变更记录：

序号	变更原因	变更内容	编制（变更）人/时间	批准人/时间	备注
1	新建	全部，版本A/0	葛方隽/2021.3	吕萍/2021.3	

安全区域边界（S3A3G3）作业指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据	符合情况
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。 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 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	符合情况： 1)网络拓扑与实际链路情况一致 2）边界路由，边界访问控制设备的配置信息准确无误 3）不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，无非授权WiFi 部分符合情况：满足1），2），3）其中一条或者两条 不符合情况：无网络拓扑，边界设备配置信息有误，存在非授权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 IOS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。	1)非使用的端口均已关闭; 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。	符合情况：1）采取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 2）所有路由交换设备的闲置端口已手动关闭 3)部署了准入系统或进行MAC绑定，权限覆盖到所有终端 部分符合情况：满足1），2），3）其中一条或者两条 不符合情况：对入网设备无任何限制措施

	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	符合情况：1）采取技术手段或管理措施对非授权设备私自外联行为进行管控 2）限制了终端设备的D多余组件的使用，如双网卡，USB接口等 部分符合情况：满足1），2）其中一条或者两条 不符合情况：未对终端的外联行为进行任何限制措施
	a)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	符合情况：1）具备授权的无线网络 2）部署了接入网关，AC控制器，且采用安全的无线加密方案 3）能够对非授权无线设备进行检查、屏蔽 部分符合情况：满足1），2），3）其中一条或者两条 不符合情况：无线网络可以直接接入，无任何管控措施
	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，访问控制规则采用白名单机制	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。	1、边界部署了访问控制设备如（防火墙、网闸、边界路由等）设备; 2、边界设备是否配置了访问控制策略，访问控制策略配置是否有效; 3、访问控制策略调用到相应的端口、route-map、出入方向等。	符合情况：1）边界部署了访问控制设备 2）访问控制策略颗粒度满足要求且真实有效 3）访问控制策略应用到实际出入方向 部分符合情况：满足1），3） 不符合情况：边界未部署访问控制设备或者访问控制策略无效

访问控制	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。	1、访问控制策略相对精简，不存在无效的访问控制策略; 2、应删除默认的any to any全通策略，根据业务和资源访问需求逐条进行策略配置; 3、根据整体边界情况配置访问控制策略，不应出现同方向或者同网段出现访问控制策略逻辑不一致的情况。	符合情况：1）访问控制策略精简，不存在多余或无效的访问控制策略 2）不存在默认的访问控制策略any to any 3）边界访问控制策略出入方向逻辑一致 部分符合情况：满足1） 不符合情况：不存在或者边界访问控制策略无效，或存在默认全通的策略
	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		符合情况：1）访问控制策略具备明确的源目地址，端口协议等配置参数 部分符合情况：\ 不符合情况：访问控制策略颗粒度不够，没有明确的源目地址、端口等参数
	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.	边界设备的访问控制策略要根据业务的实际情况进行配置，如特定端口、特定源地址、目的地址或者协议等。访问控制策略要清晰明确，避免具体业务出现大段放行的访问控制策略。	符合情况：边界设备的访问控制策略要根据业务的实际情况进行配置，如特定端口、特定源地址、目的地址或者协议等 部分符合情况\ 不符合情况：边界设备未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
	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Web服务、FTP服务等进行管控	符合情况：配置基于应用协议的访问控制策略，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Web服务、FTP服务等进行管控 部分符合情况\ 不符合情况：未对应用层协议和内容进行访问控制

	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(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	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策略相符	符合情况：关键节点网络有入侵攻击检测设备，并配置了相应策略，且策略有效 部分符合情况：\ 不符合情况：未在关键节点部署入侵攻击检测产品或等效措施

入侵防范	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	符合情况：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 部分符合情况：满足1)和2），3）其中一条 不符合情况：未部署入侵检测设备对关键网络节点受到的内部攻击进行检测。
	c)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	符合情况：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 部分符合情况：满足1)和2），3）其中一条或者两条 不符合情况：未部署对网络攻击行为进行检测和分析的产品或设备

	d)当检测到攻击行为时，记录攻击源IP、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	符合情况：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 部分符合情况：满足1），2）其中一条或者两条 不符合情况：无法对攻击行为的类型，IP，时间等攻击信息进行记录并及时提供告警
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。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，手动远程更新，手动本地更新等方	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升级，且升级时间与测评时间较为接近	符合情况：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升级，且升级时间与测评时间较为接近 部分符合情况：满足1），2）其中一条或者两条 不符合情况：未部署防恶意代码设备

	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	符合情况：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 部分符合情况：满足1），2），3）其中一条或者两条 不符合情况：未部署垃圾邮件防护产品，且未进行定期更新和升级。
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，且审计记录包含了重要的用户行为和重要安全事件	符合情况：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，且审计记录包含了重要的用户行为和重要安全事件 部分符合情况：\ 不符合情况：未部署审计平台且无法收集审计信息
	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	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	符合情况：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 部分符合情况：审计记录覆盖一部分但覆盖补全 不符合情况：未开启审计功能模块或审计记录无法进行查看

	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	符合情况：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 部分符合情况：\ 不符合情况：审计记录无法进行有效保护且存储时间达不到要求
	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	符合情况：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 部分符合情况\ 不符合情况：无法对远程访问的用户行为进行审计。
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)	符合情况：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 部分符合情况：满足1），2），3）、4）其中一条或者多条 不符合情况：不具备可信验证产品或者服务