集成其他身份鉴别措施，应通过对操作系统层面实现双因素，强化数据库安全	查看和询问系统管理员在登录数据库的过程中使用了哪些身份鉴别方法，是否采用了两种或两种以上组合的鉴别技术，如口令、数字证书 Ukey. 令牌、指	除口令之外，采用了另外一种鉴别机制，此机制采用了密码技术， 如调用了密码机或采取 SM1-SM4等算法

	中一种鉴别技术至少应使用密码技术来实现		纹等，是否有一种鉴别方法使用密码技术	
访问控制	a) 应对登录的用户分配账户和权限	应检查数据库系统的安全策略，查看业务数据的管理员是否具有系统管理功能，业务数据库的操作人员是否具有删除数据库表或存储过程的权限	查看每个登录用户的角色和权限，是否是该用户所需的最小权限	MGMT_UIEW, SYS， SYSTEM，DBSNMP，SYSMAN是 open 的状态，其他都是锁定
	b) 应重命名或删除默认账户， 修改默认账户的默认口令	1) 在 oracle 系统安装时存在部分默认口令，如 SYS：CHANGE_ON_INSTALL SYSTEM:MANAGER 2) 常用口令 ： oracle:oracle/admin/ora92(ora+ 版本) sys: oracle/admin system: oralce/admin	1) 登录验证 sys 的口令是否为 CHANGE_ON_INSTALL 2) 登录验证 system 的口令是否为 manager 3) 登录验证 dbsnmp 的口令是否为 dbsnmp	1)2)3) 使用默认口令无法登陆数据库账户
	c) 应及时删除或停用多余的、 过期的账户，避免共享账户的存在	应删除数据库中多余的过期的账户，如测试帐号等	1) 在 sqlplus 中执行命令： select username , account_ status_from dba users 2) 查看返回结果中是否存在 scott. out1n 、 ordsys 等范例数据库帐号 3) 针对上述命令获得的用户帐号，查看是否存在过期账户，询问数据库管理员是否每一个账户均为正式、有效的账户	1) 不存在示例帐户 2) 应不存在 acount status 为“ expired" 的帐户 ；所有帐户均为必要的管理帐户或者数据库应用程序帐户 (不存在测试帐户 / 临时账户) 3) 每一个数据库帐户与实际用户应为一一对应关系 4) 不存在多人共享帐户的情况

			4) 针对上述命令获得的用户帐号，询问是否存在多人共享账户的情况	
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离	在 Oracle 数据库中，尽量将数据库系统特权用户的权限进行分离	询问是否由不同员工分别担任操作系统管理员与数据库管理员	由不同员工分别担任操作系统管理员与数据库管理员
	d) 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	应检查数据库系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体（如文件或系统设备，目录表和存取控制表等）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件，数据库表等）及它们之间的操作［如读、写或执行）	询问数据库管理员，数据库系统是否由特定账户进行配置访问控制策略，具体访问控制策略是什么	由特定账户进行配置访问控制策略，并根据用户角色限制账户权限
	e) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	明确提出访问控制的粒度要求，重点目录的访问控制的主体可能为某个用户或某个进程，应能够控制用户或进程对文件、数据库表等客体的访问	询问数据库管理员，访问控制的粒度主体是否用户级或进程级，客体是否为文件、数据库表级	由管理用户进行用户访问权限分配进行设置，依据访问控制策略，对各类文件和数据库表级进行访问

	f) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	应通过 Oracle 数据库或其它措施对重要的信息资源设置敏感标记，从而实现强制访问控制功能	1) 检查是否安装 Oracle Lable Security 模块 2) 查看是否创策略：SELECT policy_name,status form DBA_SA_POLICIES 3) 查看是否创建级别：SELECT * form dba_sa_levels ORDER BY level_number 4) 查看标签创建情况：select * from dba_sa_labels. 5) 询问重要数据存储表格名称 6) 查看策略与模式|表的对应关系：select * from dba_sa_tables policles, 判断是否针对重要信息资源设置敏感标签	1) 返回的用户用户中应存在'LBACSYS' 2) 存在状态为 "enable' 的标签策略 3) -4) 返回结果不为空 5) 重要资源所在的表格名称 6) 返回结果应不为空，且项目包含 5)的结果
安全审计	a) 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	应检查数据库系统是否开启安全审计功能，查着当前审计范围是否覆盖到每个用户	1) 执行：selecet value form v$parameter where name='audit_trail', 查看是否开启审计功能 2) 用不同的用户登录数据库系统并进行不同的操作，在 Oracle 数据库中查看日志记录是否满足要求。	1) audit_trail 结果应不为 pone 2) 可在 Oracle 数据库中查看不同的用户登录数据库系统并进行不同的操作日志记录。

	b) 审计记录应包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息	应检查数据库系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户登录系统、自主访问控制的所有操作记录、重要用户行为（如增加/删除用户，删除库表）等	1)show parameter audit_trail ?>show parameter audit_sys_operations 3)select sel,upd,del,ins,gra from dba_obj_audit _opts 4)select sel,upd,del,ins,gra from dba_stmt_audit _opts 5)select sel,upd,del,ins,gra from dba_priv_audit _opts 6) 记录一条日志内容，确认其包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容	1) 应不为 none 2) 应为 true 3) 返回对象审计选项，应不全部为“-/-” 4) 返回语句审计选项，应不全部为“-/-” 5) 返回特权审计选项，应不全那为“-/-” 6) 默认满足
	c) 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	应检查 Oracle 数据库系统，查看是否对日志进行了权限设置，非授权人员不能对日志进行操作，另外，应防止审计日志空间不够而导致无法记录日志的情况发生	是否严格限制用户访问审计记录的权限，如采用 audit vault 等	安全审计管理员定期对审计记录进行备份，对审计记录的维护和导出由专人负责
	d) 应对审计进程进行保护，防止未经授权的中断	对于 Oracle 数据库系统默认符合，但是如果采取了第三方工具，则应检查数据库系统，查看未授权用户是否能中断审计进程	1) 询问是否严格限制管理员权限 2) 用户可以通过 alter system set audit_trail=none 并重启实例关闭审计功能，查看是否成功	1) 已限制管理员审计功能权限 2) 测试其他人员无法对审计进程开启、关闭操作，并记录

入侵防范	a) 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	Oracle 数据库限制远程连接 IP 地址	查看在 sqlnet. ora 文件中是否配置参数：tcp.validnode_checking，tcp,invited_nodes tcp.validnode_checking=yes tcp.invited_nodes=() # 运维访问的 IP 列表，各 IP 之间用逗号分隔	在 sqlnet. ora 文件中 tcp.validnode_checking=yes tcp.invited_nodes 已配置参数 ip 列表
	b) 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	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击，应对系统进行漏洞扫描，及时发现系统中存在的已知漏洞，并在经过充分测试评估后更新系统补丁，. 避免遭受由系统漏洞带的风险	访谈 Oracle 补丁升级机制，查看补丁安装情况： #cd $ORACLE HOME/0patch opatch lsinventory	返回 OPatch version 信息和 OUI version 信息
数据备份恢复	a) 应提供重要数据处理系统的热冗余，保证系统的高可用性	数据库系统至少达到以下的备份要求：提供本地实时备份的功能，当数发生错误时，能及时恢复数据	1) 询间系统管理员数据库的备份和恢复策略是什么，查看是否达到上述要求 2) 检查相关文档和配置，查看是否与系统管理员回答的一致	) 核查备份结果与备份策略一致 2) 核查近期恢复测试记录能够进行正常的数据恢复
	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	应提供灾备中心，对重要的数据提供异地数据级备份，保证当本地系统发生灾难性后果不可恢复的，利用异地保存的数据对系统数据能进行恢复	1）询问系统管理员是否提供异地数据备份功能，是否定时批量传送至备用场地 2) 如果条件允许，则查看其实现技术措施的配置情况	1) 已部署异地备份机房，并符合备份策略通过网络定期进行异地备份 2) 查看实现的配置结果与备份策略一致

4.5 MySQL 测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据

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	应检查 MySQL 数据库的口令策略配置，查看其身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口今复杂（如规定字符应混有大，小写字母数字和特殊字符），口令定期更新，新旧口令的替换要求	1) 尝试登录数据库，执行 mysql -u root -p 查看是否提示输入口令鉴别用户身份 2) 使用如下命令查询账号 select user, host FROM mysql.user 结果输出用户列表，查者是否存在相同用户名 3) 执行如下语句查询是否在空口令用： select * from mysql.user where length(password)= 0 or password is null 输出结果是否为空 4) 执行如下语句查看用户口今复杂度相关配置： show variables like 'validate%'; 或 show VARIABLES like "%password “	1) 用户登录数据库时，采用用户名、口令的方式进行身份鉴别 2) 查询 user 表，不存在相同的用户名 3) 不存在空口令用户； 4) 配置信息： validate_password_length 8 validat_ password_mixed_case_count 1 validate_password_number_count 1 validate_password policy MEDIUM validate_password_special_char_count 1

	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	应检查数据库系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值，对超过限制值的登录终止其鉴别会话或临时封闭帐号。查看是否设置网络登录连接超时，并自动退出	1) 询问管理员是否采取其他手段配置数据库登录失败处理功能。 2）执行 show variables like %max_connect_errors%"; 或核查 my.cnf 文件，应设置如下参数： max_connect_errors=100 3) show variables like ”%timeout%“，查看返回值	1)MySQL数据库采用第三方管理软件，且第三方管理软件设置登录失败锁定次数 2)3) 数据库管理系统本地配置了参数 max_connect_errors= 100，Wait_timeout = 28800，如果 mysql 服务器连续接收到了来自于同一个主机的请求，且这些连续的请求全部都没有成功的建立连接就被断开了，当这些连续的请求的累计值大于 max_connect_errors 的设定值时，mysql 服务器就会阻止这台主机后续的所有请求。Wait_ timeout: 一个连接 connection 空闲超过 8 个小时（默认值 28800 秒），MySQL就会自动断开这个连接
	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听	为了防止包括鉴别信息在内的敏感信息在网络传输过程中被窃听，应限制从远程管理数据，如果使用了远程访问，要确保只有定义的主机才可以访问服务器，一般通过 TCP wrappers 、iptables 或任何其它的防火墙软件或硬件实现	1) 是否采用加密等安全方式对系统进行远程管理 2) 执行 mysql>show variables like %have_ssl%" 查看是否支持 ssl 的连接特性，若为 disabled 说明此功能没有激活，或执行 \s 查看是否启用 SSL; 3) 如果采用本地管理方式，该项为不适用	1) 远程管理采用的方式 ：远程管理数据库，启用了 SSL连接特性。 2) 用户远程管理数据库时，客户端和服务器的连接不通过或跨越不可信任的网络，采取 SSH隧道加密连接选程管理通信 3) 本地管理，本条 N/A

	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	MySQL不能集成其他身份鉴别措施，应通过对操作系统层面实现双因素，强化数据库安全	1)MySQL 不能集成其他身份鉴别措施，应通过对操作系统层面实现双因素 2）访谈系统管理员，是否采用其他技术手段实现双因素身份认证，是否采用了两种或两种以上组合的鉴别技术，如口令、数字证书 Ukey. 令牌、 指纹等， 是否有一种鉴别方法使用密码技术	1) 采用的登录方式有 ：用户名口令， MySQL 数据库无法集成其他身份鉴别方式，在操作系统实现双因素，通常将服务器纳入到堡垒机管理，同时通过限制仅允许通过堡垒机坛维服务器。在堡垒机实现双因素身份认证。 常见的双因素认证方式有口令、 数字证书 Ukey. 令牌、指纹等 2) 采用的密码技术是 ： 在硬件 UKey 中使用了加密算法
访问控制	a) 应对登录的用户分配账户和权限	访谈管理员数据库用户账户及权限分配情况，并测试网络管理员、 安全管理员、 系统管理员或核查用户账户和权限设置的情况， 有些 mysql 数据库的匿名用户的口令为空，因而，任何人都可以连接到这些数据库。 如果匿名帐户 grants 存在，那么任何人都可以访问数据库， 至少可以使用默认的数据库 ” test “ . 因此， 应核查是否已禁用匿名、 默认账户的访问权限	1) 执 行 语 句 select user,host FROM mysql.user 输出结果是否为网络管理员， 安全管理员，系统管理员创建了不同账户 : 2) 执 行 show grants for' XXXX'@' localhost' ： 查看网络管理员， 安全管理员、 系统管理员用户账号的权限， 权限间是否分离并相互制约	1) 审计员的角色， 创建了不同的账户， 并为其分配了相应的权限 2) 已禁用匿名、 默认账户或限制匿名、 默认用户的权限
	b) 应重命名或删除默认账户，修改默认账户的默认口令	在 linux 中， root 用户拥有对所有数据库的完全访问权。 因而，在 linux 的安装过程中，一定要设置 root 口令，要改变默认的空口令	1) 执行 select user,host FROM mysql.user 输出结果查看 root 用户是否被重命名或被删除 2) 若 root 账户未被删除，是否更改其默认口令， 避免空口令或弱口令.	1) 数据库管理系统默认账户已被删除 2) 数据本管理系统账认账户 root 未被删除，但增强其口令复杂度， 不要空口令、 弱口令的现象

	c) 应及时删除或停用多余的、过期的账户， 避免共享账户的存在	在默认安装 mysql 中，匿名户可访问 test 数据库．我们可以移除任何无用的数据库， 以避免在不可预料的情况下访问了数据库， 同时删除数据库中多余的、 过期的账户，如测试账号等	1) 在 sqlplus 中执行命令：select username,account_status from dba_users 2) 执行下列语句 ： select * from mysql.user where user="" select user, host FROM mysql.user 依次核查列出的账户， 是否存在无关的账户。 3) 访谈网络管理员，安全管理员、系统管理员不同用户是否采用不同账户登录系统	1) 不存在示例帐户 2) 数据库管理系统用户表中不存在无关账户 3) 不存在多人共享帐户的情况
	d) 应授予管理用户所需的最小权限，实现管理用户的权限分离	有些应用程序是通过一个特定数据库表的用户名和口令连接到 WySQL 的，安全人员不应当给予这个用户完全的访问权。 如果攻击者获得了这个拥有完全访问权的用户， 他也就拥有了所有的数据库。 因此应核查用户是否行角色划分 ，核查访问控制策略，查看管理用户的权限是否已进行分离，并核查管理用户权限是否为其工作任务所需的最小权限	1) 是否对用户进行角色划分且只授予账号必须的权限 如除 root 外，任何用户不应该有 mysql 库 user 表的存取权限，禁止将 fil 、.process 、 super 权限授予管理员以外的账户 2) 查看权限表， 并验证用户是否具有自身角色外的其他用户的权限	1）2) 记录管理用户的权限分配情况：分配了网络管理员、 安全员、 审计员账号， root 账户使用需向数据库管理员申请

	d) 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	应检查数据库系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体（如文件或系统设备，目录表和存取控制表等）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件，数据库表等）及它们之间的操作［如读、写或执行）	1. 访谈管理员是否制定了访问控制策略 2. 执行语句： mysql>selcec * from mysql.user\G - 检查用户权限列 mysql>selcec * from mysql.db\G -- 检查数据库权限列 mysql>selcec * from mysql.tables_priv\G 一检查用户表权限列 mysql>selcec * from mysql.columns_privi\G - 检查列权限列管理员 输出的权限列是是否与管理员制定的访问控制策略及规则一致 3) 登录不同的用户，验证是否存在越权访问的情形	1 制定数据库访问控制策略，由专门的安全员负责对访问控制权限的授权工作： 2) 各账户权限配置，均是基于安全员的安全策略配置进行的访问控制 3) 无越权访问
	e) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	明确提出访问控制的粒度要求，重点目录的访问控制的主体可能为某个用户或某个进程，应能够控制用户或进程对文件、数据库表等客体的访问	1）执行下列语句： mysql>selcec * from mysql.user\G - 检查用户权限列 mysql>selcec * from mysql.db\G -- 检查数据库权限列 2) 访谈管理员并核查访问控制粒度主体是否为用户级，客体是否为数据库表级	1) 2) 由专门的安全员负责对访问控制权限的授权工作，授权主体为用户，客体为数据库表

	f) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	MySQL不提供该项功能	访谈管理员，是否采用其他技术手段	MySQL不提供该项功能，主要依据操作系统层面实现该项功能
安全审计	a) 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	如果数据库服务器并不执行任何查询，建议启用审计。在/etc/my.cnf 文件的[Mysql] 部分添加：1og,=/var/1og/ my1ogfile 对于生产环境中任务繁重的 MySOL数据库，启用审计会引起服务器的高昂成本，因此建议采用第三方数据库审计产品收集审计记录。应检查数据库系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户登录系统、自主访问控制的所有操作记录、重要用户行为 (如增加 / 删除用户，删除库表) 等。	1) 执行下列语句： mysql>show variables like' log_%' 查看输出的日志内容是否覆盖到所有用户，记录审计记录覆盖内容 2) 核查是否采取第三方工具增强MySQL日志功能。若有，记录第三方审计工具的审计内容，查看是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	1) 数据库本地启用了日志功能，审计内容覆盖到每个用户，能够记录用户行为和重要安全事件 2) 启用审计功能策略为 : 配置了审计日志存储位置，或部署第三方数据库审计产品，审计内容覆盖到所有用户
	b) 审计记录应包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息	应检查数据库系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户登录系统、自主访问控制的所有操作记录、重要用户行为 (如增加 / 删除用户，删除库表) 等	1) 执行下列语句： mysql>show variables like 'log_%' 查看输出的日志内容是否覆盖到所有用户，记录审计记录覆盖内容 2) 核查是否采取第三方工具增强MySQL日志功能。若有，记录第三方审计工具的审计内容，查看是否包括事件的日期和时间、用户、事	1）数据库本地启用了日志功能，审计内容覆盖到每个用户，能够记录重要用户行为和重要安全事件 2) 采用第三方数据库审计产品，审计内容覆盖到每个用户，能够记录重要用户行为和重要安全事件

			件类型、 事件是否成功及其他与审计相关的信息	
	c) 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	应保证只有 root 和 mysql 可以访问这些日志文件，其中，错误日志务必须确保只有 root 和 MySq1可以访问 hostnam'err 日志文件，由于该文件存放在 mysql 数据历史中， 文件包含如口令、地址，表名，存储过程名、代码等敏感信息，易被用于信息收集，并且有可能向攻击者提供利用数据库漏洞的信息 ，攻击者获取安装数据库的服务器的内部数据 : MySQL 日志，应确保只有 root 和 mysq1 可以访问 logfileXY 日志文件， 此文件存放在 mysq1 的历史目录中。因此，应检查 MySQL数据库系统是否对日志进行了权限设置， 非授权人员不能对日志进行操作。另外， 应防止审计日志空间不够而导致无法记录日志的情况发生，并对审计日志进行定期备	1) 访谈管理员对审计话录如何保护，对审计记录是否定期备份， 备份策略 2) 是否严格限制用户访问审计记录的权限	1) 采取了备份、转存等手段对审计记录进行保护， 避免未预期的删除、 修 改或覆盖，数据库本地日志保存时间超过 6 个月 2) 采用第三方数据库审计产 品，审计记录保存时间超过 6 个月

		份，根据《网络安全法》要求，日志应至少保存 6 个月以上		
	d) 应对审计进程进行保护，防止未经授权的中断	应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护；对于 MySQL数据库系统默认符合，但是如果采取了第三方工具，则应检查数据库系统，查看未授权用户是否能中断审计进程	1) 询问是否严格限制管理员、审计员权限 2) 用户重启实例关闭审计功能，查看是否成功	1) 非审计员账户无法中断审计进程，审计进程受到保护 2) 测试其他人员是否可以对审计进程进行开启，关闭操作，并记录

入侵防范	a) 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	直接通过本地网络之外的计算机连接生产环境中的数据库是异常危险的。 有时，管理员会打开主机对数据库的访问： > GRANT ALL ON *.* TO 'root'@'%' 其实是完全放开了对 root 的访问，因此把重要的操作限制给特定主机 异常重要 ： >GRANT ALL ON *.* TO 'root'@'localhost' >GRANT ALL ON *.* TO 'root'@'myip.athome' >FLUSH PRIVILEGES此时，即限制仅允许指定的 P(不管其是否静态) 可以访问	查看用户登录的 IP 地址；是否给所有用户加上 IP 限制，拒绝所有未知主机进行连接 注: 当 user 表中的 Host 值不为本地主机时 ，应指定特定 IP 地址，不应为 %; 或将 user 表中的 Host 值为空，而在 host 表中指定用户帐户允许登陆访问的若干主机； 在非信任的客户端以数据库账户登录应被提示拒绝， 用户从其他子网登录，应被拒绝	配置安全策略为 ：在防火墙上限制特定的终端 (IP) 连接 (访问) 数据库 : 限定的 IP 地址为 :XXXX
	b) 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	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击， 应对系统进行漏洞扫描， 及时发现系统中存在的已知漏洞， 并在经过充分测试评估后更新系统补丁， . 避免遭受由系统漏洞带的风险	访谈 MySQL补丁升级机制， 查看补丁安装情况 ： 1) 执行如下命令查看当前补于版本: show variables where variable name like "version" 2) 访谈数据库是否为企业版， 是否定期进行漏洞扫描， 针对高风险漏洞是否评估补丁并经测试后再进行安装	1) 数据库当前不有在高风险漏洞，补丁更新及时， 记录补丁信息为 : MySQL 数据库补丁定期更新版本 2) 数据库为企业版，定期进行漏洞扫描，在发现数据库漏洞时，必须经测试估后进行漏洞修补

数据备份恢复	a) 应提供重要数据处理系统的热冗余，保证系统的高可用性	任何系统都有可能发生灾难，服务器、MySQL也会崩溃，也有可能遭受入侵，数据有可能被删除。只有为最糟糕的情况做好了充分的准备，才能够在事后快速地从灾难中恢复。用户应把备份过程作为一项日常工作。数据库系统至少提供本地实时备份的功能，当数据发生错误时，能够及时恢复数据	询问系统管理员数据库的备份和恢复策略是什么	备份策略为：对数据库重要数据每天增量备份，每周全量备份： 近期恢复测试时间：每月（季度）定期进行恢复性测试演练
	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	应提供灾备中心，对重要的数据提供异地数据级备份，保证当本地系统发生灾难性后果不可恢复的，利用异地保存的数据对系统数据能进行恢复	1）询问系统管理员是否提供异地数据备份功能，是否定时批量传送至备用场地 2) 如果条件允许，则查看其实现技术措施的配置情况	部署数据备份机房：有异地备份机房，实时（定期）将数据备份到机房

4.6 终端设备测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据

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	用户的身份标识和鉴别，就是用户向操作系统以一种安全的方式提交自己的身份证实，然后由操作系统确认用户的身份是否属实的过程，身份标识要求具有唯一性。在用户进入 Windows 桌面前，如果弹出一个用户登录界面，要求用户输入用户名和密码， Windows 操作系统对用户的用户名和密码进行验证通过后，用户可以登录操作系统。 猜测密码是操作系统最常遇到的攻击方法之 -，因此对操作系统的密码策略提出要求，在 Windows 操作系统中，要求密码历史记录、密码最短长度、密码复杂度等，并要求定期更换	1) 用户需要输入用户名和密码才能登录 2)windows 默认用户名具有唯一性 3) 打开“ 控制面板 ” -》“ 管理工具 ” -》“ 计算机管理 ”一“ 本地用户机组 ”检查有哪些用户，并尝试空口令登录 4) 打开“ 控制面板 ” -》“ 管理工具 ” -》 “ 本地安全策略 ”一》 “ 账户策略 ” “ 密码策略 ”	1) 用户登录需输入用户名和密码 2) 用户具备唯一性 ： 3) 尝试使用空口令登录，未成功 4) 结果如下 ： a) 复杂性要求 ：已启用 ： b) 密码长度最小值 ：长度最小值至少为 8 位 c) 密码长度最长使用期限。不为 0 d) 密码最短使用期限 ：不为 0 e) 强制密码历史 ：至少记住 5 个密码以上
	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	非法用户能够通过反复输入密码，达到猜测用户密码的目的，因此应该限制用户登录过程中连续输入错误密码的次数。 当用户多次输入错误密码后，操作系统应自动锁定该用户或一段时间内禁止该用户登录，从而增加猜测密码难度的目的。 Windows 操作系统具备登录失败处	1) 打开“ 控制面板 ” -》“ 管理工具 ” -》“ 本地安全策略 ”一》 “ 账户策略 ”一》 “ 密码锁定策略 ” 2) 右键点击桌面 -> “ 个性化 ” -> “ 屏幕保护程序 ”，查看“ 等待时间 ”的长短以及“ 在恢复时显示登录屏幕 ”选项是否打钩	1) 结果如下 ： a) 账户锁定时间 ：不为不适用 b) 账户锁定阈值 ：不为不适用 2) 启用了远程登录连接超时并自动退出功能

