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	

安全管理中心（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
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	符合情况：对管理员的登录进行认证；使用了管理工具或特定命令； 所有操作有日志记录。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
	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	符合情况：管理员有权限划分；权限不同于审计管理员和安全管理员。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
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进行操作，并对这些操作进行审计	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	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	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	符合情况：对管理员的登录进行认证；使用了管理工具或特定命令； 所有操作有日志记录。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
	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	符合情况：管理员有权限划分；权限不同于系统管理员和安全管理员；只有审计管理员可以查看审计分析数据; 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
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	符合情况：对管理员的登录进行认证；使用了管理工具或特定命令； 所有操作有日志记录。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
	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	符合情况：管理员有权限划分；权限不同于系统管理员和审计管理员；只有安全管理员可以配置安全策略有关的参数。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
	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	符合情况：网络拓扑图中有管理区；安全设备或组件的管理设备均在管理区。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。

集中管控	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	符合情况：采用安全方式对设备进行访问，并对配置信息进行记录。 不符合情况：未采用安全方式对设备进行访问，并对配置信息进行记录。
	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	具备设备监测功能的系统或平台	符合情况：具备设备监测功能的系统或平台 不符合情况：未具备设备监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	符合情况：设备日志进行了转发；平台具备审计分析功能；审计记录保有了至少6个月以上。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
	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	符合情况：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；通过平台或工具可以实施策略管理。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。
	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	符合情况：具有安全事件管理平台或工具；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。 部分符合情况： 满足上述其中一点，但未完全满足所有条件。 不符合情况：上述条件全不满足。