		理功能，可以通过适当的配置“ 账户锁定策略 ”来对用户的登录进行限制		
	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听	为方便管理员进行管理操作，众多服务器采用网络登录的方式进行远程管理操作， Windows 一般使用“ 远程桌面 (Remote Desktop) ”进行远程管理，《基本要求》 中规定了这些传输的数据需要进行加密处理，目的是为了保障账户和口令的安全	1) 如果是本地管理成 KVM等硬件管理方式，此要求默认满足 2) 如果采用远程管理，则需采用带加密管理的远程管理方式。 在命令行输入 ” pgedit.msc “ 弹出“ 本地组策略编辑器 ” 窗口， 查着“ 本地计算机策略一》计算机配置一 >管理模板一>Windows 组件一选程桌面服务 >远程桌面会话主机 - 安全 ”中的相关项目	1) 本地或 VM，默认符合 2) 远程运维，采取加密的 RDP协议

访问控制	a) 应对登录的用户分配账户和权限	访问控制是安全防范和保护的主要策略，操作系统访问控制的主要任务是保证操作系统资源不该非法使用和访向，使用访问控制的目的在于通过限制用户对特定资源的访问来保护系统资源。在操作系统中的每一个文件或目录都包含有访问权限， 这些访可权限决定了谁能访问和如何访问这些文件和目录。对于操作系统中一些重要的文件，则需要严格控制其访问权限，从而加强系统的安全性。因此，为了确保系统的安全，需要对登录的用户分配账户，并合理配置账户权限。 在 Windows 系统中，重要目录不能对“ everyone". 账户开放， 因为这样会带来很大的安全问题，在权限控制方面，尤其要注意当文件权限更改后对于应用系统的影响	访谈系统管理员， 操作系统能够登录的账户，以及它们拥有的权限。 选 择 %systemdrive%\w indows \system 、%systemroot %\system32\config 等相应的文件夹， 右键选择“ 属性 ”>“ 安全 ”，查 看 everyone 组 、 users 组 和 administrators 组的权限设置	各用户具备最小角色， 分别登录； 不存在匿名用户，默认用户只许可管理员可以登录
	b) 应重命名或删除默认账户，修改默认账户的默认口令	对于操作系统的默认账户， 由于它们的某些权限与实际系统的要求可能存在差异，从而造成安全隐患，因此这些默认账户应重命名或被删除，并修改默认账户的默认口令。 Windows 的系统管理员账户名称就是 Administrator， 在一定环境下，	在命令行输入 "lusrmgr.msc" 弹出“ 本地用户和组 ”窗口，查看 “ 本地用户和组 -> 用户 ”中的相关项目	1 查看右侧列表中 Window 系统的认账 Administrato， 是否枝被禁用或重命名 2) 询问是否已修改默认账户口令 3) 查看是否已经禁用 guest 账户

		黑客可以省略猜测用户名这个步骤，直接破解密码。 因此，允许默认账访问的危害性是显而易见的		
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限	在命令行输入 “ lusmrgr.msc", 弹出“ 本地用户和组 ”窗口，查看“ 本地用户和组一 >用户 ”中的相关项目， 查看右侧用户列表中的用户 ，询问各账户的用途，确认账户是否属于多余的、 过期的账户或共享账户名	不存在多余账户、 测试过期账户。 不存在多部门、多人共享账户情况
入侵防范	a) 应遵循最小安装的原则仅安装需要的组件和应用程序	Windows 默认安装时会开启许多不必要的系统服务，为了避免由于多余的系统服务带来安全风险，通常遵循最小安装原则，仅安装需要的组件和应用程序等。有些操作系统中运行的多余服务和应用程序， 如：存在某台终端作为共享打印机使用	1) 查看和询问安装的组件情况 在命令行输入 "dcomcnfg" ， 打开组件服务界面，打开“ 控制台根节点 ” ->“ 组件服务 ” 一>“ 计算机 ” ->“ 我的电脑 ” . 查看右侧组件列表中的组件内容。询问系统管理员，安装的各组件的用途，有无多余的组件 2) 查看和询问安装的应用程序情况 在命令行输入 "appwiz.cpl, 打开程序和功能界面，查看右侧程序列表中的安装的应用程序 询问系统管理员，安装的应用程序的用途，有无多余的应用程序	1) 系统安装遵循最小化安装原则 2) 不存在业务所不需要的组件和应用程序

	b) 应关闭不需要的系统服务、默认共享和高危端口	Windows 默认安装时会开启许多不必要的系统服务，为了避免由于多余的系统服务带来安全风险，通常可以将其禁用或卸载。 Windows 会开启默认共享， 例如 C$、D$, 为了避免默认共享带来的安全风险，应关闭 Windows 硬盘默认共享。通过查看监听端口，能够直观地发现并对比系统所运行的服务和程序，关闭高危端口，是操作系统常用的安全加固方式	1) 查看系统服务。 在命令行输入 "services. msc “，打开系统服务管理界面，查看右侧的服务详细列表中多余的服务， 如 Alerter 、Remote Registry Servicce Messsenger,Task Scheduler 是否已启动。 2) 查看监听端口。 在命令行输入 "netstat -an ”，查看列表中的监听端口，是否包括高危端口，如 TCP 135、139 、45、 593 、1025 端口， UDP 135、137、 138、445 端口， -些流行病毒的后门端口，如 TCP 2745、3127、 6129 端口。 3) 查看默认共享。 在命令行输入 "net share" ，查看本地计算机上所有共享资源的信息，是否打开了默认共享，例如 C$、D$ 4) 查看主机防火墙策略 在命令行输入 "firewal1. cpl ”打开 Windows 防火墙界面， 查看 Windows 防火墙是否启用。点击左侧列表中的“ 高级设置 ”，打开“ 高级安全 Windows 防火墙 ”窗口。点击左侧列表中的 ” 入站规则 ”，右侧显示 Windows 防火墙的入站规则，查看入站规则中是否阻止访问多余的服务，或高危端口	1) 不存在多余的服务 2) 未启用 不必要的端口 3) 未开启默认共享 4）防火墙规则中阻止访问多余的服务，或高危端口

	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	通过设定终端接入方式、网络地址范围等条件限制终端登录，可以极大的节省系统资源，保证了系统的可用性，同时也提高了系统的安全性。对 Windows 自身来说，可以通过主机防火墙或 TCP/IP 筛选来实现以 上功能	1) 询问系统管理员管理终端的接入方式。 查看主机防火墙对登录终端的接入地址限制 在命令行输入"firewall.cpl ”，打开 Windows 防火墙界面，查看 Windowsd 防火墙是否启用。点击左侧列表中的 “ 高级设置 ”，打开 “ 高级安全 Windows 防火墙 ” 窗口，点击左侧列表中的 “ 入站规则 ”，双击右侧入站规则中的 “ 远程桌面一用户模式 (TCP-In)" ，打开 “ 远程桌面用户模式 (TCP-In) 属性 " 窗口，选择 “ 作用城 ” 查看相关项目。 查看 IP 筛选器对登录终端的接入地址限制 在命令行输入 “ gpedit.msc" 打开本地组策路编辑器界面，点击左侧列表中的 “ 本地计算机策略 -> 计算机配置 Windows 设置 -> 安全设置 ->IP 安全策略 ”，在本地计算机双击右侧限制登录终端地址的相关策略 ” ，查看 “ IP 筛选器列表 ” 和 “ IP 筛选器属性 “ 2) 网络方面对登录终端的接入方式和地址范围的限制 询问并查看是否通过网络设备或硬件防火墙对终端接入方式、网络地址范围等条件进行限	1) 通过主机防火墙设置访问控制规则 2) 通过网络防火墙、堡垒主机限制、ip 段进行接入地址限制

	d) 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	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击，应对系统进行漏洞扫描，及时发现系统中存在的已知漏洞，并在经过充分测试评估后更新系统补丁， . 避免遭受由系统漏洞带的风险	访谈系统管理员是否定期对操作系统进行漏洞扫描，是否对扫描发现的漏洞进行评估和补丁更新测试，是否及时进行补丁更新，更新的方法。 在命令行输入 "appwiz.cp1"， 打开程序和功能界面，点击左侧列表中的“查看已安装的更新”，打开“已安装更新”界面，查看右侧列表中的补丁更新情况	对操作系统补丁进行测试和安装，补丁情况为较新稳定版本
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	作为 Windows 系统，木马和蠕虫的泛滥使得防范恶意代码的破坏显得尤为重一要，因此应采取避免恶意代码攻击的技术措施或采取可信验证技术，如在主机上部署防病毒软件或其他可信验证技术。基于网络和基于主机的防病毒软件在系统上应构成立体的防护结构，属于深层防御的一部分。因此基于网络的防病毒软件的病毒库应与基于主机的防病毒软件的病毒库不同。只有当所有主机都及时更新了病毒库才能够做到防止病毒的入侵。因此应有统一的病毒管理策略，统一更新病毒库，定时查杀，及时发现入侵行为有效阻断等	1) 查看系统中安装的防病毒软件。询问管理员病毒库更新策略。查看病毒库的最新版本更新日期是否超过一个星期 2) 查看系统中采取何种可信验证机制，访谈管理员实现原理等 3) 询间系统管理员网络防病毒软件和主机防病毒软件分别采用什么病毒库 4) 询问系统管理员是否果有统一的病毒更新策略和查杀策略 5) 当发现病毒入侵行为时，如何发现，如何有效阻断等，报警机制等	) 安装有网络版杀毒软件，病毒库最新 2) 查看系统中采取何种可信验证机制，实现原理为基于可信根 TPM技术等 3) 网络版防病毒和主机防病毒均具备不同的病毒库，异构特点 4) 防病毒为网络版，统一更新病毒库 5) 发现病毒入侵，有邮件报警机制

可信验证	可基于可信根对计算设备的系统引导程序、系统程序、 重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	针对终端设备，需要终端在启动过程对预装软件 （包括系统引导程序、系统程序、相关应用程序和重要配置参数）进行完整性验证或检测， 确保对系统引导程序、系统程序、重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1）核查终端的启动 ，是否实现可信验证的过程，查看对那些系统引导程序、系统程序或重要配置参数数进行可信验证 2 修改其中的重要系统程序之 - 和应用程序之 - ，核查是否能够检测到并进行报警 3）是否将验证结果形成审计记录送至安全管理中心	1）终端具有可信根芯片或硬件 2）启动过程基于可信根对引导程序、系统程序、重要配置参数和应用程序等进行可信验证 3) 在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结果记录

4.7 应用系统测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据

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	用户的身份标识和鉴别，就是用户向操作系统以一种安全的方式提交自己的身份证实，然后由操作系统确认用户的身份是否属实的过程，身份标识要求具有唯一性。在用户进入 Windows 桌面前，如果弹出一个用户登录界面，要求用户输入用户名和密码， Windows 操作系统对用户的用户名和密码进行验证通过后，用户可以登录操作系统。 猜测密码是操作系统最常遇到的攻击方法之 -，因此对操作系统的密码策略提出要求，在 Windows 操作系统中，要求密码历史记录、密码最短长度、密码复杂度等，并要求定期更换	1) 用户需要输入用户名和密码才能登录 2)windows 默认用户名具有唯一性 3) 打开“ 控制面板 ” -》“ 管理工具 ” -》“ 计算机管理 ”一“ 本地用户机组 ”检查有哪些用户，并尝试空口令登录 4) 打开“ 控制面板 ” -》“ 管理工具 ” -》 “ 本地安全策略 ”一》 “ 账户策略 ” “ 密码策略 ”	1) 用户登录需输入用户名和密码 2) 用户具备唯一性 ： 3) 尝试使用空口令登录，未成功 4) 结果如下 ： a) 复杂性要求 ：已启用 ： b) 密码长度最小值 ：长度最小值至少为 8 位 c) 密码长度最长使用期限。不为 0 d) 密码最短使用期限 ：不为 0 e) 强制密码历史 ：至少记住 5 个密码以上
	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	非法用户能够通过反复输入密码，达到猜测用户密码的目的，因此应该限制用户登录过程中连续输入错误密码的次数。 当用户多次输入错误密码后，操作系统应自动锁定该用户或一段时间内禁止该用户登录，从而增加猜测密码难度的目的。 Windows 操作系统具备登录失败处	1) 打开“ 控制面板 ” -》“ 管理工具 ” -》“ 本地安全策略 ”一》 “ 账户策略 ”一》 “ 密码锁定策略 ” 2) 右键点击桌面 -> “ 个性化 ” -> “ 屏幕保护程序 ”，查看“ 等待时间 ”的长短以及“ 在恢复时显示登录屏幕 ”选项是否打钩	1) 结果如下 ： a) 账户锁定时间 ：不为不适用 b) 账户锁定阈值 ：不为不适用 2) 启用了远程登录连接超时并自动退出功能

		理功能，可以通过适当的配置“ 账户锁定策略 ”来对用户的登录进行限制		
	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听	为方便管理员进行管理操作，众多服务器采用网络登录的方式进行远程管理操作， Windows 一般使用“ 远程桌面 (Remote Desktop) ”进行远程管理，《基本要求》 中规定了这些传输的数据需要进行加密处理，目的是为了保障账户和口令的安全	1) 如果是本地管理成 KVM等硬件管理方式，此要求默认满足 2) 如果采用远程管理，则需采用带加密管理的远程管理方式。 在命令行输入 ” pgedit.msc “ 弹出“ 本地组策略编辑器 ” 窗口， 查着“ 本地计算机策略一》计算机配置一 >管理模板一>Windows 组件一选程桌面服务 >远程桌面会话主机 - 安全 ”中的相关项目	1) 本地或 VMJ 默认符合 2) 远程运维，采取加密的 RDP协议

访问控制	a) 应对登录的用户分配账户和权限	访问控制是安全防范和保护的主要策略，操作系统访问控制的主要任务是保证操作系统资源不该非法使用和访向，使用访问控制的目的在于通过限制用户对特定资源的访问来保护系统资源。在操作系统中的每一个文件或目录都包含有访问权限， 这些访可权限决定了谁能访问和如何访问这些文件和目录。对于操作系统中一些重要的文件，则需要严格控制其访问权限，从而加强系统的安全性。因此，为了确保系统的安全，需要对登录的用户分配账户，并合理配置账户权限。 在 Windows 系统中，重要目录不能对“ everyone". 账户开放， 因为这样会带来很大的安全问题，在权限控制方面，尤其要注意当文件权限更改后对于应用系统的影响	访谈系统管理员， 操作系统能够登录的账户，以及它们拥有的权限。 选 择 %systemdrive%\w indows \system 、%systemroot %\system32\config 等相应的文件夹， 右键选择“ 属性 ”>“ 安全 ”，查 看 everyone 组 、 users 组 和 administrators 组的权限设置	各用户具备最小角色， 分别登录； 不存在匿名用户，默认用户只许可管理员可以登录
	b) 应重命名或删除默认账户，修改默认账户的默认口令	对于操作系统的默认账户， 由于它们的某些权限与实际系统的要求可能存在差异，从而造成安全隐患，因此这些默认账户应重命名或被删除，并修改默认账户的默认口令。 Windows 的系统管理员账户名称就是 Administrator， 在一定环境下，	在命令行输入 "lusrmgr.msc" 弹出“ 本地用户和组 ”窗口，查看 “ 本地用户和组 -> 用户 ”中的相关项目	1 查看右侧列表中 Window 系统的认账 Administrato， 是否枝被禁用或重命名 2) 询问是否已修改默认账户口令 3) 查看是否已经禁用 guest 账户

		黑客可以省略猜测用户名这个步骤，直接破解密码。 因此，允许默认账访问的危害性是显而易见的		
	c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限	在命令行输入 “ lusmrgr.msc", 弹出“ 本地用户和组 ”窗口，查看“ 本地用户和组一 >用户 ”中的相关项目， 查看右侧用户列表中的用户 ，询问各账户的用途，确认账户是否属于多余的、 过期的账户或共享账户名	不存在多余账户、 测试过期账户。 不存在多部门、多人共享账户情况
入侵防范	a) 应遵循最小安装的原则仅安装需要的组件和应用程序	Windows 默认安装时会开启许多不必要的系统服务，为了避免由于多余的系统服务带来安全风险，通常遵循最小安装原则，仅安装需要的组件和应用程序等。有些操作系统中运行的多余服务和应用程序， 如：存在某台终端作为共享打印机使用	1) 查看和询问安装的组件情况 在命令行输入 "dcomcnfg" ， 打开组件服务界面，打开“ 控制台根节点 ” ->“ 组件服务 ” 一>“ 计算机 ” ->“ 我的电脑 ” . 查看右侧组件列表中的组件内容。询问系统管理员，安装的各组件的用途，有无多余的组件 2) 查看和询问安装的应用程序情况 在命令行输入 "appwiz.cpl, 打开程序和功能界面，查看右侧程序列表中的安装的应用程序 询问系统管理员，安装的应用程序的用途，有无多余的应用程序	1) 系统安装遵循最小化安装原则 2) 不存在业务所不需要的组件和应用程序

	b) 应关闭不需要的系统服务、默认共享和高危端口	Windows 默认安装时会开启许多不必要的系统服务，为了避免由于多余的系统服务带来安全风险，通常可以将其禁用或卸载。 Windows 会开启默认共享， 例如 C$、D$, 为了避免默认共享带来的安全风险，应关闭 Windows 硬盘默认共享。通过查看监听端口，能够直观地发现并对比系统所运行的服务和程序，关闭高危端口，是操作系统常用的安全加固方式	1) 查看系统服务。 在命令行输入 "services. msc “，打开系统服务管理界面，查看右侧的服务详细列表中多余的服务， 如 Alerter 、Remote Registry Servicce Messsenger,Task Scheduler 是否已启动。 2) 查看监听端口。 在命令行输入 "netstat -an ”，查看列表中的监听端口，是否包括高危端口，如 TCP 135、139 、45、 593 、1025 端口， UDP 135、137、 138、445 端口， -些流行病毒的后门端口，如 TCP 2745、3127、 6129 端口。 3) 查看默认共享。 在命令行输入 "net share" ，查看本地计算机上所有共享资源的信息，是否打开了默认共享，例如 C$、D$ 4) 查看主机防火墙策略 在命令行输入 "firewal1. cpl ”打开 Windows 防火墙界面， 查看 Windows 防火墙是否启用。点击左侧列表中的“ 高级设置 ”，打开“ 高级安全 Windows 防火墙 ”窗口。点击左侧列表中的 ” 入站规则 ”，右侧显示 Windows 防火墙的入站规则，查看入站规则中是否阻止访问多余的服务，或高危端口	1) 不存在多余的服务 2) 未启用 不必要的端口 3) 未开启默认共享 4）防火墙规则中阻止访问多余的服务，或高危端口

	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	通过设定终端接入方式、网络地址范围等条件限制终端登录，可以极大的节省系统资源，保证了系统的可用性，同时也提高了系统的安全性。对 Windows 自身来说，可以通过主机防火墙或 TCP/IP 筛选来实现以上功能	1) 询问系统管理员管理终端的接入方式。 查看主机防火墙对登录终端的接入地址限制 在命令行输入"firewall.cpl"，打开 Windows 防火墙界面，查看 Windowsd 防火墙是否启用。点击左侧列表中的“高级设置”，打开“高级安全 Windows 防火墙”窗口，点击左侧列表中的“入站规则”，双击右侧入站规则中的“远程桌面一用户模式 (TCP-In)"，打开“远程桌面用户模式 (TCP-In) 属性"窗口，选择“作用城”查看相关项目。 查看 IP 筛选器对登录终端的接入地址限制 在命令行输入“gpedit.msc" 打开本地组策路编辑器界面，点击左侧列表中的“本地计算机策略 -> 计算机配置 Windows 设置 -> 安全设置->IP 安全策略”，在本地计算机双击右侧限制登录终端地址的相关策略”，查看“IP 筛选器列表”和“ IP 筛选器属性“ 2) 网络方面对登录终端的接入方式和地址范围的限制 询问并查看是否通过网络设备或硬件防火墙对终端接入方式、网络地址范围等条件进行限	1) 通过主机防火墙设置访问控制规则 2) 通过网络防火墙、堡垒主机限制、ip 段进行接入地址限制

	d) 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	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击，应对系统进行漏洞扫描，及时发现系统中存在的已知漏洞，并在经过充分测试评估后更新系统补丁， .避免遭受由系统漏洞带的风险	访谈系统管理员是否定期对操作系统进行漏洞扫描，是否对扫描发现的漏洞进行评估和补丁更新测试，是否及时进行补丁更新，更新的方法。 在命令行输入 "appwiz.cp1"， 打开程序和功能界面，点击左侧列表中的“查看已安装的更新”，打开“已安装更新”界面，查看右侧列表中的补丁更新情况	对操作系统补丁进行测试和安装，补丁情况为较新稳定版本
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	作为 Windows 系统，木马和蠕虫的泛滥使得防范恶意代码的破坏显得尤为重一要，因此应采取避免恶意代码攻击的技术措施或采取可信验证技术，如在主机上部署防病毒软件或其他可信验证技术。基于网络和基于主机的防病毒软件在系统上应构成立体的防护结构，属于深层防御的一部分。因此基于网络的防病毒软件的病毒库应与基于主机的防病毒软件的病毒库不同。只有当所有主机都及时更新了病毒库才能够做到防止病毒的入侵。因此应有统一的病毒管理策略，统一更新病毒库，定时查杀，及时发现入侵行为有效阻断等	1) 查看系统中安装的防病毒软件。询问管理员病毒库更新策略。查看病毒库的最新版本更新日期是否超过一个星期 2) 查看系统中采取何种可信验证机制，访谈管理员实现原理等 3) 询间系统管理员网络防病毒软件和主机防病毒软件分别采用什么病毒库 4) 询问系统管理员是否果有统一的病毒更新策略和查杀策略 5) 当发现病毒入侵行为时，如何发现，如何有效阻断等，报警机制等	) 安装有网络版杀毒软件，病毒库最新 2) 查看系统中采取何种可信验证机制，实现原理为基于可信根 TPM技术等 3) 网络版防病毒和主机防病毒均具备不同的病毒库，异构特点 4) 防病毒为网络版，统一更新病毒库 5) 发现病毒入侵，有邮件报警机制

可信验证	可基于可信根对计算设备的系统引导程序、系统程序、 重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	针对终端设备，需要终端在启动过程对预装软件 (包括系统引导程序、系统程序、相关应用程序和重要配置参数) 进行完整性验证或检测， 确保对系统引导程序、系统程序、重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1）核查终端的启动 ，是否实现可信验证的过程，查看对那些系统引导程序、系统程序或重要配置参数数进行可信验证 2 修改其中的重要系统程序之 - 和应用程序之 - ，核查是否能够检测到并进行报警 3）是否将验证结果形成审计记录送至安全管理中心	1）终端具有可信根芯片或硬件 2）启动过程基于可信根对引导程序、系统程序、重要配置参数和应用程序等进行可信验证 3) 在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4) 安全管理中心可以接收设备的验证结果记录

五、安全管理中心测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作行为进行审计	要求对系统管理员进行身份认证并严格限制系统管理员账户的管理权限，仅允许系统管理员通过特定方式进行系统管理操作，并对所有操作进行详细的审计记录	1) 应核查是否对系统管理员进行身份鉴别 2) 应核查是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作 3 应核查是否对系统管理操作进行审计	1) 对管理员的登录进行认证 2) 使用了管理工具或特定命令 3) 所有操作有日志记录
	b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户的身份、系统资源配置、系统加载和启动，系统运行的异常处理、数据和设备的备份与恢复等	系统管理操作应由管理员完成，其管理、操作内容应不同于审计管理员和安全管理员	应核查是否通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、、系统资源配置、系统加载和启动，系统运行的异常处理、数据和设备的备份与恢复等	1) 管理员有权限划分 2) 权限不同于审计管理员和安全管理员
审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面	要求对审计管理员进行身份认证并严格限制审计管理员账户的管理权限，仅允许管理员通过特定	1) 应核查是否对审计管理员进行身份鉴别 2) 应核查是否只允许审计管理	1) 对管理员的登录进行认证 2）使用了管理工具或特定命令 3) 所有操作有日志记录

	进行操作，并对这些操作进行审计	方式进行审计管理操作，并对所有操作进行详细的审计记录	员通过特定的命令或操作界面进行安全审计操作 3) 应核查是否对安全事代操作进行审计	
	b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储，管理和查询等	针对综合安全审计系统、数据库审计系统等提供集中审计功能的系统，要求对审计管理员进行授权，并通过审计管理员对审计记录应进行分析	应核查是否通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等	1) 管理员有权限划分 2) 权限不同于系统管理员和安全管理员 3) 只有审计管理员可以查看审计分析数据
安全管理	a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作行为进行审计	要求对安全管理员进行身份认证并严格限制系统管理员账户的管理权限，仅允许安全管理员通过特定方式进行系统管理操作，并对所有操作进行详细的审计记录	1) 应核查是否对安全管理员进行身份鉴别 2) 应核查是否只允许安全管理员通过特定的命令或操作界面进行系统管理操作 3 应核查是否对安全管理操作进行审计	1 对管理员的登录进行认证 2) 使用了管理工具或特定命令 3) 所有操作有日志记录
	b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等	针对提供集中安全管理功能的系统，要求对安全管理员进行授权，并通过安全管理员部署安全组件或安全设备的安全策略	应核查是否通过安全管理员对系统中的安全策略进行配置，包括安全参数、主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等	1) 管理员有权限划分 2) 权限不同于系统管理员和审计管理员： 3) 只有安全管理员可以配置安全策略有关的参数

集中管控	a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控	应在网络中独立配置一个网络区域，用于部署集中管控措施。 集中管控措施包括 ：集中监控系统、 集中审计系统和集中安管系统等，通过这些集中管控措施实现对整个网络的集中管理	1) 应核查是否划分出单独的网络区域用于安全管理 2) 应核查是否各个安全设备或安全组件的配置等管理均由管理区的设备进行	1) 网络拓扑图中有管理区 2) 安全设备或组件的管理设备均在管理区
	b) 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	为了保障网络中信息传输的安全性，应采用安全方式对设备或安全组件进行管理	应核查是否采用安全方式 （如SSH、HTTPS IPSec VPN等）对安全设备或安全组件进行管理，或者是否使用独业的带外管理网络对安全设备或安全组件进行管理	采用安全方式对设备进行访问，并对配置信息进行记录，例如 ：ssh server enable ssh user cssnet service-type stelnet authentication-type password
	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	为了保障业务系统的正常运行，应在网络中部署具备运行状态监测功能的系统或设备，对网络链路、网络设备、 安全设备、 服务器及应用系统的运行状态进行 集中、实时监控	1) 应核查是否部署了具备运行状态监测功能的系统或设备，能够对网络链路、安全设备 1) 网络设备和服务器等的运行状况进行集中监测 2) 应测试验证运行状态监测系统是否根据网络链路、安全设备、网络设备和服务器等的工作状态、依据设定的阀值 （或默认阀值）实时报警	具备设备检测功能的系统或平台

	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	部署集中审计分析系统，实现对基础网络平台及其上运行的各类型设备进行信息日志收集、存储，并定期进行审计分析，从而发现潜在的安全风险。日志存储时间应符合法律法规要求，目前网络安全法要求日志保存时间不少于 6 个月	1) 应核查各个设备是否配置并启用了相关策略，将审计数据发送到独立于设备自身的外部集中安全审计系统中 2) 应核查是否部署统一的集中安全审计系统，统一收集和存储各设备日志，并根据需要进行集中审计分析 3) 应核查审生记录的留带时间是否为 6 个月	1）设备日志进行了转发 2) 平台具备审计分析功能 3) 审计记录保有了至少 6 个月以上
	e) 应对安全策略，恶意代码、补丁升级等安全相关事项进行集中管理	在安全管理区域部署集中管理措施，应实现对各类型设备（如：防火墙、IPS、IDS. WAF 等）安全策略的统一管理，应实现对网络恶意代码防护设备、主机操作系统恶意代码防护软件、病毒规则库的统一升级，应实现对各类型设备（如：主机操作系统、数据库操作系统等）的补丁升级进行集中管理等	1) 应核查是否能够对安全策略（如防火墙访问控制策略、入侵保护系统防护策略、WAF安全防护策略等）进行集中管理 2) 应核查是否实现对操作系统防恶意代码系统及网络恶意代码设备的集中管理 3）实现对防恶意代码病毒规则库的统一升级和管理	1）具有统一策略管理平台或多个（比如防火墙、IPS、IDS. WAF 等安全设备）分别策略管理的工具 2) 通过平台或工具可以实施策略管理
	f）应能对网络中的各类安全事件进行进行识别、报警和分析	能够通过集中管控措施，对基础网络平台范围内各类安全事件（如设备故障、恶意攻击、服务性能下降等）进行实时的识别和分析，并通过声、光、短信、邮件等措施进行实时报警	1) 应核查是否部署了相关系统平台够对各类安全事传进行分析并通过声、光等方式实时报警 2) 应核查监测范围是否能够覆盖网络所有可能的安全事件	1) 具有安全事件管理平台或工具 2) 相关平台或工具收集足够的可能安全事件，并具备报警提示功能

六、安全管理制度测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等	网络安全工作的总体方针和安全策略文件作为机构网络安全工作的总纲，一般明确了网络安全工作的总体目标、原则、需遵循的总体策略等内容。可以以单一的文件形式发布，也可与其他相互关联的文件作为一套文件发布	1) 核查是否具有总体方针和策略文件 2) 核查该文件是否明确了机构安全工作的总体目标，范围、原则和各类安全策略。 -般来讲，该策略文件中可以明确网络安全管理活动的责任部门或人员、也可覆盖到等级保护对象生命周期中所有关键的安全管理活动。其中安全管理框架应包括组织机构及岗位职责，人员安全管理、环境和资产安全管理、系统安全建设管理系统安全运行管理、事件处置和应急响应等方面，明确各个方面的职责分工，需要关注的管理活动、管理活动的控制方法等	1) 机构具有网络安全方针和策略文件 2) 文件明确了机构网络安全工作的总体目标、范围、原则和安全策略
管理制度	a) 应对安全管理活动中的各类管内容中建立安全管理制度	具体的安全管理制度在安全方针策略文件的基础上，根据实际情况建立。可以由若干的制度构成，或若于个分册构成。可能覆盖机房安全管理、办公环境安全管理、网络和系统安全管理供应商管理、变更管理、备份和恢复管理、软件开发	1）核查是否有安全管理制度 2) 核查制度是否覆盖机构和人员、物理和环境、安全建设和安全运维等层面的管理内容	1) 建立了安全管理制度 2) 安全管理制度覆盖了物理和环境、机构和人员、安全系统建设和安全运维等层面的管理内容

		管理等方面，可以在每个制度文档中明确该制度的使用范围、目的、需要规范的管理活动、具体的规范方式和要求		
	b) 应对管理人员或操作人员执行的日常管理操作建立操作规程	安全操作规程是指各项具体活动的步骤或方法，可以是一个操作手册，一个流程表表单或一个实施方法，但必须能够明确体现或执行网络安全策略或网络安全所要求的策略或原则。配置规范指的是重要等级保护对象中部署的关键网络安全设备、主机操作系统、数据库管理系统等的安全配置规范。这些操作设备和安全配置规范可以应用于那些需要安装或配置计算机的用户。许多组织机构都应有书面规程规定应该如何安装操作系统，如何建立新用户账户，如何分配计算机权限，如何进行事件报告等等	核查是否具有日常管理操作规程，如系统维护手册和操作规程等（包括网络设备、安全设备、操作系统等的配置规范）	1）具有日常管理操作的操作规程 2) 操作规程覆盖了物理环境、网络和通信、设备和计算、应用和数据层面的重要操作规程（如系统维护手册和操作规程）

	c) 应形成由安全策略、管理制度、操作规程，记录表单等构成的全面的安全管理制度体系	全面的安全管理制息体系包括网络安全工作的总体方针策略、各种安全管理活动的管理制度、日常操作行为的操作规程以及各类记录表单共同构成“金字塔”式结构	1) 核查是否具有总体方针策略文件、管理制度，操作规程和记录表单等 2) 核查管理体系各要素之间是否具有连贯性 一般情况下，一套全面的安全管理制度体系最常见的为 4 层架构，即由网络安全工作的总体方针策略，各种安全管理活动的管理制度、日常操作行为的操作规程和安全配置规范和各类记录表单	1) 具有各项管理制度 2) 内容覆盖全面，由总体方针、安全策略、管理制度、操作规程等构成，形成了全面的网络安全管理制度体系
制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定	安全管理制度的制定和发布，应在相关部门的负责和指导下，严格按照制度制定的有关程序和方法，规范起草、论证、审定和发布等主要环节	1) 访谈安全主管或配合人员，询问由什么部门或人员负责安全管理制度的制定，参与制定人员有哪些 2) 核查人员职责、岗位设置等相关管理制度文件，或者是否明确由专门的部门或人员负责安全管理制度的制定工作	1) 有指定部门或人员负责安全管理制度的制定 2) 相关职责文件明确了由专门的部门或人员负责安全管理制度的制定工作

	b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制	正式、有效的发布方式，原则是机构所认可的有效的发布方式，且在有效范围内由相关部门发布即可，如：正式发文发布、内部 OA发布、邮件发布、即时通讯发布等方式，不必拘泥具体的形式。	1 核查制度制定和发布要求管理文档是否说明安全管理制度的制定和程序，格式要求及版本编号等相关内容 2) 核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导签署和单位盖章等，是否注明发布范围	1) 具有制度制定和发布要求的管理文档 2) 文档内容覆盖安全管理制度制定和发布程序 3) 各项安全管理制度文档都是通过正式、有效的方式发布的，如具有版本标识和管理层的签字或单位盖章
评审和修订	a) 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订	安全管理制度的定期评审和修订主要考虑：制度体系整体性是否合理；体系各要素（如安全策略、管理制度或操作规程等）是否合理	1) 访谈信息 / 网络安全主管是否定期对安全管理制度体系的合理性和适用性进行审定 2) 核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度 安全管理制度体系涉及从上层方针到管理制度再到操作规程等整个单位等保护对象安全相关的所有文件，这里的定期一般可以为一年，具体可根据组织情况进行约定，但是，一旦发生可能引起安全管理制度不适用的事件时应该主动对安全管理制度进行检查和审定，发现不足及时修订	1) 具有安全管理制度的核查或评审记录 2) 如果有修订版本，具有修订版本的安全管理制度，修订内容与评审记录中保持一致

七、安全管理机构测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
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	为保证安全管理工作的有效实施，应设立指导和管理网络安全工作的委员会或领导小组，负责单位网络安全管理的全局工作，是网络安全组织的最高管理层	1) 访谈信息 / 网络安全主管是否成立了指导和管理网络安全工作的委员会或领导小组 2) 核查部门职责文档是否明确了网络安全工作委员会或领导小组构成情况和相关职责 3) 核查相关委任授权文件是否明确其最高领导由单位主管领导委任或授权 一般情况下，一个机构成立了指导和管理网络安全工作的委员会或领导小组，均需有正式的发文 通常，在单位的内部结构上建立一整套从单位最高管理层（网络安全领导小组并且由单位最高领导委任或授权）到执行管理层（网络安全管理工作职能部门及安全主管）以及系统日常运营层（系统管理员、网络管理员、安全管理员等）的三层及金字塔式的管理结构来约束和保证各项安全管理措施的执行。网络安全领导小组主要的职责包括对安全管理制度体系合理性和适用性的审定、对机构内关键网络安全工作进行授权和审批等，但其最主要的是负责单位网络安全管理的全局工作：网络安全管理职能部门的主要职责是对机构内重要网络安全管理工作的授权和审	1) 机构成立了网络安全工作委员会或领导小组，且有明确的文件明确其组成机构及工作职责 2) 具有由单位主管领导委任或授权的相关文件

			批、内部相关业务部门和安全管理部门之间的沟通协调以及与机构外部单位的合作、定期对系统的安全措施落实情况进行检查，以便发现问题进行改进等	

	b) 应设立网络安全管理工作的职能部门， 设立安全主管、安全管理各个方面的负责人岗位， 并定义各负责人的职责	网络安全管理工作的职能部门是机构的执行管理层，一般负责对网络安全管理工作的授权和审批， 内部相关业务部门和安全管理部门之间的沟通协调以及与机构外部单位的合作， 定期对系统的安全措施落实情况进行检查， 系统安全运行维护管理工作	1) 访谈信息 / 网络安全主管，是否设立了网络安全管理职能部门和各方面负责人 (如机房负责人、系统运维负责人，系统建设负责人等) 2) 核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责 “ 安全主管 “ 一般是一个单位安全管理工作的主要责任人，全面负责等级保护对象安全规划、 建设、 运行维护等安全管理工作， 一般由单位的高层或某一部门的主管担任。 “ 安全管理各方面的负责人 ” 一般包括物理安全负责人 (其是保护等级保护对象物理进行环境和办公环境安全的责任人） ，系统建设方面负责人 (其是保证等级保护对象安全规划、建设、工程实施过程的责任人) 和系统运行维护方面的责任人 (其是保证等级保护对象日常运行安全的责任人) 等	1) 机构设立了网络安全管理职能部门，并指定了各部门负责人 2) 具有明确的职责文件明确部门和负责人的工作职质
	c) 应设立系统管理员、审计管理员和安全管理员等岗位， 并定义部门及各个工作岗位的职责	系统管理员、网络管理员、安全管理员等为机构的日常运营层， 主要负责具体落实各项网络安全等级保护工作具体要求， 负责日常的具体安全维护工作	1) 访谈信息 / 网络安全主管是否设立了系统管理员、网络管理员和安全管生员等岗位 2) 核查岗位职责文档是否明确了各岗位职责	机构设立了系统管理员、 网络管理员、 安全管理员岗位，且具有明确的各部门职责说明文档

人员配备	a) 应配备一定数量的系统管理员、 审计管理员和安全管理员等	由于部分岗位人员拥有关键的操作权限， 为避免人员失误或渎职现象的发生，应配备一定数量的安全管理人员， 如系统管理员、审计管理员和安全管理员等	1) 访谈信息 / 网络安全主管各个安全管理岗位人员配备情况 2) 核查管理人员名单，查看其是否明确机房管理员、 系统管理员、 网络管理员、 安全管理员等重要岗位人员的信息 . 3) 与技术核查结合，各个岗位是否根据管理人员名单予以授权，如主机核查时系统管理员是否和管理人员名单一致	1) 人员配备文档中明确了各岗位人员的配备人员及数量 2) 管理人员名单中明确机房管理员、系统管理员、网络管理员、 安全管理员等重要岗位人员的信息 3) 各个岗位根据管理人员名单任职
	b) 应配备专职的安全管理员，不可兼职	安全管理员不能兼任其他与等级保护对象相关的管理岗位， 如系统管理员、网络管理员等	1）访谈安全主管，询问安全管理员的配备情况，是否是专职 2) 核查管理人员名单，确认安全管理员是否是专职人员	人员配备文档表明安全管理员没有兼任系统管理员、 网络管理员等
授 权 和 审 批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等	通过对部门和岗位职责的描述， 应能明确指出部门或岗位可以进行审批的事项内容	1) 访谈安全主管，询问对哪些等级保护对象活动进行审批， 审批部门是什么部门， 审批人是什么岗位 2) 核查部门职责文档是否明确各部门的审批事项和审批岗位 3) 核查岗位职责文档是否明确各岗位的审批事项 4) 核查审批记录，是否与相关职责文件描述一致。	1) 部门和各岗位的职责文件中包含了相关事项的审批描述 2) 审批记录和相关职责文件描述一致

	b) 应针对系统变更、 重要操作、物理访问和系统接入等事项建立审批程序，按审批程序执行审批过程， 对重要活动建立逐级审批制度	相关的管理制度文档中一般对系统变更 （如变更管理制度 ） ．物理访问（如机房管理制度 ）、系统接入（如网络管理制度 ）等重要活动明确审批流程，包括逐级审批流程。另外，要求保存审批过程记录文档， 并要求保证执行中的审批程序、 宙批部门及批准人与审批制度文档中规定的一致性	1) 访谈安全主管，询问其对重要活动的审批范围（如系统变更、重要操作、物理访问和系统接入、 重要管理制度的规定和发布， 人员的配备和培训、产品的采购、外部人员的访问等），审批程序如何， 其中哪些事项需要逐级审批 2) 核查系统变更、 重要操作、 物理访问和系统接入等事项的相关管理制度是否明确相关操作的逐级审批程序 3) 核查经逐级审批的记录，查看是否具有各级批准人的签字和审批部门的盖章，是否与相关制度一致 系统变更， 一般分为重大变更和普通变更， 前者如系统运行业务改变或系统核心设备更换等，后者如点如系统或设备配置更改等； 重要操作， 如设备加电或断电等； 物理访问主要指对机房或重要办公区域的访问； : 系统接入一般指外部系统或网络接入等级保护对象 逐级审批活动的重要程度可以是从执行管理层（安全主管、负责人 ）到运营层 （ 各管理员 ）的二级审批，也可以是从最高层 （网络安全领导小组 ）到执行管理层再到运营层的三级审批。	1 相关管理制度中明确了系统变更、 物理访问和系统接入等重要操作的审批流程 2) 具有相关事项的审批记录 3 逐级审批的记录， 具有各级批准人的签字和审批部门的盖章，与相关制度一致

	c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批等信息	审批事项可能会根据审批部门变更、审批人变更以及相关审批流程发生变更，因此需要及时根据实际情况变化进行审查并更新相关内容。另外需定期对相关审批事项进行审查，以更新需要更新的相关信息	1 访谈信息 / 网络安全主管对各类审批事项进行更新 2) 核查是否具有对相关审批事项的定期审查记果和授权更新记录 需要形成审批事项列表，在该列表中明确审批事项、涉及的审批部门、批准人等，并要求定期对该列表进行更新维护，如部门职责或岗位职责改变则某 - 审批活动涉及的审批部门和批准人则会改变，活动的重要程度改变则该活动的审批流程也会改变等	具有定期审查审批事项的记录和授权更新记录
沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作，定期召开协调会议，共同协作处理网络安全问题	一个单位的等级保护对象运行可能涉及到多个业务部门，因此，为保障整个等级保护对象安全工作的顺利完成，需要各业务部门的共同参与和密切配合。此处沟通方式的要求，要求采取例会或不定期召开会议的形式进行网络安全问题处理	1) 访谈信息 / 网络安全主管，是否建立了各类管理人员之间、组织内部机构之间以及网络安全职能部门内部的合作与沟通机制 2) 核查相关会议记录，是否涵盖安全相关内容。其中，针对组织内部机构之间以及网络安全职能部门内部的安全工作会议文件或会议记录，查看是否具有会议内容、会议时间、参加人员和会议结果等描述，是否具有安全管理委员会或领导小组安全管理工作执行清况的文件或工作记录 (如会议记录 / 纪要，网络安全工作决策文档等）	1) 内部机构之间网络安全职能部门内部建立了相相关沟通交流机制 2) 具有定期召开会议的记录

	b) 应加强与网络安全职能部门、 各类供应商、 业界专家及安全组织的合作与沟通	与外界各类单位、 部门的沟通与合作机制可能有多种方式，如与网络管理部门定期汇报、检查工作，与供应商定期会议商讨系统中的安全问题， 与业界专家进行安全评审咨询等方式	1) 访谈信息 / 网络安全主管 ，是否建立了与网络安全管理部门、 各类供应商、 业界专家及安全组织的合作与沟通机制 2) 核查相关沟通合作记录，是否具有与网络安全管理部门、 各类供应商、 业界专家沟通交流的记录	1）与网络安全管理部门、各类供应商、业界专家及安全组织的合作与沟通机制 2）具有日常沟通交流的记录和文件
	c) 应建立外联单位联系列表，包括外联单位名称、合作内容、 联系人和联系方式等信息	与外联单位的联系应建立联系列表并根据实际情况维护更新列表信息、明确合作内容以及联系人等相关的信息	核查外联单位联系列表，是否记录外联单位名称、合作内容、联系人和联系方式等信息	具有外联单位联系列表，且包括外联单位名称、合作内容、联系人和联系方式等信息
审核和检查	a) 应定期进行常规安全检查，检查内容包括系统日常运行、 系统漏洞和数据份等情况	常规的安全检查不同于日常的安全巡检， 常规的安全检查一般是半年， 一年或者每季度开展， 汇总一段时间内的系统状态	1) 访谈信息 / 网络安全主管是否定期进行了常规安全核查 2) 核查常规安全核查记录是否包括了系统日常运行	系统漏洞和数据备份等情况	1) 定期 (如每月或每季度) 进行安全检查 ，检查内容涵盖系统日常运行状态、 数据备份、 漏洞检查等内容 2) 具有相关的检查记录
	b) 应定期进行全面安全检套，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、 安全管理制度的执行情况等	全面的安全检查可自行组织或通过第三方机构进行， 无论哪种方式， 检查内容均应涵盖技术和管理各方面安全措施的落实情况， 如果是单位内部进行的全面安全检查相当于对等级保护对象	1) 访谈信息 / 网络安全主管，是否定期进行了全面安全核查，核查内容都有哪些 2) 核查全面安全核查记录类文档， 是否包括了现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等	1) 定期开展全面安全检查，检查内容覆盖技术有效性和管理措施落地执行情况等 2）具有全面安全检查记录

		安全的自评估。 定期可以是半年一次也可以是一年一次		
	c) 应制定安全检查表格实施安全， 汇总安全检查数据，并对安全检查结果进行通报	无论是日常检查还是定期全面的安全检查都需要制定安全检查格 ，记录全面检查结果， 并形成安全检查报告， 同时也要求将安全检查结果通知给相关人员， 尤其是运营层的各岗位管理员	1) 访谈安全管理员，询问是否制定安全核查表格实施安全检查 ，是否对检查结果进行通报 2) 核查安全检查表格， 安全检查记录， 安全检查报告等文档， 是否具有安全检查表格、 安全检查记录、 安全检查报告， 安全检查结果通报记录 3) 核查安全检查报告，查看报告日期与检查周期是否一致， 报告中是否具有检查内容、 检查时间、 检查人员， 检查数据汇总表、 检查结果等的描述	1）具有安全检查表格，安全检查记录，安全检查报告等文档 2）安全检查报告日期与检查周期一致， 报告中具有检查内容、 检查时间、 检查人员， 检查数据汇总表、检查结果等的描述

八、安全管理人员测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
人员录用	a) 应指定或授权专门的部门或人员负责人员录用	对员工的安全要求应该从聘用阶段就开始实施，无论是长期聘用的员工还是合同员工、 临时员工， 都应在员工的聘用合同中明确说明员工在网络安全方面应遵守的规定和应承担的安全责任，并在员工的聘用期内实施监督机制。为保证人员录用过程的规范，应明确专门的部门和人员负责	访谈信息 / 网络安全主管是否由专门的部门或人员负责人员的录用工作	1) 具有相关的职能部门专门负责人员录用工作 2) 具有明确规定负责人员录用工作的部门或人员的制度
	b) 对被录用人员的身份，安全背景， 专业资格或资质等进行审查，对其所具有的技术技能进行考核	聘用员工时， 应充分饰选、 审查，特别是那些可能接触敏感信息的员工，需要进行包括身份、 背景，专业资格和资质方面的审查和技术技能的考核	1 核查人员安全管理文档是否说明录用人员应具备的条件 （如学历要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等） 2) 核查是否具有人员录用时对录用人身份、背景、 专业资格和审查的相关文档或记录，是否记录审查内容和审查结果等 3) 核查人员录用时的缺技能考核文档或记录，是否记录考核内容和考核结果等	1) 人员录用管理文档说明了不同岗位录用人员的条件。 2) 具有人员录用的审查记录 3) 具有人员录用的技能考核记录

	c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议	保密协议面向所有被录用人员，岗位安全协议则主要面向关键岗位，并根据岗位不同约束各自在岗位上的安全责任	1) 核查保密协议，所有录用人员是否签署保密协议，明确保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容 2) 核查岗位安全协议文档，关键岗位是否签署岗位安全协议，明确岗位女全责任、协议的有效期限和责任人签字等内容 关键岗位的人员主要是指涉及到本单位核心业务或者核心技术的岗位人员，包括从事系统安全管理的安全管理员、系统管理员、 网络管理员等。 岗位安全协议不同于保密协议， 其与岗位职责有关， 主要在协议中明确如果未履行岗位职责或因失职而引发安全事件应该承担的安全责任	1) 具有相关人员签字的人员保密协议，明确保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容 2）具有关键岗位人员签字的岗位责任协议， 明确岗位安全责任、 协议的有效期限和责任人签字等内容
人员离岗	a) 应及时终止离岗人员的所有访问放限，取回各种身份证、 钥匙、徽章等以及机构提供的各种软硬件设备	解雇、 退休、 辞职、 合同到期或其他原因离开单位或离岗的人员在离开前都必须到相应管理部门办理严格的调离手续，包括交回其拥有的相关证件、 徽章、密钥、访问控制标识、单位配给的设备等	1) 访谈人事负责人，询问是否及时终止离岗人员的所有访问权限。取回各种身份证件、 钥匙、 徽章等以及机构提供的软硬件设备 2) 核查人员离岗记录文档，是否具有离岗人员终止其访问权限，交还身份证件、软硬件设备等的登记记录	具有离岗人员交还各类资产的登记记录

	b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开	调离后的保密承诺可单独签署，或者在保密协议中有相关条款明	1）核查人员离岗的管理文档是否规定了人员调离手续和离岗要求 2) 核查是否具有按照离岗程序办理调离手续的记录 3) 核查保密承诺文档是否有调离人员的签字	1）具有相关规范人员调离手续要求的管理文档 2) 具有相关人员调离手续的记录 3) 具有调离人员签字的保密承诺文档
安全意识教育和培训	a) 应对各类人员进行安全意识教育和机构技能培训 ，并告知相关的安全责任和惩戒措施	安全意识教育和培训是对人员的安全意识、 安全技能等方面进行提高的手段之一，保证人员具有与其岗位职责相适应的安全技术能力和管理能力，以减少人为操作失误给系统带来的安全风险	1) 访谈安全主管，询问是否对各类人员(普通用户、 运维人员、 单位领导等) 进行安全教育、岗位技能和安全技术培训 2) 核查网络安全教育和技能培训文档，是否明确培训周期、培训方式 培训内容和考核方式等相关内容 3) 核查安全责任和惩戒措施管理文档是否包含具体的安全责任和惩戒措施	1) 有相关文档明确要求对人员进行安全意识教育和岗位技能培训 2）具有网络安全教育和技能培训文档，明确培训周期、 培训方式 培训内容和考核方式等相关内容 3 具有相关文档明确安全责任和惩戒措施
	b) 应针对不同岗位制定不同的培训计划 ，对安全基础如识、岗位操作规程等进行培训	针对不同岗位需要不同的培训的计划，培训计划一般在年初制定本季度规划或者年末制定下年的计划，由各个部门制定自己部门的计划后汇总至培训主管部门	1) 访谈安全主管，询问是否针对不同的岗位制定不同的计划，并按照计划对各个岗位人员进行安全救育和培训 2) 核查安全教育和培训文档，查看是否明确规定应进行安全教育和培训 3) 核查是否具有不同岗位的培训计划，查看培训内容是否包含网络安全基础知识、岗位操作规程等 4) 核查安全教育和培训记录是否有培训人员、培训内容、培训结果等的描述	1) 具有安全教育和培训管理文档， 明确规定应进行安全教育和培训 2) 具有针对不同岗位人员的培训计划 3) 具有相关培训记录

	c) 应定期对不同岗位的人员进行技能培训	安全技能考核不同于工作考核，主要注重岗位人员是否具有胜任该岗位所需技能的能力	1) 访谈安全主管，询问对各个岗位人员是否定期进行安全技能，考核周期多长，考核内容有哪些 2) 核查考核记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等，查看记录日期与考核周期是否一致	具有定期的各岗位人员技能考核记录，记录的考核人员包括各个岗位的人员，考核内容包含安全知识、安全技能等，记录日期与考核周期一致
外部人员访问管理	a) 应在外部人员物理访问受控区前先提出书面申请，批准后由专人全程陪同，并登记备案	外部人员访问受控区域需要经相关人员批准并进行有效控制	1) 核查外部人员访问管理文档，是否明确允许外部人员访问的范围，外部人员进入的条件、外部人员进入的访问控制措施等 2) 核查外部人员访问重要区域的书面申请文档是否具有批准人允许访问的批准签字等 3) 核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等	1) 相关管理文档明确了外部人员物理访问受控区域的要求 2) 具有相关申请并批准进入的记录 3) 具有外部人员访问受控区域的相关登记记录
	b) 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	外部人员存在接入受控网络的情况，需严格控制并采取相关的管理措施	1) 核查外部人员该问管理文档是否明确外部人员接入受控网络前的申请审批流程 2) 核查外部人员访问系统的书面申请文档是否明确外部人员的访问权限，是否具有允许访问批准签字等 3) 核查外部人员访问系统的登记记录是	1) 相关管理文档明确了外部人员逻辑访问受控网络系统的审批要求 2) 具有相关申请并批准接入网络的记录 3) 具有外部人员逻辑访问受控区域的相关登记记录

			否记录外部人员访问的权限、 时间、 账户等	
	c) 外部人员离场后应及时清除其所有的访问权限	外部人员特别是获得访问权限的外部人员， 离场需进行严格的控制，并清除其所有的访问权限	1）应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限 2) 核查外部人员访问系统的登记记录是否记录了访问权限清除时间	1 具有相关管理文档明确外部人员离场后清除其权限的要求 2) 具有相关清除访问权展的记录
	d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，复制和泄露任何敏感信息	对获得系统访问授权的外部人员，需进行更加严格的保密控制措施	核查外部人员的访问保密协议或记录表单类文档，是否明确人员的保密义务 （如不得进行非授接权操作，不得复制信息等）	具有相关外部人员签字的保密协议， 明确其保密义务

九、安全建设管理测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由	《等级保护对象安全等级保护定级报告》是全国各类等级保护对象定级报告的通用模板，具体文档内容参见 www.djbh.net.	1) 核查定级文档是否明确测评系统的安全保护等级 2) 核查是否给出了定级的方法和理由	具有明确描述定级方法理由和最终定级结果的定级报告书
	b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定	定级结果的准确性需要安全技术专家论证评审。若初步定级结果为第二级、第三级，可组织本行业和网络安全行业专家进行评审，若为四级，则需网络安全等级保护专家评审委员会专家进行评审	1) 核查是否对测评系统组织相关部门或相关专家对定级结果进行了认证和审定 2) 核查是否有定级结果的评审和论证记录文件	具有相关专家对定统结果论证意见
	c) 应保证定级结果经过相关部门的批准	定级结果需由上级部门或本单位相关部门的批准	1) 核查是否获得了相关主管部门的批准 2) 核查是否有定级结果的审批文件	具有主管部门审批意见或本单位相关部门的审批意见
	d）应将备案材料报主管部门和相应公安机关备案	有主管部门的，备案材料需向主管部门和公安机关备案，没有主管部门的，备案材料需向相应公安机关备案	1）核查是否向主管部门备案 2）核查是否有备案证明证书	具有主管部门和公安机关的备案证明

安全方案设计	a) 系统确定安全保护等级后，安全规划设计需根据其安全保护等级确定基本安全保护措施	系统确定安全保护等级后，安全规划设计需根据其安全保护等级确定基本安全保护措施	1) 核查是否根据系统等级选择相应的安全保护措施 2) 核查是否根据风险分析的结果补充安全措施 3) 核查设计类文档是否根据系统等级或风险分析结果采取相应的安全保护措施 这里的安全规划设计类文档要求根据等级保护对象的安全保护，判断等级保护对象现有的安全保护水平与国家等级保护管理规范和技术标准之间的差距，提出等级保护对象的基本安全保护需求	安全设计文档有明确描述系统安全保护等级，并在相关章节中描述安全措施设计是依据系统等级和其特殊安全需求进行选择

	b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行整体安全体划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件	被测系统是整个单位等级保护对象的一部分，其安全方案应作为单位整体安全规划的一部分，且其安全性在设计上与其位系统可能存在共享，譬如在网络结构设计、安全措施部署上都具有共享关系，因此单位的整体安全规划也很有必要，安全规划是等级保护对象安全等级保护实施的环节之一，也是确保安全等级保护有效实施的重要环节，其目标是根据等级保护对象的划分情况，等级保护对象的定级情况、等级保护对象承载业务情况，通过分析明确等级保护对象安全需求设计合理、满足等级保护要求的安全方案	1) 核查是否有保护对 的相关设计文档 2）核查保护对象的总体规划和设计文档，且文档内容是否连贯配套，内容是否含密码技术相关内容 一般情况下，配套文件中包括总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等内容。在定期开展等级测评和安全评结后，如果发现等级保护对象安全现状已经不满足等级保护的基本安全要求或者发现等级保护对象有新的安全需求，则应该调整和修订安全保证体系的相关配套文件 安全规划管理示例： a) 安全规划设计是指对系统总体安全建设规划，近期和远期安全建设工作计划、安全方案等进行设计、编制 b) 安全方案设计是指根据系统的定级情况、承载业务情况，通过分析明确等级保护对象的安全需求，设计既满足自身需求又满足等级保护要求的、合理的安全方案，包括总体安全方案和详细设计方案	具有单位总体的安全规划文档和被删系统安全设计文档，且包含相关密码设计内容（如果采用了密码产品和算法）

			c) 总体安全方案包括总体安全策略、安全技术框架、 安全管理框架，详细设计方案包括技术措施实现内容和管理措施实现内容 d)XX 处负责依据相关文件， 委托设计单位编制系统安全规划设计系列文件，并不断完善 e) 编制完成的系统安全规划设计系列文件经各处审核、 网络安全领导小组及相关专家论证评审、 XX审批 安全方案设计目录示例 ： 目录： 1. 总体安全方案 总体安全策略 总体安全技术框架 安全管理框架 总体建设规划设计方案 2、详细安全设计方案 技术措施实现内容 管理措施实现内容 3、近期安全建设工作计划 4、远期安全建设工作计划	

	c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施	设计合理的安全方案是保障等级保护对象安全建设和运行的基础，安全设计方案应当对系统安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等内容作出具体的规划和设计，并经过论证、审定和批准	1) 核查是否组织相关人员对系统规划和建设文档进行论证和评审 2) 核查评审的文档和批准意见	具有总体安全规划和安全设计方案的专家论证、批准意见
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定	我国对网络安全产品的管理在不同发展阶段可能存在不同的管理政策，因此在该条款的理解上，应根据当下国家的管理要求去落实，目前而言，在此方面国家的主要管理要求是连从产品获得《计算机等级保护对象安全专用产品销售许可证》才能在市场上流通的政策。产品购买方在采购过程中应从已获得销售许可证的产品系列中选取	1) 访谈建设负责人产品采购的流程或流通的标准 2) 抽样核查网络安全产品的销售许可标志	网络安全产品均具有销售许可证
	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	如若被测系统中采用了商用密码产品，则该产品的采购和使用需符合国家的用密码管理部门的要求，(如《信息安全等级保护商用密码管理办法》等)	1) 访谈建设负责人是否采用了商用密码产品或服务 2) 核查使用的密码产品的许可证明或批文 密码产品是指采用密码技术对信息进行加密保护或安全认证的产品，如加密电子证书等	密码产品符合国家相关部门的要求

	c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单	在采购产品时，不仅要考虑产品的使用环境、安全功能、成本（包括采购和维护成本）等因素，还要考虑产品本身的质量和安全性，因此需要预先对产品进行选型测试	1) 访谈建设负责人产品来购流程 2) 核查产品采购管理制度或要求 3) 核查采购管理内容是否覆盖产品的选择方式以及定期审定和更新产品列表 通常情况下，产品采购的管理需要制定相关制度要求，产品采购管理示例： 产品采购管理是指对等级保护对象软硬件产品采购过程的管理，包括安全产品、网络产品、服务器以及应用和系统软件等 由 XX处提出产品采购需求，由 XX处按照政府采购流程进行产品采购，对于大宗产品的采购必须经过XX审批 采购的防火墙，IDS. 防病毒软件等安全产品必须具有公安部下发的《计算机安全产品销售许可证》，采购的密码产品必须符合国家密码管理部门的相关规定	具有产品选型测试报告、候选产品清单和定期更新名单

自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制	为避免开发过程中对系统造成影响，要保证开发环境与实际运行环境纷开，测试数据和测试结果受到控制	1) 访谈建设负责人，开发的控制流程和控制措施有哪些 2) 核查软件开发相关管理的规定和要求 3) 管理内容是否覆盖开发环境和运行环境分开的规定以及测试数据是否受控 开发人员和测武人员分离，即开发人员不能做测试人员，测试数据和测试结果受到控制，是指它们应该与软件设计相关档文一起有专人管理，并且对他们的使月和访问进行严格限制	1) 开发环境与运行环境分离 2) 有明确的管理要求控制测试数据和测试结果的使用
	b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则	为保证软件开发过程的安全性和规范性，应制定软件开发方面的管理制度，规定开发过程的控制方法和人员行为准则	1) 访谈安全建设负责人，是否有软件开发方面的管理制度 2) 核查管理制度内容是否覆盖软件开发的整个生命周期 3) 开发过程中是否覆盖开发过程的控制方法和行为准则	具有软件开发管理制度，明确了开发过程中相关管理要求

	c) 应制定代码编写安全规范，要求开发人员参照规范编写代码	一般一个应用软件需要多名开发人员共同开发，然而不同开发人员有不同的代码编写风格，这给代码的维护、整合等工作带来了很大的困难。因此，要求针对不同的开发语言制定相应的代码编写规范，并要求所有开发人员都按照相应的规范编写代代码，这将给代码的阅读、理解、维护、修改、跟踪调试、整合等带来极大的方便	1）访谈系统建设负责人是否有代码编写安全规范 2）代码编写规范是否明确代码的编写规则	具有代码编写安全规范
	d) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制	系统开发过程中，开发人员需编制软件设计的相关文档和使用指南，而且，系统开发文档的保管、使用应严格管理，加以限制。	1) 访谈系统建设负责人是否有人负责对软件设计的相关文档进行管控 2) 被测评系统是否有开发文档和使用说明文档	具有软件开发过程中的相关文档（如软件概要设计文档、软件详细设计文档等）和使用指南
	d) 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在恶意代码进行检测	应在软件开发过程中加强软件的安全性测试，以便及早发现软件的安全漏洞、在软件安装前进行代码安全审计，通过工具测试和人工确认的方式识别恶意代码，这是保证软件安全运行的最后一道屏障。 可通过第三方检测机构内或机构内部自行测试	1）访谈安全建设负责人，是否在软件开发的生命周期中进行安全性测试 2) 核查是否具有安全性测试报告和代码审计报告	具有阶段性软件安全测试报告和软件安装前代码审计报告

	e) 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制	对程序资源库的访问，维护等应进行严格管理	1) 访谈建设负责人是否对程序资源库进行管控 2) 核查是否有管控记录文件 要求对程序源代码及源程序库的修改、更新和发布都得到授权和批准。这里的发布 - 方面包括向程序员发布程序源代码，另一方面包括修改或更新程序代码后应用软件重新上线	具有程序资源库修改、更新、发布的授权、批准记录
	f) 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查	软件开发需保证开发人员为专职人员，并对其开发过程能够有效的控制	1) 访谈建设负责人开发人员是否为专职人员 2) 核查软件开发管控制度是否对开发过程和人员的行为准则进行了规定和要求	开发人员为专职人员，有相关管理要求或手段对开发人员进行控制、监视或审查
外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码	同自行软件开发一样，对于外包软件，在交付前同样需要进行恶意代码检测，以保证软件的安全性，可要求外包方进行检测或机构内部自行检测	1) 访谈建设负责人是否做恶意代码检测 2) 核查是否有恶意代码检测报告	具有恶意代码检测报告
	b) 应保证开发单位提供软件设计文档和使用指南	软件开发完成之后，应要求外包开发单位提供软件设计相关文档和使用指南	1) 访谈建设负责人是否有软件设计的相关文档和使用指南 2) 核查是否提供了软件生命周期中的所有文档	具有软件开发的相关文档，如需求分析说明书、软件设计说明书等

	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	后门和隐蔽信道的审查在可专业的测试进行，若开发单位无法提供该类报告，则需提供书面材料保证软件源代码中不存在后门和隐蔽信道	1) 访谈建设负责人，外包开发单位是否提供源代码 2) 核查是否提供源代码的安全检查报告 3) 核查软件源代码及源代码的审查记录 审查软件中可能存在的后门时，一般通常在系统的设计者利用应用系统的开发时机，故意设置机关，用以监视计算机系统，但有时也因偶然考虑不周而存在（如漏洞）。可以通过人工或采用专业工具（如 Fortify SCA、Checkmarx 等) 事方式进行源代码审查，发现软件中可能存在的后门	1. 提供软件源代码 2. 具有软件测试报告，内容涵盖后门和隐蔽信道的测试
工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理	等级保护对象工程实施应当指定或授权专门的部门或人员负责工程实施过程的管理，以保证实施过程的正式有效性	1）访谈建设负责人，工程实施是否指定专门部门或人员进行工程实施过程的管控 2）核查部门或岗位职责文档	指定了专门部门或人员对工程实施过程进行进度和质量控制

	b) 应制定安全工程实施方案控制实施过程	工程实施过程的控制需要事先制定实施方案，对工程时间限制、进度控制和质量控制等内容进行规定	1) 访谈建设负责人是否有工程实施方案 2) 核查工程实施方面的管理制度以及控制方法 总体的工程实施方案应说明任务量、计划进度、实施阶段、各阶段结束的标志和开始的条件、完成时提交的内容等。一旦实施方案确定，就必须按照方案的阶段安排逐步开展工作，并进行量化和考核，否则将造成工程实施组织的混乱，无法保证工程的顺利完成。 详细的工程实施方案要求的正式执行行是相对于系统工程能力成熟度模型（SSE-CMM)中所定义的一级，非正式执行。该级仅要求对所有基本实践都被执行，而对执行的结果并无明确要求。因此，正式执行意味着对执行结果和执行工程必须严格控制，根据制定的工程实施方案落实各个执行中间结果，保证实施结果与预定目标相符	具有工程实施方案，内容包括工程时间限制、进度控制等 方面的方面
	c) 应通过第三方工程监理控制项目的实施过程	一般来讲，对于外包实施项目，需要第三方工程监理的参与，来控制项目的实施过程，对工程进展，	1) 访谈建设负责人测评系统是否为外包项目 2) 核查是否聘请了第三方监理	第三方工程监理，工程监理报告明确了工程进展、时间计划、控制措施、工程质量等

		时间计划、 控制措施、 工程质量等进行把关	3) 核查监理报告以及主要控制措施	
测试验收	a) 应制订测试验收方案， 并依据测试验收方案实施测试验收 ，形成测试验收报告	此处的测试验收， 可以包括外包单位项目实施完成后的测试验收， 也可包括机构之间的内部开发部门移交给运维部门过程的验收等	1）访谈建设负责人是否对测试验收进行管控 ）2 核查是否有调试验收方案和测试验收报告	1）具有工程测试验收方案， 方案中明确说明了参与测试的部门、人员、测试验收内容、现场操作过程等内容 2) 测试验收报告具有相关部门和人员对测试验收报告进行审定的意见
	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	为保证系统建设工程按照既定方案和要求实施，并达到预期要求，在工程实施完成之后， 系统交付使用之前，应当指定或授权专业机构依据安全方案进行安全性测试	1 访谈建设负素人在系统证线前是否展开安全性测试 2) 安全性测试是否括密码应用方面的内容 一般情况下， 上线前的安全测试由第三方测试单位进行， 第三方测试单位是指非系统拥有者和系统建设方，第三方测试有别于开发人员或用户进行的测试， 其目的是为了保证测试工作的客观性。 第三方一般属于权威的专业测试机构， 针对物理环境、 硬件设施、 软件设施等方面可能存在的缺陷或问题进行测试	具有上线前的安全测试报告，报告包含密码应用安全性测试相关内容
系统交付	a) 应制定交付清单， 并根据交付清单对所交接的设备、 软件和文档等进行清点	系统在工程实施并验收完以后， 需要根据协议有关要求， 按照交付清单对设备备、 软件、 文档进行交付	1 访谈建设负责人是否对系统交付建立管控流程以及交付清单 2) 核查交付清单内容	具有交付清单，交付清单对交付的各类设备、软件、文档等有明确的说明

	b) 对负责运行维护的技术人员进行相应的技能培训	系统交付时， 交付单位或部门需要对运维和操作人员进行必要的培训	1) 访谈建设负责人是否对运行维护人员进行技能培训 2) 核查培训记录相关记录文档	具有交付技术培训相关文档，内容包括培训内容、培训时间和参与人员等方面的信息
	c) 应提供建设过程文档和运行维护文档	交付单位或部门需提供建设过程中的文档和指导用户进行运行维护的文档，以便指导运维人员和操作人员后期的运行维护	1) 访谈建设负责人建设过程的管控措施 2）核查建设过程文档和运行维护文档	在系统交付的文档中包括指导用户进行维护的文档等，且符合管理规定相关要求
等级测评	a) 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应及时整改还	对等级保护对象进行等级测评是检验系统达到相应等级保护要求的途径，也是发现系统安全隐患的重要途经，通过选择有资质的测评机构对系统进行定期的测评， 有助于系统发现问题并进行及时的整改，就目前来说， 第三级等级保护对象应当每年至少进行一次测评	1) 访谈等级测评负责人是否每年定期开展等级测评 2) 核查等级测评报告和整改记录	1) 定期开展测评工作，且非首次，以往进行过几次测评，并根据测评结果进行相应的安全整改 2) 具有以往等级测评报告和安全整改方案
	b) 应在发生重大变更或级别发生变化时进行等级测评	系统在发生重大的网络结构调整或大范围的设备更换， 应用系统功能变化等变更时， 应重新进行等级测评，并评估系统级别是否发生变化，若变化， 则需按照最新的安全保护等级要求进行测评	1) 访谈测评系统是否发生过重大变更或开级 2) 核查重大升级变更或改造的文件	1）有过重大变更或级别发生过变化， 若有，及时开展了等级测评 2) 具有相应情况下的等级测评报告

	c) 应确保测评机构的选择符合国家有关规定	目前国家对等级保护测许机构的管理遵从测评机构名录管理要求，即在国家网络安全等级保护工作协调小组办公室推荐测评机构名单内的测评机构均可透，具体参见 www.dibh.net	1) 访谈测评负责人是否选择了具有测评资质的测评机构 2) 到 www.djbh.net 上核查该机构是否符合要求	等级测评的测评单位具有国家相关等级测评资质的单位
服务供应商的选择	a) 应确保服务供应商的选择符合国家的规定	对各类供应商的选择均应符合国家对其的管理要求（如相关资质管理要求、销售许可要求等）	1 访谈建设负责人如何选择服务商 2) 核查服务商资质文件	选择的安全服务商符合国家有关规定
	b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务	服务提供商所提供服务的质量，将直接影响到系统的安全，为了减少或者杜绝这些服务带来新的安全问题，在选择服务商的时候，除了选择具有相应服务资质的机构，还要以协议或合同方式明确其职责以及后期的服务承诺等	1) 访谈建设负责人对服务供应商的管控措施 2) 核查服务供应商的服务内容和协议	具有与安全服务商签订的服务合同或安全责任合同书，并明确了后期的技术支持和服务承诺等内容
	c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制	对供应商的监视和评审主要基于与其所签订协议中的网络安全相关条款和条件，验证其所提供服务与协议的符合程度，通过定期评审其工作服务报告，确保有足够的服务能力按照可行的工作计划履行其服务职责	1 访谈建设负责人是否对服务供应商进行定期监督、评审和审核 2) 核查对服务供应商的管理规定或要求 3) 核查服务供应商服务报告或服务审核报告	1）具有安全服务商定期提交的安全服务报告 2) 定期审核评价安全服务供应商所提供的服务，具有服务审核报告 3) 具有安全服务商评价审核管理制度，明确了针对服务商的评价指核内容等

十、安全运维管理测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
环境管理	a) 应指定专门的部门或人是负责机房安全、 对机房的出入进行管理，定期对机房供配电、空调、温湿度控制，消防等设施进行维护管理	机房是存放等级保护对象基础设施的重要场所 ，要落实机房环境的管理责任人，因此要确保机房的运行环境良好、安全， 应对机房环境进行严格管理和控制	1) 访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，如对机房的出入进行管理、对基础设施 (如空调、供配电设备、灭火设备等) 进行定期维护 2) 核查来访人员登记记录 3) 来访人员记录内容是否包括了来访人员、来访时间、离开时间，携带物品等 4) 核查设施维护记录 S) 设施维护记录内容是否包括了维护日期、维护人、维护设备、故障维护结果等	1）指定部门和人员负责机房安全管理工作， 如对机房的出入进行管理， 基础设施 (如空调、供配电设备、灭火设备等) 进行定期维护 2) 具有来访人员登记记录 3) 来访人员记录内容包括了来访人员、来访时间、离开时间、携带物品等 4) 具有设施维护记录护结果等 5) 设施维护记界内容包格了维护日期、维护人、 维护设备、故障原因、维护结果等
	b) 应建立机房安全管理制度，对有关物理访问、 物品进出和环境安全等方面的管理作出规定	为保证系统有个良好安会的运行环境，应针对机房建立管理规定或要求	1) 核查机房安全管理制度 2) 制度内容是否包括了机房物理访问、物品带进带出机房和机房环境安全等 3) 核查机房物理访问、物品带进带出机房和机房环境安全等相关记录	1) 具有机房安全管理制度 2) 制度内容包括了机房物理访问、 物品带进带出机房和机房环境安全 3) 具有机房物理访问， 物品带进带出机房和机房环境安全等相关记录

	c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸质文件和移动介质等	加强内部办公环境的管理是控制网络安全风险的措施之一，为保证内部办公环境的独立性、敏感性，应降低外部人员无意或有意访问内部区域的可能性，同时杜绝都员工因无意行为而泄露敏感文档而导致网络安全事件的发生	1) 核查办公环境的安全管理制度 2) 制度内容是否明确了来访人员的接待区域 3) 核查员工的办公桌面上是否合有敏感信息的纸质文件和移动介质	1) 具有办公环境的安全管理制度 2）制度内容明确了来访人员的接待区域 3) 员工的办公桌面上是否合有敏感信息的纸质文件和移动介质
资产管理	a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容	等级保护对象资产种类较多，如保护对象的资产管理比较混乱，容易导致等级保护对象发生安全问题或不利于发生安全问题时有效应急	1) 核查资产清单 2) 资产清单内容是否包括了资产范围(含设备设施、软件、文档等）、资产责任部门、重要程度和所处位置等	1) 具有资产清单 2) 资产清单内容包括了资产范围(含设备设施、软件、文档等)任部门、重要程度和所处位置等
	b) 根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施	信息资产的重要程度不同，在系统中所起的作用也不尽相同，应综合考虑资产的价值、在系统件的地位，作用等因素，按照重要程度高低对资产进行分类、分级管理，分类的原则应在相关文档中选行明确，且需明确重要资产和非重要资产在资产管理环节(如入库、维修、出库)的不同要求	1) 核查资产管理制度 2) 制度内容是否包括了资产的标识方法以及不同资产的管理措施要求 3) 核查资产清单中的设备是否具有相应的标识 4) 核查资产清单中的设备上的标识方法是否符合相关要求	1) 具有资产管理制度 2) 制度内容包括了资产的标识方法以及不同资产的管理措施要求 3) 资产清单中的设备具有相应的标识 4) 资产清单中的设备上的标识方法符合相关要求
	c）应对信息分类与标识方法作出规定，并对信息的使用，传输和存储等进行规范化管理	信息作为资产的一种，可根据其所属的类别不同，重要程度不同进行信息的整理分类(一般可分为：敏感、内部公开、对外公开等不同类别），不同类别的信息在使用、传输和存储等方面管理要求也应不同	1) 核查安全管理制度中是否明确了对信息进行分类与标识的原则和方法 2) 核查安全管理制度中是否明确了对不同类信息的使用、传输和存储等操作的要求	1）安全管理制度中具有对信息进行分类与标识的原则和方法 2) 安全管理制度中具有对不同类信息的使用、传输和存储等操作的要求。

介质管理	a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储介质专人管理，并根据存档介质的目录清单定期查点	介质类型可包括纸介质、磁介质、光介质等，由于存储介质是用来存放系统相关数据的，因此，介质管理工作非常重要，如果管理不善，可能会造成数据的丢失或损坏，应为存储介质提供安全的存放环境并进行妥善的管控	1) 访谈资产管理员 / 存储介质管理员当前使用的存储介质类型或数据存储方式 2) 访谈资产管理员 / 存储介质管理员当前使用的存储介质是否指派专人管理 3) 核查存储介质（主要指移动存储介质，如脱机的硬盘、光盘、移动硬盘、U盘等）管理记录，记录内容是否包括了使用、归还、归档等	1）存储介质存放在指定的环境中 2) 指定了部门或人员负责存储介质的管理 3) 定期对存储介质进行盘点
	b) 应对介质的物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归等进行登记记录	需系统存在离线的存储备份介质应对其进行管控，如对介质进行两地传输时，应遵循一定的管理要求，应选择可靠的传送人员，并对打包交付过程签字确认等	1) 访谈资产管理员 / 存储介质管理员是否在存储介质的物理传输情况，如脱机的硬盘、光盘、移动硬盘、U 盘等的物理传输 2) 如有存储介质的物理传输，核查安全管理制度是否明确了物理传输过程的管理要求 3) 核查物理介质传输的管理记录，记录内容是否包括了执行人、存储介质信息、存储介质打包、存储介质交付、存储介质归档、存储介质查询等	1) 安全管理制度中具有介质在物理传输时的管理流程和要求 2) 物理介质传输的管理记录，记录内容包括了执行人、存储介质信息、存储介质信打包、存储介质交付、存储介质归档、存储介质查询等
设备维护管理	a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门成人员定期进行维护管理	对设备进行有效的维护管理，在一定程度上可降低系统发生安全问题的概率，应明确设备管理的责任部门或人员	1）访谈设备管理员是否指派部门或专人对各类设施、设备进行定期维护管理 2) 核查部门职责或人员岗位职责文	1) 指定部门或人员对各类设施进行定期维护 2) 部门职责或人员岗位职责具有文档具有设备维护管理责任

			档是否明确了设施、设备的维护管理责任	
	b) 应建立配套设施、 软硬件维护方面的管理制度。 对其维护进行有效管理， 包括明确维护人员的责任、 维修和服务的审批、维修过程的监督控制等	系统的正常运行依赖于对设备的正确使用和维护。 为了保证对设备的正确使用和维护， 应建立相应的管理规定或要求， 相关人员必须严格按照规定要求对设备进行使用和维护， 并认真做好使用和维护记录	1) 核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容 2) 核查是否留有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符	1）具有设备维护管理方面的制度，在制度中明确了维护人员的责任、 维修和服务的审批、 维修过程的监督控制等方面内容 2) 具有维修和服务的审批、 维修过程等记录， 审批、 记录内容是否与制度相符
	c) 信息处理设备应经过审批才能带离机房或办公地点， 含有存储介质的设备带出工作环境时其中重要数据应加密	信息处理设备的流转容易引起信息泄露的风险，必须严加管控 ，因此信息处理设备带离机房或办公等常规使用的地点时必须经过审批或采取加密的管控措施	1）核查设备带离机房的审批流程 2) 核查设备带离机房或办公的审批记录 3) 核查含有存储介质的设备带离机房的记录，记录中是否有对重要数据的加密措施	1) 具有设备带离机房的审批流程 2) 具有设备带离机房或办公的审批记录 3) 重要数据的存储介质带出工作环境时采取 XX 加密措施后方可带离办公环境
	含有存储介质的设备在报废或重用前， 应进行完全清除或被安全覆盖， 保证该设备上的敏感数据和授权软件无法被恢复重用	存储介质在报废或重用时， 容易引起敏感信息的泄露， 应采取相应的处理的措施施	核查含有存储介质的设备在报废或重用前所采取清除措施或安全覆盖措施	1) 具有设备在报度或重用前， 必须采取措施进行处理的要求 2）具有相应的处理记录

	d) 应来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	安全漏洞和隐患是引起安全问题的主要根源，采取有效的措施来及时识别系统漏洞和隐患，　并对识别出的漏洞和隐患根据评估的情况进行修补	1) 核查用来发现安全漏洞和隐患的措施 2) 核查相关安全措施执行后的报告或记录 3) 核查修复漏洞或消除隐患的操作记录	1) 定期进行漏洞扫描，　对发现的漏洞及时进行修补或评估可能的影响 2) 具有漏洞扫描报告，　报告描述了存在的漏洞、严重级别，　原因分析和改进意见等方面 3) 漏洞报告的时间跟定期扫描的要求相符
	e）应定期开展安全测评，　形成安全测评报告，　采取措施应对发现的安全问题	定期开展安全测评有利于及时发现系统潜在的安全问题，　安全测评局限于风险评估、等级测评，　只要是通过对系统的全面测试评估方法	1) 核查以往开展安全测评所获得的测评报告，确认测评工作是否定期开展 2) 核查安全整改工作相关的文档，如整改方案、整改报告、工作总结等	1) 具有安全测评报告 2) 安全测评定期开展 3）具有安全整改工作相关的文档，如整改方案、整改报告、工作总结等
网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限	没有明确的责任和权限要求，　容易发生泄职事件，因此要对管理员进行明确的划分并进行岗位职责的定义	1) 核查管理员职责文档，确认是否划分了不同的管理员角色 2) 核查管理员职责文档，确认是否明确了各个角色的责任和权限	1) 管理员职责划分了不同的管理员角色 2) 管理员职责明确了各个角色的责任和权限
	b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户进行控制	账户管理应由专门的部门或人员来负责，并对账户的生命周期进行管控	1) 访谈运维负责人指派哪个部门或人员进行账户管理，含网络层面、系统面、数据库层面、　业务应用层面 2) 核查账户管理记录，记录内容是否包括了账户申请、　建立、停用、删除、重置等相关的审批情况。	1) 指定了某部门　(某岗) 负责账户的管理工作 2) 有相关审批记录或流程，对申请账户、建立账户、　删除账户进行有效控制

	c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与补丁、口令周期更新等方面做出规定	对系统和网络安全管理缺乏规范性指导或规范性指导规定不一致，容易造成人员读职或无作为，因此对网络和系统安全应建立相应的管理策略和规程类的管理要求	1) 核查网络和系统安全管理制度 2) 制度内容是否包括了安全策略、账户管理（用户责任，义务，风险、权限审批、权限分配、账户注销等）、配置文件的生成及备份、变更审批、授权访问、最小服务、升级与补丁。、计日志管理、登录设备和系统的口令更新周期等	1) 具有网络和系统安全管理制度 2）制度内容至少包括了安全策略、账户管理（用户责任，义务，风险、权限审批、权限分配、账户注销等）、配置文件的生成及备份、变更审批、授权访问、最小服务、升级与补丁。、计日志管理、登录设备和系统的口令更新周期等
	d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等	配置规范和配置基线是保障等级保护对象安全运行的基本前提，应对设备的配置和操作建立操作规范和配置基线	1) 核查重要设备的配置和保作手册，重要设备如操作系统、数据库、网络设备、安全设备、应用和组件等 2) 手册内容是否包括了操作步聚、维护记录、参数配置等	1) 具有重要设备的配置和操作手册，如操件系统，数据库、网络设备、安全设备、应用和组件等的配置和操作手册 2) 手册内容至少包括了操作步聚，维护记录、参数配置等
	e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置、修改等内容	运维操作日志缺失，不利于安全事件的回溯或追踪，因此要对日常的记录运维操作日志进行详细的记录	1) 核查运维操作日志 2) 日志内容是否包括了网络和系统的日常巡检、运行维护记录、参数的设置、修改等内容	1) 具有运维操作日志 2) 日志内容至少包括了网络和系统的日常巡检、运行维护记录、参数的设置、修改等内容
	f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为	没有明确的职责要求，密易引起人员读职或无作为，应对日志、监测、报警数据等指定专人负责和统计	1) 访谈网络和系统相关人员是否指派部门或人员对日志、监测和报警数据等进行统计、分析 2）核查日志、监测和报警数据的统计、分析的报告	1) 指派了部门或人员对对日志、监测和报警数据等进行统计、分析

				2) 具有日志、监测和报警数据的统计、分析的报告
	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	变更管理不当，极易引起安全问题，对运维过程中的变更操作需严格控制，变更的审批过程中保留痕迹，事后能够更新变更内容	1) 核查配置变更审批程序，如对改变连接、安装系统组件或调整配置参数的审批流程 2) 核查配置变更审计日志 3）核查配置变更记录 4) 核查配置信息库更新记录	1) 具有配置变更审批程序，如对改变连接、安装系统组件或调整配置参数的审批流程 2) 核查配置变更审计日志 3）核查配置变更记录 4) 核查配置信息库更新记录
	h）应严格控制运维工具的使用，经过审批才可接入进行操作，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中的敏感数据	IT 运维工具包括商业的专用运维工具，也有自行开发运维工具，无论采取哪种工具，都需进行严格的管控	1) 核查运维工具的使用审批程序 2) 核查运维工具的使用审批记录 3) 核查通过运维工具执行操作的审计日志	1) 具有运维工具的使用审批程序 2) 具有运维工具的使用审批记录 3) 具有通过运维工具执行操作的审计日志
	i) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道 , 操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道 ,	远程运维是系统安全的隐患之一，如远程控制不当容易通成安全事件，应对远程运维的开通进行严格的控制，如确实需要开通，需要对操作过程日志进行留存并保证不可更改，运维结束后即刻关闭	1) 核查远程运维的方式，使用的端口或通道 2) 核查开通远程运维的审批程序 3) 核查开通远程运维的审批记录 4) 核查通过远程运维执行操作的审计日志	1) 具有远程运维的方式，使用的端口或通道 2) 具有开通远程运维的审批程序 3) 具有开通远程运维的审批记录 4) 具有通过远程运维执行操作的审计日志

	j) 应保证所有与外部的连接均得到授权和批准，应定期的检查违反规定无线上网及其他违反网络安全策略的行为	对所有外部链接进行管控，并且定期对违规外联进行检查	1) 核查开通对外连接的审批程序 2) 核查开通对外连接的审批记录。 3) 核查开展违反规定无线上网及其他违反网络安全策略行为的检查记录	1) 具有开通对外连接的审批程序 2) 具有开通对外连接的审批记录。 3) 具有开展违反规定无线上网及其他违反网络安全策略行为的检查记录
恶意代码防范管理	a) 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	恶意代码对等级保护对象的危害极大，并且传播途径有多种方式，提升所有用户的防恶意代码意识是规避恶意代码发生概率的基本途径。恶意代码的防范不仅仅需要安装防恶意代码工具来解决，为有效预防恶意代码的侵入，除了提高用户的防恶意代码象识外，还应建立完美的恶意代码管理制度并有效实施	1) 核查提升员工防恶意代码意识的培训或宣传记录 2) 核查恶意代码防范管理制度 3) 核查外来计算机或存储设备接入系统前进行恶意代码检查记录	1) 开展提升员工防恶意代码意识的培训或宣传记录 2) 具有恶意代码防范管理制度 3) 开展外来计算机或存储设备接入系统前进行恶意代码检查记录
	b) 应定期验证防范恶意代码攻击的技术措施的有效性	防恶意代码工具的技术措施最常见的是安装恶意代码软件，该类措施有效性保障就是定期升级恶意代码库，并对检测的恶意代码进行分析，另外如采用可信计算机技术也可防恶意代码攻击，需定期验证可信技术的有效性	1）核查恶意代码防范措施 2）核查恶意代码防范措施执行记录 3) 核查恶意代码防范措施特征库的更新记录	1）具有恶意代码防范措施 2）具有查恶意代码防范措施执行记录 3) 具有恶意代码防范措施特征库的更新记录
配置管理	a) 应记录和保有基本配宣信息，包括网络拓扑结构、各个设备安装的软件组件、软件组	系统配置信息的准确性，是系统正常运行的有效保障，因此要对系统的基本信息予以及时有效的记录和保存	1) 核查配置信息保存记录 2) 记录内容是否包括了网络拓扑结构、各个设备安装的软件组件、软件	记录和保存基本的配置信息，配置信息

	件的版本和补丁信息、 各个设备或软件组件的配置参数等		组件的版本和补丁信息、各个设备或软件组件的配置参数等	主要包括 ：网络拓扑、软件组件、设备配置等内容
	b) 应将基本配置信息改变纳入变更范畴， 实施对配置信息改变的控制， 并及时更新基本配置信息库	配置信息及时间同步是配置管理流程的重要环节， 该条要求与变更管理和系统管理中的相关条款比较类似，应关注几方面信息保持一致	1）核查配置变更管理程序 2) 核查配置信息变更记录	1) 具有记录和保存配置信息的管理措施，且基本配置信息改变后会及时更新配置信息库 2) 对配置信息的变更流程具有相应的管控程序或手段
密码管理	a) 应遵循密码相关的国家标准和行业标准	密码生产需要授权许可， 密码产品需要符合国家和行业的相关标准	1) 访谈安全管理员当前使用的密码产品类型 2) 如果使用密码产品，核查密码产品的销售许可证明或国家相关部门出具的检测报告中所遵循的相关国家标准和行业标准	1) 确认密码产品类别、型号 2) 具有密码产品销售许可证明 3）未使用密码产品，本条不适用
	b) 应使用国家密码管理主管部门认证核准的密码技术和产品	系统使用的密码产品要有国家密码主管部门核发的相关型号证书	核查密码产品是否具有销售许可证明或国家相关部门出具的检测报告	密码产品具有密码产品销售许可证明
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、 审批后才可实施	变更管理受控是降低系统由变更带来安全问题的有效手段， 因此要对变更策略进行明确的规定， 并对变更流程进行全程管控	1) 核查变更方案，方案内容是否包括了变更类型，变更原因，变更过程、变更前评估等内容 2) 核查变更方案评审记录 ，记录内容是否包括了评审时间、参与人员、评审结果等 3) 核查变更过程记录，记录内容是是	1) 具有相应的变更方案， 方案内容是否包括了变更类型， 变更原因， 变更过程、变更前评估等内容 2) 具有 XXX 变更方案评审记录和变更过程记录文档

			否包括了变更执行人，执行时间、操作内容、变更内容等	3) 对于新建或执行过变更操作的被测系统，此条可不适用
	b) 应建立变更的申报和审批控制程序， 依据程序控制所有的变更，记录变更实施过程	执行变更操作要遵循变更管控的相关控制程序， 约束变更过程， 并有效记录	1) 核查变更控制的申报、控制审批程序 2) 核查变更实施过程的记录 3) 记录的内容是否包括申报的变更类型、申报流程、审批部门、批准人等	1) 不同变更类型具有相应的变更管控策略， 如变更类型、变更原因、变更影响分析等 2) 具有 XXX变更实施过程的记录文档 3) 对于新建或未执行过变更操作的被测系统，可没有相关记录
	c) 应建立中止变更并从失败变更中恢复的程序， 明确过程控制方法和人员职责， 必要时对恢复过程进行演练	变更失败恢复程序一般会在变更方案中予以明确， 变更方案除了描述变更过程操作外， 重要的是明确变更失败后的恢复操作	1）核查变更失败后的恢复程序、 工作方法和相关人员职责。 2) 核查恢复过程演练记录	1）对变更失败后的恢复程序、工作方法和职责进行了文件化的规定和要求，具有变更失败后的恢复程序 2) 具有 XX 变更恢复演练记录和恢复流程 3) 对于新建或未执行过变更操作的被测系统，可没有相关记录

备份与恢复管理	a) 应识别需要定期备份的重要业务信息、 系统表据及软件系统等	对于要备份的信息进行识别， 并制定相应的备份策略	核查数据备份策略，策略内容至少明确了备份周期、备份的信息类别或数据类型	1) 具有数据备份策略 2) 数据备份策略内容至少包括了备份周期、备份的信息类别或数据类型
	b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等	对需要备份的制定相应的备份策略，如备份方式、 备份频度、 存储介质等等	核查备份与恢复管理制度，制度内容至少明确了备份方式、备份频度、存储介质、保存期等	1) 具有备份与恢复管理制度 2) 制度内容至少包括了备份方式、 备份频度、存储介质、保存期等
	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	数据备份策略是根据数据性质的不同，选择不同的备分内容、 备份方式等，数据恢复策略是指数据库在遭到各种事件导致数据丢失时利用介质备份数据进行恢复的方法和操作	1) 核查是否有数据备份策略、备份程序 2) 核查是否具有数据恢复策略、恢复程序	1) 具有数据备份策略、备份程序 2) 具有数据恢复策略、恢复程序
安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件	如发现系统有潜在的弱点和可疑事件，应及时向安全主管部门汇报， 并提交相应的报告或信息	1) 核查运维管理制度中对于发现安全弱点和可疑事件后的汇报要求 2) 核查以往发现过的安全弱点和可疑事件对应书面报告或记录	1) 在网络安全事件管理相关规定中明确告知用户在发现安全弱点和可疑事及时向安全管理部门报告 2) 具有 XXX 安全弱点和可疑事件对应的报告或记录文档
	b) 应制定安全事件报告和处置管理制度， 明确不同安全事件的报告、 处置和响应流程， 规定安全事件	安全事件的分类分级标准可参考 GB/T20986-2007《信息安全技术信息安全事件分类分级指南》	核查运维管理制度，其中明确了不同安全事件的报告，处置和响应流程 ，规定安全事件的现场处理、事件报告和后期恢复的管理职责等内容	1) 在安全事件报告和处置管理制度明确了与安全事件有关的工作职责， 包括报告单位（人）、接报单位（人）和处置单位等职责 2) 具有 XXX安全事件报告的模板文件

	的现场处理、 事件报告和后期恢复的管理职责等			
	c) 应在安全事件报告和响应处理过程中分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训	对安全事件报告和响应处理的过程应进行详细的记录， 并对事件发生的原因进行分析和总结	1) 核查以往的安全事件报告和响应处置记录或相关模板 2) 文档的内容是否包括了引发安全事件的系统弱点，不同的安全事件发生的原因、 处置过程、 经验教训总结、补救措施等	1) 未发生过网络安全事件，则不适用。 2) 发生过安全事件的， 具有 XXX安全事件报告和响应处置记录文件， 文件内容符合 XXX 安全事件报告模板的相关要求，如安全事件发生的原因、 处置过程、经验教训总结、补救措施等
	d) 对造成系统中断和造成信息泄露的重大安全事件应采用不同的处理程序和报告程序	对不同的安全事件应制定不同的处理程序和报告程序	核查安全事件报告和处理程序文档，是否针对重大安全事件制定了不同的处理和报告程序，是否明确了具体报告方式、报告内容、报告人等	1) 针对不同安全事件形成不同的报告流程 2) 发生过安全事件， 且具有安全事件的报告
应急预案管理	a) 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资金保障、事后教育和培训等内容	应急预案框架一般为单位总体应急预案管理的顶层文件， 明确应急组织构成员职责、 应急预案启动条件、 响应、后期处置、 预案日常管理、 资源保障等内容， 与各类网络安全事件专项应急预案共同构成整个应急预案体系	核查应急预案框架，内容是否包括了启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等	1) 具有应急预案框架 2) 应急预案框的框架覆盖了启动应急预案的条件、 应急组织构成、 应急资源保障、事后教育和培训等方面的内容

	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	对重要事件制定专定应急预案，并对处理流程、恢复流程进行定义	核查针对重要事件的应急预案，预案内容是否包括了应急处理流程、系统恢复流程等	1）具有重要事件的专项应急预案，如针对机房（供电、火灾、漏水等）、系统（病毒爆发、数据泄露等）、网络（断网、拥塞等）等各个层面 2）专项事件应急预案包含应急处理流程、恢复流程
	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	应急预案培训和演练是应急的重要环节。应定期组织相关人员予以培训和演练，以保障及时有效的处理应急事件	1) 核查以往开展过应急预案培训所产生的记录，确认培训的频度，记录内容是否包括了培训对象、培训内容、培训结果等 2) 核查以往开展过应急预案演练所产生的记录，确认演练的频度，记录内容是否包括了演练对象、演练内容、演练结果等	1) 具有定期（每季度、每半年、每年）对相关人员进行应急预案培训和演练 2) 具有应急预案演练所产生的记录，确认演练的频度，记录内容包括了演练对象、演练内容、演练结果等
	d) 应定期对原有的应急预要重新评估，修订完善	根据每次应急演练的情况，对应急预案进行重新评估和修订	核查应急预案修订记录，记录内容是否包括了修订时间、参与人、修订内容、评审情况等	1) 具有应急预案修订记录 2) 记录内容包括了修订时间、参与人、修订内容、评审情况等
外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定	外包服务商应满足国家相关主管部门的相关规定和要求，以证明其具有相应的服务能力	1) 访谈运维负责人是否有外包运维服务情况 2) 如果采用外包运维服务，核查外包运维服务商是否符合国家的有关规定	1) 无外包运维，则本条不适用 2) 有外包运维，主要外包内容是什么，外包服务单位名称以及所承担服务的资质证明
	b) 应与选定的外包运维服务商签订相关的协议，明确规定外包运维的范围、工作内容	针对外包运维服务商提供那些服务内容，应在相关协议中予以明确	1) 核查外包运维服务协议 2) 协议是否包括了外包运维的范围和工作内容	1) 具有外包运维服务协议 2) 协议包括了外包运维的范围和工作内容

	c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力， 并将能力要求在签订的协议中明确	外包服务运维服务商应具有按照等级保护要求的开展安全运维工作的能力，意味着该外包运维服务商以往具有根据等级保护开展运维工作的实例，选择方在考虑选择哪个服务商时，应着重考虑相关运维人员具备等级保护相关运维的能力 （如进行过等级保护相关方面的培训 ）	核查外包运维服务协议是否包含了其具有按照等级保护要求的开展安全运维工作的能力要求	外包运维服务协议内容包括了服务商具有按照等级保护要求的开展安全运维工作的能力要求
	d) 应在与外包运维服务商签定的协议中明确所有相关的安全要求， 如可能涉及对敏感信息的访问、 处理、存储要求，对 1T 基础设施中断服务的应急保障要求等	与外包服务商签订的协议中， 应明确相关网络安全要求， 以确保在单位和服 商之间关于双方要履行的有关网络安全要求的义务不会存在误解和分歧。可能 的网络安全要求包括 ：可以访问的信息类型及方法 ，权限分配、关于数据保护求、网络安全培训等等	核查外包运维服务协议内容是否包括了可能涉及对敏感信息的访问、处理、存储要求， 对 IT 基础设施中断服务的应急保障要求等	外包运维服务协议内容包括了可能涉及对敏感信息的访问、 处理、存储要求，IT 基础设施中断服务的应急保障要求等

十一、云计算安全扩展要求测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
基础设施位置	应保证云计算基础设施位于中国境内	云服务商对机房选址时，应确保机房位于中国境内、确保云计算服务器及运行关键业务和数据的物理设备等基础设施位位于中国境内	1) 访谈并查阅最新的机房清单 2) 核查云计算服务器及运行关键业务和数据的物理设备等基础设施是否都在中国境内	部署整个云计算环境的机房云计算服务器及运行关键业务和数据的物理设备等基础设施均位于中国境内
网络架构	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	云服务方侧的云计算平台单独作为定级对象定级，云租户侧等级保护对象也应作为单独的定级对象定级，云平台的等级要不低于云上租户的业务应用系统最高级	1) 访谈云平台等级及云上客户业务系统等级，核查相关定级备案材料 2) 核实是否存在客户业务应用系统等级高于平台等级的情况	1) 提供云平台及云上客户业务系统的定级备案材料 2) 云客户业务系统安全保护等级不高于云计算平台 / 系统的安全保护等级
	b) 应实现不同云服务客户虚拟网络之间的隔离	同一个物理主机上的虚拟机间可能通过硬件背板、不同物理机上的虚拟机可能通过网络进行通信，这些通信流量对传统的网络安全控制而言是不可见的，无法进行监控或封堵，为防止多租户间的相互影响及恶意攻击，确保租户安全及云平台安全，应对不同的云服务客户网络间进行有	2)1) 核查不同云客户间是否采取隔离手段或措施 2) 检查相关的隔离技术说明文档，并查看相关的隔离测试报告 3) 测试验证不同云服务客户之间的网络隔离措施是否有效	1) 虚拟网络隔离技术 (如 VPC)实现不同云服务客户间的网络资源的隔离 2) 云防火墙采用“基于业务可视化的结果进行业务梳理和业务隔离“的技术，帮助用户实现专有云环境中东西向流量的隔离

		效的网络隔离，以保证云服务客户的访问与其他租户能够实现有效隔离		
	c) 应具有根据云服务客户业务需求提供通信传输、 边界防护、入侵防范制等安全机制的能力	为应对源自各个层面的攻击，云服务商应该为云服务客户提供通信传输、边界防护、入侵防范等安全防护措施，云服务客户可根据业务安全防护需求选择适当的安全防护措施，提升业务系统的安全防护能力以应对外来的威胁攻击	1) 核查云服务商提供的通信传输、 边界防护、入侵防范等安全防护措施，并检查安全措施形成的安全防护能力 2) 云服务商提供的通信传输、边界防护、入侵防范等安全防护能力是否能满足云服务客户业务需求	1) 通信传输、 边界防护、 入侵防范等对应云安全产品或安全服务的说明 2) 各安全产品业务安全防护配置情况
	d) 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、 选择安全组件、配置安全策略	云服务客户可以根据自身的业务需求，在云服务商提供的安全组件上自定义安全策略，如定义安全访问路径、选择安全组件、配置安全策略	1) 访谈云计算平台提供的安全组件有哪些，安全组件是否支持用户自定义 2) 核查云服务客户是否能够自定义安全策略，包括定义访问路径、选择安全组件、配置安全策略	云安全产品的配置控制台截图， 显示可以自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略

	e) 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或云计算平台选择第三方安全服务	API(Application Ppogramming Interface，应用程序编程接口) 是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件的以访问一组例程的能力 ，而又无需访问源码，或理解为内部工作机制的细节 ,API 本身是抽象， 仅定义了一个接口，云计算目前面临的互操作性问题的重要原因就是缺乏标准化和被广泛认可接受的 API 标准，因而云服务商应提供开放和公开的 APIs，允许第三方安全产品或服务接入	1) 访谈是否提供了开放接口或开放性安全服务， 并查阅接口设计文档或开放性安全服务文档 2) 核查并进行测试验证是否允许第三方安全产品或安全服务接入到云计算	1) 提供允许第三方安全产品接入的开放接口说明 2) 云平台部署安全异构区， 允许第三方安全产品接入， 云安全生态支持用户选择第三方安全产品， 通过联调后允许第三方安全产品接入
访问控制	a) 应在虚拟化部署访问控制机制，并设置访问控制机则	位于云平台边界外，云平台缺乏或缺失控制和管理的网络环境，被认为是不可信网络，与之对应的是可信网络，在可信与不可信网络间实施有效的安全控制，对，网络安全来说至关重要。通常使用虚拟防火墙进行可信与不可信网络间的连接控制，通过防火墙的访问控制策略配置，仅允许必要的流量通过，而其他流量均被禁止。虚拟网络边界主要包括云计算平台和云服务客户业务系统虚拟网络边界，不同云服务客户间的网络访问边界、云服务客户不同安全保护等级业务系统间的网络边界。可以防止攻	1) 访谈确认云计算平台的虚拟网络边界处采用的访问控制机制， 并核查访问控制规则 2) 核查并测试访问控制规则是否有效	1) 访谈确认云计算平台的虚拟网络边界处采用的访问控制机制， 并核查访问控制规则 2) 核查并测试访问控制规则是否有效

		击者通过未授权的 IP 地址访问可信网络，或以未授权的方式访问服务、协议或端口		
	b) 应在不同等级的网络区域边界部署访访问控制机制 ，设置访问控制规则	云平台边界、云平台内网络区域边界、云服务客户不同业务边界将网络划分为不同等级的安全域，结合边界访问控制技术可以实现整个系统的纵深防御，可以减少未授权访问或运行环境交更的风险。因此，应在不同等级的网络区域边界部署访问控制设备，设置访问控制规则	1) 访谈并查阅网络拓扑， 记录网络安全区域划分情况 2) 检查各网络区域边界处采用的安全控制机制，查看访方问控制列表 3) 核查访问控制规则是否有效， 并测试验证是否能够拒绝不同区域间的非法访问	在不同等级的网络区域边界部署了边界防火墙 ：云防火墙和 VPC 并且设置了访问控制规则 ；云平台内部采用 VPC隔离， VPC间通过云防火墙实现东西流量隔离

入侵防范	a）应能检测到云服务客户发起的网络络攻击行为，并能记录攻击类型、攻击时时间、攻击流量等	云平台应能够对云服务客户端发起的访问，进行入口流量镜像分析，对东西向、南北向的攻击行为进行深入分析，并结合相关的云安全产品对异常流量的处理。记录攻击类型、攻击时间、攻击流量等	1）访谈云服务商是否采取了入侵防范措施对网络入侵行为进行防范，如部署API 攻击系统、网络回溯系统和网络入侵保护系统等入侵防范设备或相关组件，是否能够对云服务客户发起的网络攻击行为进行检测和报警 2) 检查相关入侵检测产品规则库是否进行及时更新，对异常流量和未知威胁的监控策略、报警策略是否有效 3) 检查相关入侵检测产品产品白皮书及销售许可证	1) 部署流量安全监控设备，通过对云入口镜像流量包的深度解析，实时地检测出各种攻击和异常行为 2) 虚拟机层面部署防恶意代码软件 (如阿里云安骑士》进行基线检查、并对恶意文件进行扫描、恶意进程查杀，并且提供入侵检测功能，规则库定期更新 3) 部署主机入侵检测，实时检测云环境中所有物理服务器主机，并及时发现文件篡改、异常进程、异常网络连接、可疑端口监听等行为，规则库定期更新 4) 部署态势感知系统，从攻击者的角度有效捕捉高级攻击者使用的0Day 漏洞攻击、新型病毒攻击事件，以及有效展示正在发生的安全攻击行为，实现业务安全可视和可感知，解决因网络攻击导致数据泄露的问题，并通过溯源服务追踪黑客身份

	b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等	在云计算服务的关键节点如虚拟网络节点出入口实施安全防护，部署应用层，防火墙、入侵检测和防御设备以及流量清洗设备来提升网络攻击防范能力，对虚拟 网络节点的网络攻击行为进行检测，并记录攻击类型、攻击时间、攻击流量等	1) 检查是否部署网络攻击行为检测设备或相关组件对虚拟网络节点的网络攻击行为进行防范，并能记录攻击类型、攻击时间、攻击流量 2) 核查网络攻击行为检测设备或相关组件的规则库是否为最新	1) 通过部署的流量安全监控设备对云入口镜像流量包的深度解析，实时地检测出各种攻击和异常行为 2) 部署入侵检测设备并记录相关攻击原始日志， 检测到攻击行为本地产生告警 10g，保存至日志服务（log Service)
	c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量	为避免异常流量影响虚拟机与宿主机的正常运行，虚拟机与宿主机、虚拟机与虚拟机间的通信，部署流量监测设备、入侵防护系统等对虚拟机与宿主机、虚拟机与虚拟机之间的流量进行实时监测	1) 访谈云计算平台是否具备虚拟机与宿主机之间、 虚拟机与虚拟机之间的异常流量的检测功能 2) 查看异常流量的监测策略， 并测试验证对异常流量的监测策略是否有效	【预期结果或主要证据】 虚拟机与虚拟机之间通过云防火墙，虚拟机与宿主机之间通过流量安全监控， 对流量进行检测， 发现异常流量进行告警， 告警日志同步到日志管理平台进行分析
	d) 应在检测到网络攻击行为、异常流量情况时进行告警	部署流量监测设备、入侵防护系统等对网络流量进行分析、检测，当检测到网络攻击行为、异常流量时提供告警机制，及时告知相关人员，避免网络攻击行为、异常流量影响系统正常运行	1) 核查网络入侵有哪些 2) 检查在检测到网络攻击行为、 异常流量时是否进行告警， 并查看相关告警记录 3) 测试验证其对异常流量的检测策略是否有效	1) 流量安全监控具备相关告警功能，包括本地日志告警、复信，邮件等类型 2) 主机入侵检测实时检测云环境中所有物理主机服务器， 并及时发现文件篡改、 异常进程、 异常网络连接、可疑端口监听等行为 3) 云防火墙通过流量的可化可清晰的酶别出端口滥用情况、 协助甄别流量是否安全， 在检测到异常情况时会进行短信或邮件告警

安全审计	a) 应对服务商或云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启	对特权命令的操作可能超越系统、实体、网络、虚拟机和应用控制的措施，因而需要对特权命令的执行进行严格控制，使用加以限制并严格控制，并对操作进行审计，以防止出现的滥用和破坏	1) 访谈是否授权特权命令执行的权职，是否部署审计工具对云服务和云服务客户执行特权命令进行审计 核查审计记录是否有效，并查阅审计记录是否包括虚拟机删除、虚拟机重启 3) 测试验证删除或重启测试虚拟机时，是否能够被审计	提供完整的审计回放和权限控制服务，能够对操作过程进行实时监控，并支 持以切断操作会话的方式阻断违规操作等异常行为
	b) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计	云服务商应在云服务客户授权后才能够对云客户系统和数据的访问，为避免云服务商的恶意访问，云服务客户应采取审计机制，对云服务商的操作行为进行审计，以避和及时发现违规的操作	1) 访谈云服务商是否允许访问云服务客户系统和数据 2) 是否采取了相关的审计机制，能够记录云服务商对云服务客户系统和数据的操作，并核查审计记录的有效性	2）云服务商对云服务客户系统的操作需提交工单，使用云服务客户的账户，相关操作行为通过云服务客户的管理平平台进行审计
身份鉴别	当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制	认证是验证或确定用户提供的访问凭证是否有效的过程，是网络安全第一道防线。在远程管理云计算平台中的设备时，双向认证有助于保证双向安全，有效 的防止重放攻击和拒绝服务攻击。双向认证保证了终端不会被伪装服务器攻击，云计算平台不会被非法入侵，大大的提高了云计算平台和终端设备连接的安全性	1) 访谈管理员，当远程管理云计算平台中设备时，管理终端和云计算平台之间采用的身份验证机制是什么 2) 核查采用的身份验证机制是否实现了双向身份验证	1) 认证方式采用双向身份验证机制 2) 认证接入到统一身份认证中心，对接入到网络内的所有用户进行统一身份认证

访问控制	a) 应保证当虚拟机迁移时，访问控制策略随其迁移	虚拟机迁移包括不同云平台间的迁移，以及将云平台中的服务器、应用和数据迁移至本地环境。对于虚拟机迁移而言，若缺乏安全保障措施，监听者可能通过监听源与目标服务器间的网络，获得迁移过程中的全部数据，还可能修改传输数据，植入恶意代码，控制虚拟机。因此，为保证迁移安全，可进行加密传输，或通过链路加密模式，同时将访问控制策略同时迁移，以防止未授权的访问	1) 访谈管管理员是否对虚拟机进行计移，迁移采取的方式是什么 2) 核查虚拟机迁移的过程中是否将控制策略进行随迁，查看迁移记录	提供虚机迁移后的安全组策略的的前后对比截图
	b) 应允许云服务客户设置不同虚拟机之间的访问控制策略	云平台在同一时间段内，承载多个或大量的的租户。若租户虚拟机间无有效的安全访问控制策略可能导致虚拟机非法访问、租户数据泄露，对于多租户环境下，多个用户共享计算、存储、网络等虚拟资源，若共享模块存在漏洞，租户可对其他租户资源发起攻击，或对自己的其他资源，如虚拟机进行攻击。因此，云计算环境下多租户或同一用户间不同虚拟机间应允许访问	1) 访谈管理员，不同虚拟间是否允许配置访问控制记录 2) 记录配置的访问控制策略，核实策略是否真实有效	提供安全组、云防火墙的访问控制策略

入侵防范	a) 应能检测虚拟机之间的资源隔离失效，并进行告警	1) 虚拟机和宿主机共享资源，若虚拟机间的资源、内存和存储空间隔离失效，云服务商未采取相应的应对措施检测恶意行为且无告警措施，可能导致虚拟机非法占用资源，从而导致其他虚拟机无法正常运行。因此，对虚拟机间的资源隔离进行实时监控，并在检测到异常时进行告警，从而降低虚拟机出现异常的风险	1) 访谈管理员，实现对虚拟机资源隔离的措施 2) 核查是否对虚拟机资源进行监控，是否能够检测到虚拟机资源隔离失效并进行告警	提供虚拟机资源监控、隔离措施、以及入侵告警方式和记录
	b）应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警	规范虚拟机的管理操作，可强化虚拟化环境安全，所有的虚拟机新建或重启应都由系统管理员来创建和保护，若某些用户（如如开发人员、测试人员和培训中）需重启虚拟机，应通过系统管理员创建和管理或进行授权，为避免虚拟机的非授权创建或重启，应对所有虚拟机的运行状态进行检测，并提供异常报警机制；以便能及时发现虚拟机的非法重建和重启	1) 核查非授权用户是否有权限新建或重启虚拟机 2) 访资管理员是否采取相关措施对虚拟机的新建或重启进行监视，并对虚拟机的新建或重启行为进行安全审计 3) 安全监视工具是否能够对虚拟机的新建或重启操作进行告警	提供新建新建或重启虚拟机的机制，部署安全监视工具对新建或重启虚拟机的操作进行监视、审计，提供违规启停客户虚拟数据安全审计记录，提供告警方式及记录

	c) 应能够检测恶意代码感染及在虚拟机间蔓廷的情况，并进行告警	恶意代码感染可能导致虚拟机无法正常运行或被非法利用，虚拟机被非法利用后，可能被作为跳板机，若无有效的虚拟机隔离技术措施，可能导致恶意代码任宿主机或虚拟机间蔓延，从而破坏整改云计算环境，因此对整个云平台进行恶意代码检测，防止恶意代码的入侵，并对恶意代码的感染和蔓延情况进行监测、告警，降低恶意代码感染的风险和损失	1) 检查是否部署安全产品或服务对虚拟机进行恶意代码进行检测，　　并进行告警 2) 检查是否采取虚拟机隔离技术或其其他手段有效防止病毒蔓延整个云环境 3) 检查是否采用相关安全措施能够检测恶意代码在虚拟机间的蔓延并进行告警。	部署安全产品或服务对虚拟机进行恶意代码进行检测，　并进行日志记录，并进行告警
镜像和快照保护	a) 应针对重要业务系统提供加固的操作系统镜像像或操作系统安全加固服务	进行操作系统安全如固，关闭不必要的端口、协议和服务，减少系统的攻击面。云计算环境中，所有操作系统均应进行安全加固处理、仅提供必要的端口、协议和服务，以满足业务需求。防恶意代码软件、文件完整性监控、日志记录均应作为基本的操作系统加固需求。通过安全加固，可提升服务器安全性，防止外来用户和木马病毒对服务器的攻击，保护云平台和云用户安全。应鉴于业内最佳实践，参考国际标准规范形成操作系统安全加固指南或手册　，并应用到镜像或操作系统，并及时访问权限进行限制	1) 核查云服务商是否提供操作系统安全加固基线或相关安全加固服务 2) 检查加固基线是否合规，　　否对基线进行定期更新	提供带防恶意代码软件镜像模板的说明

	b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改	虚拟机镜像、快照无论在静止还是运行状态都有被窃取、篡改或替换的危险，攻击者可能是黑客，也可能是云服务商员工。若无法保证虚拟机镜像、快照的完整性，　可能被非法篡改、恶意代码植入，或安全合规配置被更改，导致虚拟机被部署运行时，系统遭受攻击　，因此必须保证虚拟机镜像、快照的完整性。虚拟机镜像、快照的完整性主要通过哈希校验的方式实现，一旦发生变化　　，哈希值将改变，因此　，在下一次使用虚拟机镜像或快照时　，应进行完整性校验，以保证期间未授权的更改。对虚拟机进行补丁更新或安全配置更改　　，都应进行审计记录并进行报警。虚拟机镜像、快照的完整性验证结果，应即通过电子的方式告知用户	1) 核查是否对虚拟机的变更进行检测， 2) 若进行检测空是否有相关的检测记录，发现镜像或快照被变更时，是否提供告警方式	ESC、虚拟机镜像和快照的完整性校验记录、结果

	c) 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 被非法访问	数据加密技术是最基本的安全技术，被誉为信息安全的核心。采用密码技术将保护信息置换为密文，在存储或传输过程中，即使被非授权人员获得，也可以保证这些信息不为其所知，从而保护信息。对虚拟机镜像、快照采取密码技术进行加密 ，可有效的保证存在于镜像、快照中的敏感数据的安全性。此外，通过访问控制的方式，限制用户对虚拟机镜像、快照的非法访问，也可以保护其安全性	1) 核查是否对虚拟机镜像、 快照进行加密，采用了何种加密技术 2) 核查是否采取访问控制或其他措施对虚拟机镜像、快照进行保护	采用加密技术对虚拟机镜像、 快照进行加密， 保证其在传输、 存储过程中的安全性， 通过访问控制的方式限制虚拟机镜像、 快照被非法访问
数据完整性和保密性	a) 应确保云服务客户数据、用户个大信息等存储于中国境内，如需出境应遵循国家相关规定	《网络安全法》第三十七条规定，基础设施运营者在中国境内运营中收集和产生的个人信息和重要数据应当在境内存储。为满足网络安全法规定，云服务商 提供的存储机制应保证云服务客户数据、用户个人信息等存储于中国境内，若需 要出境，应当满足国家相关的规定	1) 查阅相关文档查看云服务客户数据存储方式，访谈客户业务数据、用户个人信息等存储所在的服务器节点以及与其存储相关的设备是否部署在中国境内的机房 2) 核查客户业务数据、 个人信息等数据是否存在出境的情况， 是否依据国家相关规定制定了数据出境的规定	1) 机房的部署、 数据存储位置均位于中国境内 2) 制定云上数据出境的相关规定，符合国家相关规定的要求
	b) 应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据管理权限	为避免云客户数据的非法访问，对数据的管理权限进行控制，仅允许云服务客户管理员访问，若其他用户 （云服务商或第三方用户 ）需对数据进行管理，必须由云服务客户管理员提供授权，方能进行数据管理	1) 核查云服务客户的授权机制， 如授权流程、授权方式及授权内容 2) 检查云计算平台是否有云服务客户数据的管理权限，是否有相关的授权	云服务客户根据账号创建子账号，提供云服务商或第三方使用， 云服务客对子账号进行授权和收回

	c) 应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到整性受到破坏时采取必要的恢复措施	为确保虚拟机迁移后业务能够正常切换，迅速进行，必须确保数据在迁移过程中完整性。因此，云服务商应对迁移过程中的数据提供完整性校验措施或或手段，且能够在发现数据完整性遭到破坏时提供恢复措施，来保证业务迁移后正常运行	1) 核查虚拟机迁移过程中是否采用校验码或密码技术 2) 测试采用的校验码技术或密码技术是否能够保证数据在迁移过程中的完整性 3) 核查采用措施是否能够在完整性受到破坏时，提供相应的恢复手段，保业务正常运行	云服务商提供虚拟机迁移技术，保证迁移过程通过密码机进行加密传输，实现了源机与目标机的数据同步，保证业务正常切换
	d) 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程	云计算环境中，云服务商和和用户对密钥管理系统具有不同的所有权和控制权，在云服务中，数据的所有权属于云服务客户，数据却保存在云服务商控制的存储资源上，服务客户可自行部署或采用云服务商提供的密钥管理解决方案，实现数据的加解密，云服务商应支持云客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程	1) 核查云服务客户是否部署密钥管理解决方案 2) 核查云服务商为云服务客户提供的密钥管理解决方案 3) 查阅密钥管理解决方案相关文档，核查部署的密钥密钥管理解决方案是否能够保证云服务客户自行实现数据的加解密过程	云服务商或云客户部署经国家密码管理局检测认证的硬件加密机，云服务客户借助此服务实现对加密密钥的完全控制和对数据进行加解密操作
数据备份恢复	a) 云服务客户应在本地保存其业务数据的备份	数据丢失会对客户业务造成重大巨大影响，在云计算中，用户数据大部分存在云中，有一定的风险。因此，云用户（租户）应将业务数据本地保存备份，防止数据意外丢失	1) 核查云服务商是否支持云服务客户将数据本地备份保存 2) 检测云服务客户是否对业务数据进行本地备份保存	提供支持 open API 的说明，云服务商支持云客户本地保存业务数据备份、转存，并有数据备份记录

	b）应提供查询云服务客户数据及备份存储位置的能力	在云计算环境中，大量用户数据被存储在不同的物理位置，供应用程序及操使用，在公有云、私有云、混合云中数据都有可能发生移动，其存储地点有可能位于同一数据中不同服务器或不同数据中心，云服务商应为云服务客户提供数据存储及备份位置	1) 核查云服务商是否提供数据备份及存储位置查询的接口 2) 测试验证是否能够查询到用户数据存储以及备份的位置	提供 ECS 查询实例所在物理机房的截图；提供 RDS查询实例所在宿主机所在机房位置的截图；提供 OSS查询 Buket 所在服务器，和资产系统查询此服务器所在机房地址的说明
	c) 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致	云服务商为云服务客户提供了云存储服务模式，对用户数据进行备份，并将多个副本存在不同的服务节点中。为降低成本，云服务商可能减少数据备份量，网络攻击也可能使多副本数据之间存在不一致，为确保备份数据的可用性、正确性和一致性，应定期核查数据是否多副本存储，并对多副本数据的完整性进行检测，确保各副本间内容的完整性和一致性	1) 访谈云服务商为云服务客户提供的云存储模式是否多副本存储， 检查多副本是否均可用 2) 核查是否对多副本进行一致性比对，是否有对比记录	提供云服务商提供的数据存储说明，多副本进行一致性比对的机制及对比记录和结果
	d) 应为云服务客户将业务系统和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	云服务商为云服务客户提供迁移服务，保证云服务客户业务系统和有关数据迁移到新的服务器上正常运行，云服务商应为云服务客户提供全程的协助，保证迁移活动顺利完成，确保数据在迁移过程中的完整性	1) 访谈采用的云服务商是否支持云服务客户业务系统及数据的迁移， 云服务商是否提供协助帮助云服务客户完成迁移 2) 核查云服务商提供的迁移措施、 手段	提供迁云服务的说明及协助说明

剩余信息保护	a）应保证虚拟机所使用的内存和存储空间回收时得到完全清除	当用户退出云服务时，用户释放内存和存储空间后，云服务商需要保证安全地删除用户的数据，避免发生数据残留。数据残留是指存储介质中的数据被删除后，并未彻底清除，在存储介质中留下了存储过数据的痕迹，残留的数据信息可能被攻击者非法获取，造成严重损失。一般来说，在数据销毁时可以采用覆盖、消磁、物理破坏等方法。云服务商应保证用户虚拟机释放内存和存储空间安全地删除，且采用了完全清除机制	1) 核查虚拟在迁移和删除后，　内存和存储空间回收时采用的删除机制是否能够使数据彻底清零 2) 核查内存清零机制、数据删除机制、检测是否能够实现数据完全清除	各云租户之间的内存和持久化存储空可相对独立，　租户资源释放时能够被释放和清除，　内部系统鉴别信息完全清除；　物理硬盘报废时使用随机数据多次写入进行数据写入和清除，　对于曾经存储过用户数据的内存和磁盘，一旦释放和回收，其上的残留信息将被自动进行零值覆盖；释放的存储空间由分布式文件系统回收， 禁止任何用户访问，　并在被再次使用前进行内容擦除　(包括云盘每一块上的内容　)，最大限度保证用户的数据安全性
	b) 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	为防止业务数据意外丢失，云客户业务数据在云上一般多副本存储，当云服务客户删除业务数据时，应采取数据清除机制将云计算平台所有副本全部删除	核查云服务客户在删除业务数据时，　采用的删除机制是否能够将云存储中的所有副本删除	使用的数据删除机制保证云服务客户业务数据删除时，　云存储中所有副本删除
集中管控	a) 应能对物理资源和虚拟资源按照策略做统一管理调度与分配	云计算通过对物理资源的整合与再分配，提高了资源的利用率，一台物理机的资源可能被多个虚拟机所共享。对物理资源、虚拟资源的统一分配与调度，能 多提高资源利用率	1) 核查是否部署了资源调度平台或其他平台对物理资源、　虚拟资源进行统一分配与调度 2) 核查资源管理平台是否能够实现物理资源、虚拟资源统一分配与调度的	提供资产管理系统的截图，　提供物理资源、虚拟资源水位管理的系统的截图

	b) 应保证云计算平台管理流量与云服务客户业务流量分离	通过带外管理或策略配置的方式将网管量和业务流量分开，为网管流量建专属的通道，在这个通道中，只传输管理流量，管理流量与业务流量分离，可以提高网管的效率与可靠性，有利于提升管理流量的安全性	1) 检查网络架构和配置策略，核查云平台管理流量是否采用带外管理或策略配置等方式 2) 核查并测试管理流量与云服条客户业务流量是否分离	云平台管理流量通过带外管理，云服务客户业务流量通过上层网络；管理流量网络层使用的是经典网络，和业务网络默认隔离，云平台管理流量与业务流量完全分离
	c) 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并 实现各自的集中审计	在云运维方面，为缓解云服务商和云服务客户间的不信任，云服务商和云服务客户应进行明确的职责划分，各自收集各自部分的审计数据，并对审计数据进行集中审计，实现云计算平台全面的信息审计，实现云计算环境下合规性、业务连续性、数据安全性等方面的审计要求，有效控制审计数据在云中面临的风险	1) 核查云服务商和云服务客户间是否进行职责划分 2) 检查云平台是否支持云服务商和云服务客户收集各自的审计数据 3) 检查云服务商和云服务客户是否部署集中审计平台支持各自收集审计数据的集中审计	1) 云平台运维侧及租户侧分别部署了不同的审计产品： 云平台运维侧的，全部日志， 全部传给云盾 (安全审计) 2) 租户侧部署了租户的审计产品，负责采集租户侧的审计日志，并完成审计功能。
	d) 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测	为便于云服商和云服务客户能够及时掌握系统运行情况，云服务商和云服务客户的职责应明确划分，对各自控制的虚拟化资源（虚拟化网络、虚拟机、虚拟化安全设备等）运行状况集中监测	1) 核查云服务商和云服务客是否进行职责划分 2) 检查云平台是否支持云服务商和云服务客户集中监测各自控制部分虚拟源 (虚拟化网络、 虚拟机、 虚拟化安全设备等) 的运行状况	1) 云监控中心提供了资源实时监控、告警和通知服务， 可以监控云服务器 ECS、负载均衡 SLB、云数据库 RDS 和对象存储 OSS相关指标 2) 云管平台能够对虚拟资源运行状况进行集中监测

云服务商选择	a) 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	为确保云服务商提供的服务符合安全性需求，云服务客户应当选取安全合规的云服务商，且云服务商提供的安全保护能力等级应具有相应的或高于业务应用系统需求的安全防护能力	1) 访谈系统建设负责人确认选择的云服务提供商提供的云计算平台的安全服务等级，并核查云计算平台的安全防护等级 2) 访谈管理员，业务系统的安全防护等级 3) 核查云服务商提提供商提供的云计算平台的安全防护能力能够满足业务应用业务系统需求	云服务商提供云平台安全保护等级说明，云平台安全保护等级具有相应或高于业务应用系统所需求的安全防护能力
	b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标	云服务商与云服务客户签订协议（如SLA），协议的内容可能会因不同的云服务 客户、业务类型、服务形式等发生很大变化。协议内容应尽可能全面的包括信息安全管理需求，明确云服务商所提供的云服务内容以及云服务商需提供的技术指标	1) 核查是否与云服务商签订服务水平协议或服务合同 2) 检查服务水平协议或服务合同的内容是否对云服务商所提供的云服务内容和需提供的技术指标进行规定	1) 云服务商与云服务客户签订 SLA 文本 2)SLA 文本内容包括了云服务商所提供的云服务内容和需提供的技术指标
	c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等	云服务商与云服务客户签订协议（如SLA)中是否对云服务商的权限与责任进行规定，规定内容是否包括云服务商的管理范围，职责划分、访问授权、隐私保护、行为准则、违约责任等	检查云服务商与云服务客户签订协议（如 SLA)中是否对云服务商的权限与责任进行规定，规定内容是否包括云服务商的管理范围，职责划分、访问授权、隐私保护、行为准则、违约责任等	1）云服务商与云服务客户签订 SLA 文本 2) SLA文本内容规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等

	d) 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除	云服务商与云服务客户签订协议（如SLA)中内容应包括业务关系到期和受影响的用户数据的处理方案，当云服务客户与云服务商服务合约到期后，云服商应向云服务客户提供完整的数据，且制定相关规定保证相关数据在云计算平台上完全清除	1) 核查云服务商应与云服务客户签订协议（如 SLA)中是否规定业务关系到期和受其影响的用户数据的处理方案，是否规定合约到期后云服务商向云服务客户提供完整的数据 2) 核查云服务商应与云服务客户签订协议是否规定合约到期后云服务商清除云计算平台上的数据	1) 云服务商与云服务客户签订 SLA 文本 2)SLA 文本内容规定云服务商的权限与责任， 规定业务关系到期和受其影响的用户数据的处理方案， 规定合约到期后云服务商向云服务客户提供完整的数据
	e) 应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据	云服务客户应与云服务商签署保密协议，协议中应规定云服务商不得以任何理由泄露云服务客户数据	1) 访谈云服务客户是否与云服务商签订保密协议 2) 核查保密协议是否规定云服务商不得以任何理由泄露云服务客户数据	1) 云服务客户与云服务商签订保密协议 2) 保密内容明确规定数据归云服务客户所有， 云服务商不得以任何理由泄露云服务客户数据
供 应 链管理	a）应确保供应商的选择符合国家有关规定	在安全产品采购和使用、安全服务提供商选择以及云服务商的选择时，应确保符合国家有关规定要求。如《公安部关于加强信息网络安全检测产品销售和使用通知》，《含有密码技术的信息产品政府采购规定》等，此外部分特殊行业，如金融、电力、能源等。也对安全产品的采购和使用有规定。 云服务商在选择安全服务提供商时，应充分考虑国家法律法规、行业规范等要求，以保持云计算安全服务的而持续性和合规性，如 （商用密码管理	1) 访谈确认选择的云服务商 2) 核查云服务商提供的产品或服务清单，检查供应商的选取是否满足国家安有关规定， 如查阅安全产品的销售许可证、提供加密服务的资质	服务商提供的产品或服务清单符合规定， 供应商的选取满足国家安有关规定， 如查阅安全产品的销售许可证、提供加密服务的资质

		条例》规定，商用密码产品发生故障，必须由国家密码管理机构制定的单位维修		
	b) 应提供应链安全事件信息或安全威胁信息及时传达到云服务客户	云服务商应及时向云服务客户及相关供应商通报安全事件，保障其知情权的同时作为风险评估的输入（如影响服务正常提供或涉及敏感信息泄露等重大问题），应及时向相关方提供信息，便于采取相应的应对措施	1) 核查云服务商是否定期向云服务客户通报安全事件 2) 检查是否有相关的供应链安全事件报告或威胁报告 3) 核查供应链安全事件报告或威胁报告，查看事件报告是否及时，报告内容是否能够明确相关事件信息或威胁信息	云服务商推送最新的安全事件信息，以保证第一时间传达给云服务客户
	c) 应将供应商的重要变更及时的传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制	云服务商与云服务客户应建立供应链协议（如 SLA），如果云服务商所进行的的任何变更，可能对云服务客户造成影响，应评估变更带来的安全风险，告知云服务客户，或事前得到客户授权，以便于云服务客户能够制定相应的措施应对可能引发的风险	1) 检查云服务商与云服务户之间的供应链协议（如 SLA），核查云服务商所进行的任何变更是否及时告知客户或事前得到客户授权 2) 检查云服务客户是否对变更的风险进行安全评估，是否采取相应的安全措施应对安全风险	(1) 云服务商通过云管平台推送通知和公告，云服务客户通过自己的控制台查看相关风险和控制变更的信息 (2) 云服务商对所有变更均有变更流程控制，云服务客户可以根据需求定制、选择自己感兴趣的风险信息
云计算环境管理	a) 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	云计算平台的运维地点原则应位于中国境内，若确实因业务需求，需通过境外对境内的云计算实施运维操作，应满足国家相关规定	1) 访谈管理员运维地点，核查运维地点是否在中国境内 2) 访谈管理员是否存在境内对境外云计算平台的运维操作，若存在，核查是否满足国家相关规定	1) 提供仅允许在中国境内进行运维操作，其他区域禁止运维操作的规定 2) 若存在境外运维操作，提供相关运维制度，共提供符合国家相关规

				定的 说明

十二、移动互联安全扩展要求测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
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	无线接入设备的安装位置选择不当，易被攻击者利用，特别是通过无线信号过度覆盖的弱点进行无线渗透攻击，因此要选择合理的位置安装无线接入设备	1) 核查无线接入设备的物理位置、确定无线信号的覆盖范围 2) 测试无线信号的覆盖范围，测试在一定范围内是否可以进行渗透攻击与电磁干扰等	1) 无线接入设备的部署方案 2) 无线接入设备的物理部署位置合理 3) 无线接入信号覆盖范围在合理范围内，未出现过度覆盖或被电磁干扰
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	保证无线网络与有线网络之间的网络边界隔离与安全访问控制，要求在有线网络与无线网络边界之间的和数访问和数据流通过无线接入网关设备，防止无线安全防护边界缺失	核查有线网络与无线网络边界之间是否部署无线接入网关设备	1) 查阅网络拓扑结构图（含有线网络、无线网络），有明确边界划分 2) 在有线网络与无线网络边界之间部署无线接入网关设备
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模块进行认证	为保证无线接入终端的安全接入，可在无线接入设备上开启认证功能，部署认证服务器对无线接入终端认证，也可以采用国家密码管理机构批准的密码模块的认证	核查是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证	1) 无线接入设备开启接入认证功能，移动终端接入需要进行认证 2) 采用认证服务器或国家密码管理机构批准的密码模块进行认证

入侵防范	a) 应能检测到非授权的无线接入设备和非授权的移动终端的接入行为	保证接入到无线网络中的无线设备均为已授权的无线设备，防止私搭乱建无线网络所带来的安全隐患，比如网络中用户自己搭建的非法 wifi，，或恶意搭建的 wifi 钓鱼等	1) 核查是否能够检测到非授权的无线接入设备和非授权的移动终端的接入行为 2) 测试验证是否能够检测非授权的无线接入设备和非授权的移动终端的接入行为	1) 通过无线入侵检测/防范系统(WIDS/WIPS) 能够检测到非授权无线接入设备和移动终端的接入行为 2) 非授权无线接入设备和移动终端接入的检测日志
	b) 应能够检测到针对无线接入设备的网络扫描、 DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为	为保证无线接入设备的安全性，防止被攻击者采用技术手段进行攻击，要求能够对无线网络攻击进行检测与记录	1) 应核查是否能够对网络扫描、 DDoS攻击、密钥破解、 中间人攻击和欺骗攻击等行为进行检测 2) 应核查规则库版本是否及时更新	1) 通过无线入侵检测/防范系统(WIDS/WIPS) 能够检测到对无线网络的扫描和攻击行为 2) 无线网络攻击行为的检测日志 3) 无线入侵检测 /防范 (WIDS/WIPS) 的规则库版本号
	c) 应能够检测到无线设备的 SSID 广播、 WPS等高风险功能的开启状态	为保证无线接入设备的安全性，应检测内部无线网络接入设备的 SSID 广播、 WPS等高风险功能的是否已关闭，如发现未关闭时应及时关闭相关高风险功能	应核查是否能够检测 无线网络接入设备的 SSID 广播、 WPS等高风险功能的开启状态	1) 无线接入设备的 SSID 广播、 WPS等高风险功能开启状态的检测日志 2) 无线接入设备的 SSID 广播、 WPS等高风险功能关闭的配置
	d) 应禁止多个 AP 使用同一个鉴别密钥	为保证无线 AP 的安全，禁止多个 AP 使用同一个鉴别密钥。比如：使用同一个认证密钥一旦被破解则使用相同密钥的 AP 都面临相同风险	先核查是否分别使用了不同的鉴别密钥	1) 无线 AP 的管理员登录口令设置 2) 不同的无线 AP 的管理员登录口令不同
	e) 应能够阻断非授权无线接入设备或非授权移动终端	为保证接入无线网络中的设备和终端均为授权终端，要求定位和阻断非授权无线接入设备或非授权移动终端。比如：发现非授权	1) 应核查是否能够阻断非授权无线接入设备或非授权移动终端接入 2) 应测试验证是否能够阻断非授权	1) 通过设置策略能够阻断非授权无线接入设备或非授权移动终端接入 2) 定位与阻断策略 (含黑白名单策略)

		无线接入设备，采用地址冲突等方式进行阻断	无线接入设备或非授权移动终端接入	
移动终端管控	a) 应保证移动终端安装、注册并运行终端管理客户端软件	为保证移动终端的安全性，应按照统一的生命周期管理对移动终端管理，移动终端应安装、注册并并运行终端管理客户端软件	应核查移动终端是否安装、 注册并运行终端管理客户端软件	1) 移动终端安装，注册并运行了客户端软件 2) 移动终端管理软件服务端相关客户端的记录
	b) 移动终端应接受移动终端管理服务端的设备命周期管理、设备远程控制， 如：远程锁定、远程擦除等	为保证移动终端的远程可管可控，防止设备丢失造成的数据泄漏等安全风险，要求移动终端接受移动终端管理服务端的设备生命周期管理、设备远程控制。比如：远程移动端数据擦除	1) 应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略 2) 应测试验证是否能够对移动终端进行远程锁定和远程擦除等	1) 移动终端管理服务端设置安全策略，能够对移动终端设备远程控制 2) 移动终端管理服务端安全策略配置
移动应用管控	a) 应具有选择应用软件安装、运行的功能	为保证移动终端应用软件安装与运行的可管可控 要求对移动终端管理客户端的应用软件安装与运行的功能进行管理，以选择是否安装应用软件，运行哪些功能等	应核查是否具有应用软件安装、 运行的功能	1) 移动终端管理服务端设置的安全策略，能够对移动终端的应用软件安装进行控制 2) 移动终端管理服务端设置的安全策略
	b) 应只允许指定证书签名的应用软件安装和运行	为保证移动终端应用安装的可管可控，要求对移动应用软件使用指定的证书进行签名，保证安装文件的完整性，防止被恶意用户篡改	应核查移动应用是否由指定证书签名	1) 移动应用使用了指定证书进行签名 2) 使用的证书以及证书签发机构

	c) 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	为保证移动终端应用安装的可管可控，在移动终端管理系统中加入白名单，控制移动终端软件的应用安装范围，仅允许白名单内的移动应用进行安装、运行。比如：设置白名单仅允许安装企业建设的移动应用商店内的移动应用	1) 应核查是否具有软件白名单功能 2) 应测试验证白名单功能是否能够控制应用软件安装、运行	1) 移动终端管理服务端设置白名单，能够对移动终端的应用软件安装进行控制 2) 移动终端管理服务端设置的白名单
移动应用软件采购	a) 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	要求移动终端安装、运行的应用软件应采用证书进行签名，保证应用软件的完整性，或者要求使用可靠的移动应用软件的分发渠道，降低移动应用软件安装带来的风险	应核查移动应用软件是否来自可靠分发渠道或使用可靠证书签名	1) 移动应用软件下载使用来自于官网或内部应用商店等可靠渠道 2) 移动应用软件下载渠道 3) 移动应用软件采用的签名证书
	b) 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	为保证移动终端安装的移动应用软件件的安全性，要求安装使用的移动应用软件需要由指定的开发者开发， 比如： 移动终端安装、运行的移动终端管理软件应明确开发单位 / 开发者等	应核查移动应用否由指定的开发者开发	1) 移动应用软件由指定的开发者开发 2) 移动应用软件开发者单位及开发者相关信息
移动应用软件开发	a) 应对移动业务应用软件开发者进行资格审查	为保证移动业务应用软件的安全性，要求对开发者进行基本的资格审查。比如：工作简历、技术能力、资格证书、项目实施情况等	应访谈系统建设负责人， 是否对开发者进行资格审查	1) 移动应用开发者的资格符合要求 2) 移动应用开发者资格审查记录或相关资质材料

	b) 应保证开发移动业务应用软件的签名证书合法性	为保证移动业务应用软件所采用的证书的合法性，要求采用国家移动业务应用软件的签名证书是否具有合法性	应核查开发移动业务应用软件的签名证书是否具有合法性	1) 移动业务应用软件的签名证书具有合法性 2) 签名证书的签发机构
配置管理	应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别	为保证无线接入设备和移动终端的安全接入，要求对无线接入设备和移动终端的设备情况进行登记和记录， 形成合法设备配置库、当设备接入无线网络时进行比对，如不在配置库内则认为非法设备，不允许接入	应核查是否建立无线接入设备和合法移动终端配置库， 并通过配置库识别非法设备	1) 建立无线接入设备和合法移动终端配置库，并可以进行比对识别 2) 无线接入设备和合法移动终端配置库信息

十三、物联网安全扩展要求测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
感知节点设备物理防护	a) 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	许多感知节点资源受限，成本低廉，可能散布在无人职守的区域，如果所处物理环境对感知节点设备造成物理破坏，将会导致感知节点无法正常工作，并很难及时发现	1) 核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备所处物理环境具有防挤压、防强振动等能力的说明，是否与实际情况一致 2) 核查感知节点设备所处物理环境是否采取了防挤压、防强振动的防护措	1) 感知节点设备所处物理环境的设计或验收文档明确了感知节点设备所处物理环境的防物理破坏要侧如具有防挤压、，防强振动等的说明。 2) 感知节点设备所处物理环境采取了防物理破坏的相应防护措施，例如，室外监控摄像机的外部安装需要在建筑物的外墙上安装孔和支架，并注意避免强烈撞击
	b) 感知节点设备在工作状态所处物理环境应能正确反应环境状态（如温湿度传感器不能安装在阳光直射区域）	避免感知节点设备所处物理环境错误，导致采集到错误信息或采集不到信息	1) 核查感知节点设备所处物理环境的设计或验收文档，是否有感知节点设备在工作状态所处物理环境的说明，是否与实际情况一致 2) 核查感知节点设备所处物理环境是否能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）	1) 感知节点设备所处物理环境的设计或验收文档明确了感知节点设备在工作状态所处物理环境的说明 2) 感知节点设备所处物理环境能正确反映环境状态，例如温湿度传感器不能安装在阳光直射区域，监控摄像机的镜头不要对准强光处

	c) 感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等	感知节点资源有限，常采用短距离无线通信方式，如果所处环境存在强干扰阻挡屏蔽等情况，容易导致感知节点无法传输信息	1) 核查感知节点设备所处物理境的设计或验收文档，是否有感知节点设备所处物理环境防强干扰，防阻挡屏蔽等能力说明，是否与实际情况一致 2) 核查感知节点设备所处物理环境是否采取了防强干扰，防阻挡屏蔽等能防护措施	1）感知节点设备所处物理环境的设过或验收文档有感知节点设备所处物理环境防强干扰、 防阻挡屏蔽等能力的说明。例如，红外摄像机安装位置应该避免潮湿、多尘、强电磁辐的场所 2) 感知节点设备所处物理环境采取了防强干扰，防阻挡屏蔽等能措施。例如， 室外监控摄像机探头如果经常会遇上热气而起雾， 考虑安装镜头除雾器；如果监控摄像机探头安装在玻璃后面，要确保镜头靠近玻璃 （如果距离太远，玻璃容易反射图像 ）
	d) 关键感知节点设备应具有可供长时间工作的电力供应 （关键网关节点设备应具有持久稳定的电力供应 ）	感知节点和网关节点设备往往 24 小时开机，无专人职守， 如果关键感知节点没有可供长时间工作的电力供应 （关键网关节点设备应具有持久稳定的电力供应） ，将会因电力耗尽而无法正常工作	1) 核查关键感知节点设备 （关键网关节点设备 ）电力供应设计或验收文档，是否标明电力供应要求，其中是否明确保障关键感知节点设备长时间工作的电力供应措施 （关键网关节点设备持久稳定的电力供应措施 ） 2) 核查是否具有相关电力供应措施的运行维护记录，是否与电力供应设计一致	1) 关键感知节点设备 （关键网关节点设备 ）电力供应设计或验收文档标明了电力供应要求， 其中明确了保障关键感知节点设备长时间工作的电力供应措施 （关键网关节点设备持久稳定的电力供应措施 ）. 例如， 监控摄像机交流电压适应范围一般是 200-240V, 抗电源电压变化能力较弱， 在系统中使用时需要添加稳压电源 2) 核查相关电力供应措施的运行维护记录，确保与电力供应设计一致

接入控制	应保证只有授权的感知节点可以接入	感知节点数量巨大，无专人职守，这些设备可能被劫持或物理破坏，然后非法节点伪装成客户端或者应用服务器发送数据信息、执行操作，因此需要对感知节点进行标识和鉴别，以保证只有授权的感知节点可以接入	1) 核查感知节点接入机制设计文档是否包括防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述 2) 对边界和感知层网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法	1) 感知节点接入机制设计文档包括了防止非法的感知节点设备接入网络的机制以及身份鉴别机制的描述。通常采用各类感知终端和接入设备在接入网络时设备唯一标识，并禁用闲置端口、设置访问控制策略等防护手段。例如，在视频专网中部署视频接入安全管理系统，对摄像机及其它前端IP设备进行品牌、型号、IP，MAC等绑定，并进行准入策略管控，只有通过认证的设备才允许接入 2) 对边界和感知层网络进行渗透测试，不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法
入侵防范	a) 应能够限制与感知节点通信的目标地址，以避免陌生地址的攻击行为	对感知节点通信的目标地址进行限制，防止被攻击后参与DDOS攻击或成为攻击跳板	1) 核查感知层安全设计文档，是否有对感知节点通信目标地址的控制措施 2) 核查感知节点设备，是否配置了对感知节点通信目标地址的控制措施 3) 对感知节点设备进行渗透测试，测试是否能够限制感知节点设备对违反访问控制策略的通信目标地址进行访问或攻击	1) 感知层安全设计文档有对感知节点通信目标地址的控制措施说明。例如，在网络摄像机的汇聚交换机上划分VLAN 2) 感知节点设备配置了对感知节点通信目标地址的控制措施，相关配置参数符合设计要求。例如，在汇聚交换机上划分VLAN,在汇聚交换机的接口上配置相关的VLAN数据 3) 对感知节点设备进行渗透测试，能够限制感知节点设备对违反访问控

				制策略的通信目标地址进行访问或攻击
	b) 应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为	对网关节点通信目标地址进行限制，防止被攻陷后参与 DDOS 攻击或成为攻击跳板	1) 核查感知层安全设计文档，是否有对网关节点通信目标地址的控制措施说明 2) 核查网关节点设备，是否配置了对网关节点通信目标地址的控制措施，相关配置参数是否符合设计要求 3) 对网关节点设备进行渗透测试，能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击	1) 感知层安全设计文档有对网关节点通信目标地址的控制说明。例如，通过防火墙或配置交换机 VLAN 对网关节点通信目标地址进行控制 2) 网关节点设备配置了对网关节点通信目标地址的控制措施，相关配置参数符合设计要求。例如，相关防火墙或交换机 VLAN 的配置参数符合设计要求 3) 对网关节点设备进行渗透测试，测试是否能够限制网关节点设备对违反访问控制策略的通信目标地址进行访问或攻击

感知节点设备安全	a) 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	感知节点设备数量巨大，往往在线批量进行软件应用配置或变更，如果没有采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更，容易导致感知节点监测数据泄露或设备被非法关闭	1) 核查感知节点设备是否采取了一定的技术手段防止非授权用户对设备上软件应用进行配置或变更 2) 通过试图接入和控制传感网访问未末授权的资源，测试验证感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源的行为控制是否有效	1）感知节点设备采取了一定的技术手段防止非授权用户对设备上软件应用进行配置或变更，例如，给感知节点设备配置安全性强用户名和登录密码 2) 感知节点设备的访问控制措施对非法访问和非法使用感知节点设备资源行为控制有效
	b) 应具有对其连接的网关节点设备（包括读卡器) 进行身份标识和鉴别的能力	很多物联网感知节点是处在无人值守的位置，就给了攻击者可趁之机，便于从无人值守的设备中获得用户身份等的隐秘信息，并以此设备对通信网络进行攻击，因此需要具有对其连接的网关节点设备 (包括读卡器) 进行身份标识和识别的能力	1) 核查是否对连接的网关节点设备 (包括读卡器) 进行身份标识与鉴别 2) 测试验证是否不存在绕过身份标识与鉴别功能的方法	1) 连接的网关节点设备 (包括读卡器) 进行身份标识与鉴别，配置了符合安全策略的参数 2) 不存在绕过身份标识与鉴别功能的方法
	c) 应具有对其连接的其他感知节点设备 (包括路由节点) 进行身份标识和鉴别的能力	攻击者通过假冒网络中已有的感知节点或网关节点，可以监听传感网络中传输的信息，向传感网络中发布假路由信息或传送假的数据信息、进行拒绝服务攻击等。需要具有对其连接的其他感知节点设备 （包括路由节点) 进行身份标识和鉴别的能力	1) 核查是否对某他感知节点设备 (包括路由节点) 设备进行身份标识与鉴别，是否配置了符合安全策略的参数 2) 测试验证是否不存在绕过身份标识与鉴别功能的方法	1) 对连接的某他感知节点设备 (包括路由节点) 设备进行身份标识与鉴别，配置了符合安全策略的参数 2) 不存在绕过身份标识与鉴别功能的方法

网关节点设备安全	a) 应设置最大并发连接数	由于物联网感知节点数量巨大，如果大量感知节点设备在很短时间内接入网络或向网关节点发出连接请求，而网关节点全部进行响应和连接，很可能会导致网关节点超负荷运行或宕机，需要对网关节点设备设置最大并发连接数	核查网关节点设备是否配置了最大并发连接数参数	网关节点设备配置了最大并发连接数参数
	b) 应具备合法的连接设备 (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	物联网感知层大量使用无线通信和电子标签技术， 大部分为无人值守设备， 使得隐私信息威胁问题非常突出。如果隐私信息被攻击者非法获取，将会给用户带来安全隐患。网关节点设备需要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，降低被攻击者非法获取隐私数据的风险	1) 核查网关节点设备是否能否对连接设备 (包括终端节点、 路由节点、 数据处理中心) 进行标识并配置了鉴别功能 2) 测试验证是否不存在绕过身份标识与鉴别功能的方法	1) 网关节点设备能对连接设备 (包括终端节点、 路由节点、 数据处理中心) 进行标识并配置了鉴别功能； 或者部署了接入安全管理系统， 可以进行准入策略管控， 只有通过认证的设备才允许接入 2) 不存在绕过身份标识与鉴别功能的方法
	c) 应具备过滤非法节点和伪造节点所发送的数据的能力	攻击者通过假冒网络中已有的感知节点或网关节点，可以监听传感网络中传输的信息，向传感网络中发布假的路由信息或传送假的数据信息、进行拒绝服务攻击等。需要具备过滤非法节点和伪造节点所发送的数据的能力	1) 核查是否具备过滤非法节点和伪造节点发送的数据的功能 2) 测试验证是否能够过滤非法节点和伪造节点发送的数据	1) 具备过滤非法节点和伪造节点发送的数据的能力。例如，部署视频专用防火墙， 仅允许通行相关视频网络协议，对其他协议进行阻挡；并启动终端准入策略，根据注册终端、未注册终端、未知设备、替换设备终端类型进行不同的阻断和记录策略 2) 能够过滤非法节点和伪造节点发送的数据

	d) 授权用户应能够在设备使用过程中对关键密钥进行在线更新	由于物联网中的感知节点和网关节点数量巨大，部署位置广泛，人工更新关键密钥则变得更加困难，因此需要提供授权用户在设备使用过程中对关键密钥进行在线更新的能力	核查感知节点设备是否对其关键密钥进行在线更新	感知节点设备支持对其关键密钥进行在线更新
	e) 授权用户应能够在设备使用过程中对关键配置参数进行在线更新	由于物联网中的感知节点和网关节点数量巨大，部署位置广泛，人工更新关配置参数则变得更加困难，因此需要提供授权用户在设备使用过程中对关键配置参数进行在线更新的能力	核查感知节点设备是否支持对其关键配置参数进行在线更新及在线更新方法是否有效	感知节点设备支持对关键配置参数进行在线更新，并且在线更新方式有效
抗数据重放	a) 应能够鉴别数据的新鲜性，避免历史数据的重放攻击	数据新鲜性 (data freshness) 是指对所接收的历史数据或超出时限的数据进行识别的特性。可以使用时间戳或计数器，提供数据新鲜性保护。 在联网监控视系统中，用于防止攻击者替换监控视频 (掩饰非法活动)	1) 核查感知节点设备鉴别数据新鲜性的措施，是否能否避免历史数据重放 2) 将感知节点设备历史数据进行重放测试，验证其保护措施是否生效	1) 感知节点设备在读取或状态控制过程中具有数据传输新鲜性保护机制，如时间戳、序列号等内容。 2) 将感知节点设备历史数据进行重放，感知节点设备应能在读取或状态控制过程中发现时间戳、 序列号或者其他新鲜性保护信息不符合要求
	b) 应能够鉴别历史数据的非法修改， 避免数据的修改重放攻击	物联网的感知节点往往是大规模部署，并且存在大量无人值守设备，这些设备可能被劫持，攻击者通过假冒网络中已有的感知节点或网关节点，可以对历史数据进行非法修改，向传感网络中发布假的路由信息或传送假的数据信息。需要能够鉴别历史数据的非法修改，避免数据的修改重放攻击	1) 核查感知层是否配备检测感知节点设备历史数据被非法篡改的措施，在检测到被修改时是否有必要的恢复措施 2) 测试验证是否能够避免数据的修改重放攻击	1) 具备对网络节点存储数据的完整性检测机制，实现鉴别信息、协议转换规则、 审计记录等重要业务数据的完整性检测， 具备对传输数据的完整性检测机制， 实现重要业务数据传输完整性保护，例如：校验码、消息摘要和数字签名等 2) 具有通信延时和中断的处理机制，能够避免数据的修改重放攻击

数据融合处理	应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用	传感网络和通信网络是异构网络，在异构网络数据汇总时，攻击者可以利用传感网络的安全性等特点，伪造通信网络的命令指示，从而使得物联网设备断开或者做出错误的操作或响应；或诱使物联网设备向通信网络发送假冒的请求制应，从而使得通信网络做出错误的判断而影响网络安全。需要对来自传感网的改据进行数据融合处理，使不同种类的数据可以在同一个平台被使用	1) 核查是否提供对来自传感网的数据进行数据融合处理的功能 2) 测试验证数据融合处理功能是否能够处理不同种类的数据	1) 具备对来自传感网的数据进行数据融合处理的功能，实现对感知数据、控制数据及服务关联数据的加工、处理和协同，为物联网用户提供对物理世界对象的感知和操控服务的接口 2) 数据融合处理功能能够处理不同种类的数据，将感知对象和控制对象与传感网系统、标签识别系统、智能设备接口系统等以数据通信类接口或数据通类接口的方式进行关联，实现物理世界和虚拟世界的接口绑定
感知节点管理	a) 应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护	一旦感知节点设备或网关节点设备被非法关闭（或损坏），将导致相关数据无法采集。在联网监控视频系统发生该现象时，将导致非法活动不能被及时发现和追朔	1) 访谈系统运维负责人是否有专门的人员对感知节点设备、网关节点设备进行定期维护，由何部门或何人负责，维护周期多长 2) 核查感知节点设备、网关节点设备部署环境维护记录是否记录维护日期、维护护人、维护设备、故障原因、维护结果等方面内容	1) 有专门的人员对感知节点设备、网关节点设备进行定期维护。如果物联网的定期维护由第三方提供服务，应提出人员资质、身份审核、可信证明、诚信承诺等要求，以确保其在物联网系统维护过程中的安全可信 2) 感知节点设备、网关节点设备部署环境维护记录包括了维护日期、维护护人、维护设备、故障原因、维护结果等方面内容

	b) 应对感知节点设备、 网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确的规定， 并进行全程管理	物联网的感知节点往往是大规模部署，并且存在大量无人值守设备，需要对感知节点设备、网关节点设备入库、存储、部署、 携带、 维修、 丢失和报废等过程作出明确的规定，并进行全程管理	核查感知节点和网关节点设备安全管理文档是否覆盖感知节点设备、网关节点设备入库、 存储、 部署、 携带、 维修、丢失和报废等方面	1) 感知节点和网关节点设备安全管理文档覆盖感知节点设备、 网关节点设备入库、 存储、 部署、 携带、 维修、丢失和报废等方面内容 2) 对于远程维护设备的， 应具有远程维护安全规范 3) 感知节点和网关节点设备安全管理文档， 应明确感知节点和网关节点设备到期废弃后， 需要对原来采集的数据、 访问日志等信息进行及时的备份或销毁管理， 部分设备在复用之前需要进行必要的初始化状态重置、 缓存数据清理等操作， 避免原系统信息的泄露。 高敏感数据的存储介质采取物理销毁的方式进行销毁
	c) 应加强对感知节点设备、网关节点设备部署环境的保密性管理， 包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等	物联网的感知节点和网关节点往往包含隐私数据， 一旦隐私数据被非法获取， 会造成隐私泄漏和恶意跟踪，给用户带来安全隐患。 需要加强对感知节点设备、 网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等	1) 核查感知节点设备、网关节点设备部署环境的管理文档中是否包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等内容 2) 核查是否具有感知节点设备、网关节点设备部署环境的相关保密性管理记录	1) 感知节点设备、 网关节点设备部署环境的管理文档中包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等内容 2) 具有感知节点设备、 网关节点设备部署环境的相关保密性管理记录

第四级增加或增强要求	应对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令	可控性是物联网最为特殊的地方，要采取措施来保证物联网不会因为错误而带来控制方面的灾难，包括控制判断的冗余性、控制命令传输渠道的可生存性、控制结果的风险评估能力等。需要对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限时可以影响对另一类数据采集终端的管理指令，	核查是否能够智能处理不同数据之间的依赖关系和制约关系	物联网设备、服务或者系统对对信息和数据的及时性、安全和隐私保护等方面有特定要求的应用场景（如健康服务、监测系统和紧急服务等），能够从感知终端、存储的历史背景信息或设定的输入等获取到不同数据之间的依赖关系和制约关系等，并根据这些关系进行智能处理，一类数据达到某个门限时可以影响对另一类数据采集终端的影响

十四、工业控制系统安全扩展要求测评指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据
室外控制设备物理防护	a) 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	对于室外的控制设备需保证其物理环境安全，应放置在采用铁板或其他防火材料制作的箱体或装置中，并紧固于箱体或装置中。 箱体或装置具有透风、散热、防盗、防雨和防火能力等，确保控制系统的可用性，使控制设备工作在其正常工作温度范围内，保护控制设备免受火灾、雨水等外部环境的影响，避免控制设备因宕机、线路短路、火灾、被盗等因素引发其他生产事故，从而影响生产运行	1) 核查是否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 2) 核查箱体或装置是否具有透风、散热、防盗、防雨和防火能力等	1) 室外控制设备均放置于采用铁板其或他防火材料制作的箱体或装置中并紧固 2) 箱体材质使用铁板或其他防火材料制作的证明 3) 箱体或装置具有通风散热口、散热孔或排风装置，能透风、散热，或者环境温度在控制设备正常工作温度范围内 4) 箱体或装置有防盗措施，并实施 5) 箱体或装置具有防雨能力，箱体或装置内无雨水痕迹

	b) 室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行	高电压高场强等强电磁干扰可能使控制设备工作信号失真，性能发生有限度的降级，甚至可能使系统或设备失良，严重时会使系统或设备发生故障或事故，而高温等强热源导致环境温度偏高，若超过控制设备最高工作温度，则会导致控制设备无法正常工作，同时加速控制设备老化。因此，室外控制设备应远离雷电、沙暴、尘暴、大阳噪声、大功率启停设备、高压输电线等强电磁干扰环境和加热炉、反应釜、蒸汽等强热源环境，确保环境电磁干扰水平和环境温度在控制设备正常工作范围之内，以保证控制系统的正常运，对于确实无法远离强电磁干扰、强热源环境的室外控制设备，应做好应急处置及检修，保证控制设备的正常运行	1) 核查放置位置是否远离强电磁干扰和热源等环境 2) 无法避免时，核查是否有应急处置及检修维护记录	1) 室外控制设备远离雷电、沙暴、尘暴、太阳噪声、大功率启停设备、高压输电线等强电磁干扰环境和加热炉、反应釜、蒸汽等强热源环境 2) 对于无法远离强电磁干扰、强热源等环境的室外控制设备，有应急处置及检修维护记录，检修维护记录显示控制设备均正常运行
网络架构	a) 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	工业控制系统中现场设备层、现场控制层、过程监控层、生产管理层与生产过程强相关，而企业资源管理层等企业其他系统与生产过程弱相关，同时企业其他系统可能与互联网相连，为此工业控制系统与企业其他系统之间划分为两个区域，区域间应采用单向的技术隔离手段，保证数据流，工业控制系统单向流向企业其他系统，即只读属性，不允许写操作	1) 核查工业控制系统和企业其他系统之间是否否署有效的单向隔离策略实施访问控制 2) 核查是单向隔离设备设置有效的隔离措施 3) 核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施	1) 工业控制系统与企业其他系统之部署单向隔离设备 2) 单向隔离设备设置有效的隔离措施，数据只能从工业控制系统单向流向企业其他系统，同时不存在多余的策略 3) 使用无线通信的工业控制系统边界采用与企业其他系统隔离强度相同的措施

	b) 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	工业控制系统内部根据承载业务的不同和网络架构的不同，进行合理的分区分域，通常将具有相同业务特点的工业控制系统划分为一个独立区域，不同业务特点的工业控制系统应划分为不同的安全域，在不同安全域之间采用工业防火墙、虚拟局域网等技术手段进行隔离	1) 核查工业控制系统内部是否根据业务特点划分了不同的安全域 2) 核查各安全域之间访问控制设备是否配置了有效的访问控制策略，将各安全域进行了隔离	1) 工业控制系统内部根据业务特点划分了不同的安全域 2) 不同的安全域之间访问控制设备运行正常，且配置了有效的访问控制策略，无无效或多余的访问控制策略
	c) 涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其他数据网及外部公共信息网的安全隔离	涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备进行组网，禁止与其他数据网共用网络设备，在物理层面上实现与其他数据网及外部公共信息网的安全隔离，禁止生产网与其他网络之间直接进行通信的行为	核查涉及实时控制和数据传输的工业控制系统是否在物理层面上独立组网	涉及实时控制和数据传输的工业控制系统，使用了独立的网络设备进行组网，在物理上与其他数据网及外部公共信息网安全隔离、无连接
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认证技术手段实现身份认证、访问控制和数据加密传输	对于 SCADA. RTU 等工业控制系统可可能使用使用广域网进行控制指令或相关数据交换，在控制指令或相关数据交换过程中，应采用加密认证手段实现身份认证，访问控制和数据加密传输。只有目标身份通过认证后，才能进行数据交换，数据交互过程中进行访问控制，即对通信五元组甚至控制指令进行管控，并在广域网传输控制过程中进行数据加密传输，防止非授权、恶意用户进入工业控制系统，防止控制指令或相关数据被窃取	核查工业控制系统广域网传输的控制指令或相关数据是否采用认证技术实现身份认证、访问控制和数据加密传输	工业控制系统广域网传输的控制指令或相关数据采用认证技术实现身份认证、访问控制和数据加密传输

访问控制	a) 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	工业控制系统中常采用工业专有协议和专有应用系统，而 E-Mail、Web、Telnet、Rlogin、FTP等通用应用和协议是网络攻击最常用的载体，应在工业控制系统区域边界、工业控制系统与企业其他系统之间部署访问控制设备，在保证业务正常通信的情况下，以最小化原则，只允许工业控制系统中使用的专有协议通过，拒绝 E-Mail、Web、Telnet、Rlogin、FTP等一切通用网络服务穿越区域边界进入工业控制系统网络	1) 核查在工业控制系统与企业其他系统之间的网络边界是否部署访问控制设备，是否配置访问控制策略 2) 应核查设备安全策略，是否禁止 E-Mail、Web、Telnet、Rlogin、FTP等通用网络服务穿越边界	工业控制系统与企业其他系统之间的网络达界部署访问控制设备，配置访问控制策略禁止 E-Mail、Web、Telnet、Rlogin、FTP等通用网络服务通过
	b) 应在工业控制系统内安全域和安全域之间的边界防护机制失效时，及时进行报警	工业控制系统内安全域与安全域之间边界防护安全管控故障或失效时，需要存在相应的检测机制，及时进行告警，便于安全管理员及时处理，避免边界防护的失效，防止存在大范围防护盲区	1) 核查设备是否可以在策略失效的时候进行告警 2) 核查是否部署监控预警系统或相关模块，在边界防护机制失效时可及时告警	1) 工业控制系统内安全域与安全域之间边界防护设备策略失效时进行告警 2) 部署或存在监控预警系统或模块，在边界防护机制失效时可及时告警
拨号使用控制	a) 工业控制系统需使用拨号访问服务的，应限制具有拨号访问权限的用户数量， 并采取用户身份鉴别和访问控制等措施	对采用拨号方式进行网络访问的工业控制系统，在网络访问过程中对用户的连接数量及会话数量进行限制，限制用户数量，同时对网络访问者进行身份鉴别验证，只有身份鉴别验证通过后才能建立连接，并对采用拔号方式的用户进行访问控制，限制用户的访问权限	核查拨号设备是否限制具有拨号访问权限的用户数量，拨号服务器和客户端是否使用账户口令等身份鉴别方式，是否采用控制权限账户等访问控制措施	1) 拨号设备限制具有拨号访问权限的用户数量 2) 拨号服务器和客户端使用账户口令等身份鉴别方式进行身份认证 3) 拨号服务器和客户端采用控制账户权限等访问控制措施

	b) 拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、特殊加密和访问控制等措	拨号服务器和客户端使用的操作系统可能存在安全漏洞，安装、配置不不符合安全需求，参数配置错误，使用、维护不符合安全需求。安全漏洞没有及时修补，应用服务和应用程序滥用，开放不必要的端口和服务等。这些漏洞会成为各种信息安全问题的隐患，一旦漏洞被有意或无意地利用，就会对系统的运行造成不利影响。因此需从账户管理和认证授权、日志、安全配置、文件权限、服务安全、安全选项等方面经安全加固的操作系统。同时在服务器与客户端建立通信时，应采取数字证书认证方式，对建立的通信内容进行加密，保证通信内容的保密性，，并对客户端进行访问控制	核查拨号服务器和客户端是否使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施	1) 拨号服务器和客户端使用经安全加固的操作系统 2) 拨号服务器和客户端采取数字证书认证、传输加密和访问控制等措施
无线使用控制	a) 应对所有参与无线通信的用户《人员、软件进程或者设备》提供唯一性标识和鉴别	无线通信网络是一个开放性网络，它使无线通信用户也不像有线通信用户受通信电缆的限制，而是可以在移动中通信，它在赋予无线用户通信自由的同时也给无线通信网络带来一些不安全因素，如通信内容容易被窃听、通信内容可以被更改和通信双方可能被假冒。因此对无线通信中需进行身份鉴别，在借助于运营商（无线）网络的组网中，需要对通信端（通信应用设备或通信网络设备）建立：基于用户的标识（用户名、证书等），标识具有唯一性且支持对该属性进行鉴别；在工业现场自建无线	1) 核查无线通信的用户在登录时是否采用了身份鉴别措施 2) 核查用户身份标识是否具有唯一性	1) 无线通信用户在登录时采用了身份鉴别措施 2) 无线通信用户身份标识具有唯一性

		(WIFI 、WirelessHART 、ISA100.1la. WIA-PA)网络中，通信网络设备应在组网过程中具备唯 -一标识，且支持对该设备属性进行鉴别		
	b) 应对所有参与无线通信的用户 （人员、软件进程或者设备 ）进行授权以及执行使用进行限制	无线通信中的应用设备或网络设备需支持对无线通讯策略进行授权 ，非授权设备或应用不能接入无线网络 ；非授权功能不能在无线通信网络中执行响应动作，对于授权用户对执行使用权限进行策略控制	核查无线通信过程中是否对用户进行授权，核查具体权限是否合理，核查未授权的使用是否可以被发现及告警	无线通信过程中对用能户进行授权，具体权限合理，未授权的使用可以被发现及告警
	c) 应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护	在无线通信过程中，对传输报文进行加密处理，加密方式包括对称加密 / 非对称加密、脱敏加密、 私有加密等， 保证无线通信过程的机密性，保证传输报文的机密性	核查无线通信信传输中是否采用加密措施 ，保证传输报文的机密性	无线通信信传输中是否采用加密措施 ，保证传输报文的机密性
	d) 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	在应用无线通信技术的工业生产环境中，应具备识别、检测工业环境中其他授权无线设备射频信号的应用，并对未授权的无线接入行为及应用进行审计、报警及联动管控，避免无线信号干扰影响生产、 避免未	核查工业控制系统是否可以实时监测其物理环境中发射的未经授权的无线设备； 监测设备是否能及时告警并对试图接入的无线设备进行屏蔽	1) 工业控制系统可实时监测其物理环境中发射的未经授权的无线设备 2) 监测设备能发现未经授权的无线设备试图接入或干扰控制系统的行为

	无线设备，报告未经授权试图接入或干扰控制系统的行为	授权用户通过无线接入控系统对生产造成破坏		
控制设备	a) 控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制	控制设备自身应实现对应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求； 考虑到控制系统历史原因、 更新周期缓慢和自主可控范围较低，在其自身不满足上述条件时，需通过上位控制系统或其他管理设备实现同等功能或通过管理手段进行控制	1) 核查控制设备是否具有身的鉴别、访问控制和安全审计等功能， 如控制设备具备上述功能， 则按照通用要求测评和安全审计 2) 如控制设备不具备上述功能， 则核查是否由由其上位控制或管理设备实现同等功能或通过管理手段控制	1) 控制设备自身具有身份鉴别、访问控制和安全审计等功能，参考通用要求 2) 控制设备自身不具备身份份鉴别、访问控制和安全审计等功能，上位控制系统或其他管理设备实现身份鉴别、访问控制和安全审计等功能 3）上位控制或其他管理设备也有实现身份鉴别、访问控制和安全审计等功能的，存在管理措施进行身份鉴别、访问控制和安全审计控制
	b) 应在经过充分测试评估，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作	由于工业控制系统专用软件较多的特殊性 , 相关应用软件与补丁可能存在兼容性问题，考虑到工业控制系统需长期稳定地运行 , 在对控制设备进行补丁更新、固件更新时，需要对控制系统进行充分的测试验证。兼容性测试、 严格的安全评估后， 在停产维修阶段对离线系统进行更新升级，保障控制系统的可用性	1) 核查是否有测试报告或测试评估记录 2) 核查控制设备版本、 补丁及固件是否经过充分测试后进行了更新	对控制设备进行补丁更新、固件更新等工作经过充分测试评估 ，有测试报告或测试评估记录

	c) 应关闭或拆除控制设备的软盘驱动、光盘驱动、 USB接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理	软盘驱动、光盘驱动、 USB接口、 串行口或多余网口等控制设备外设的使用，为病毒、木马、蠕虫等恶意代码入侵提供了途径， 关闭或拆除控制设备上不需要的外设接口可减少被感染的风险 ，避免通过不必要的外设接口对工业控制系统造成破坏。如不具备拆除条件或确需保留的，可采用主机外设统一管理设备、隔离存放有外设接口的工业主机 / 控制设备等安全管理技术手段进行严格管控	1) 核查控制设备是否关闭或拆除设备的软盘驱动、 光盘驱动、 USB接口、串行口或多余网口 2) 核查保留的软盘驱动、光盘驱动、USB接口、串行口或多余网口等是否通过相关的措施实施严格的监控管理	1) 控制设备关闭或拆除设备的的软盘驱动、光盘驱动、 USB接口、串行口或多余网口 2) 保留的软盘驱动、光盘驱动、 USB 接口、串行口或多余网口等有相关技术措施进行严格监控管理
	d) 应使用专用设备和专用软件对设备进行更新	对控制设备更新应使用专用硬件设备和专用软件进行更新，确保专用设备和专用软件的独立性，防止交叉感染	核查是否使用专用设备和专用软件对控制设备进行更新	使用专用设备和专用软件对控制设备进行更新，有明显的标识和相应的登记记录
	e) 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	控制设备上线前，需要进行脆弱性检测以及恶意代码检测，确保控制设备固件中不存在恶意代码程序	核查由相关部门出具或认可的控制设备的检测报告， 明确控制设备固件是否不存在恶意代码程序	控制设备有相关部门出具或认证葯检测报告，明确控制设备固件中不存在恶意代码程序
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	工业企业在采购重要及关键控制系统或网络安全专用产品时，应该了解该产品是否已通过国家相关的认证标准，并且在相关专业机构进行了安全性检测。重要设备可参考国家互联网信息办公室会同工业和信息化部、 公安部、 国家认证认、 监督管理委员会等部门制订的《网络关键设备和网络安全专用产品目录》	1) 访谈安全管理员系统使用的工业控制系统重要设备及网络安全专用产品是否通过专业机构的安全性检测 2) 核查工业控制系统是否有通过专业机构出具的安全性检测报告	工业控制系统重要设备及网络安全专用产品有通过专业机构出具的安全性检测报告

外包软件开发	应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容	工业企业在进行外包项目时，应该与外包公司及控制设备提供商签署保密协议或合同，以保证其不会将本项目重要建设过程及内容进行宣传及案例复用，目的在于保障工业企业在建设时期的敏感信息、重要信息等内容不被泄露	核查是否在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的内容	外包软件开发合同中有针对开发单位、供应商针对设备及系统在生命周期内保密、禁止关键技术扩展和设备行业专用等方面的约束条款
第四级增加或增强要求	a) 应在工业控制系统与企业其他系统之间应划分为两个区域 ，区域间应采用符合国家或行业规定的专用产品实现单向安全隔离	工业控制系统中现场设备层、现场控制层、过程监控层、生产管理层与生产程强相关，而企业资源管理层等企业其他系统与生产过程弱相关，同时企业其系统可能与互联网相连，为此工业控制系统与企业其他系统之间划分为两个区，区域间应采用单向的技术隔离手段，保证数据流只能工业控制系统单向流向业其他系统，即只读属性，不允许写操作。单向安全隔离产品需符合国家规定，有行业特定规定的需符合行业规定	1) 核查工业控制系统和企业其他系统之间是否部署单向隔离设备 2) 核查是否采用了有效的单向隔离策略实施访问控制 3) 核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离强度相同的措施 4) 核查所使用的专用产品是否符合国家规定， 如有行业特殊规定的是否行业规定	1) 工业控制系统和企业其他系统之间部署单向隔离设备 2) 单向隔离设备设置有效的隔离措施，保证数据只能从工业控制系统单向流向企业其他系统，同时不存在多余的策略 3) 使用无线通信的工业控制系统边界采用与企业其他系统隔离强度相同的措施 4) 使用的单向隔离设备符合国家规定，行业特殊规定的符合行业规定，有国家或行业相应证书或证明

	b) 涉及实时控制和数据传输的工业控制系统禁止使用拨号访问服务	第四级安全区域边界相对于第三级增加了拨号控制使用要求，为了防止被任何人员或个体拨号访问，涉及实时控制和数据传输的工业控制系统需禁止使用拨号访问服务，保证实时控制和数据传输工业控制系统边界安全。对具有实时性要求得工业控制系统，采取禁止使用拨号访问服务策略，从物理层面实现实时控制数据传输功能的工业控制系统不被任何人员或个体拨号访问	核查涉及实时控制和数据传输的工业控制系统内是否禁止使用拨号访问服务	实时控制和数据传输的工业控制系统内未使用或禁止拨号访问服务