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	

安全计算环境-安全设备-堡垒机（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
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，堡垒机只有经过授权的合法用户才能访问，一般来说，用户登录堡垒机的方式包括:通过浏览器以WEB方式登录，通过SSH方式登录。无论是采用哪一种的登录方式，都需要对用户身份进行鉴别。 堡垒机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。	通过浏览器以WEB方式登录 打开浏览器，在地址输入框中输入堡垒机的URL地址，如https://xx.xx.xx.xx。回车后进入jumpserver堡垒机的登录界面，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，登录后，用户就可通过WEB界面对堡垒机进行配置管理 2)应核查堡垒机用户管理-用户列表，查看相应设置，看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。 3)查看系统设置-安全设置-密码校验规则里设置，并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	1)堡垒机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	符合情况：通过用户名口令方式登录，口令长度8位以上，口令复杂度包含大写字母、小写字母、数字，口令有效期为90天； 部分符合情况：通过用户名口令方式登录，口令长度8位以上，复杂度为小写字母、数字、特殊字符，但未配置口令有效期； 不符合情况：通过用户名口令方式登录，口令长度为6位，复杂度为纯数字，未配置口令有效期，口令为弱口令。
	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堡垒机	进入管理界面，应核查系统设置-安全设置-认证，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web登录连接超时并自动退出功能	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。 在限制登录失败次数框下，可以查看到“最大登录失败次数”的配置，应配置对应次数。 2)配置并启用了远程登录连接超时并自动退出功能。然后在左侧导航树中选择系统设置-安全设置-基本中，可以查看到“连接最大空闲时间”的配置。	符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，会话空闲30分钟自动退出； 部分符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，但未配置连接超时自动退出措施； 不符合情况：未配置登录失败处理功能和连接超时自动退出措施。
	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	为避免口令传输过程中别窃取，不应当使用明文传送的Telnet、HTTP服务，而应当采用SSH、HTTPS等加密协议等方式进行交互式管理	应询问系统管理员采用何种方式对堡垒机进行远程管理，核查通过WEB界面管理是否都通过https(SSL)协议进行加密处理	通过WEB界面进行远程管理时，通过https协议进行加密处理	符合情况：仅采用https协议进行管理，防止鉴别信息在网络传输过程中被窃听； 不符合情况：仅采用http协议进行管理，无法防止鉴别信息在网络传输过程中被窃听。
	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,目前主流堡垒机多采用“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，用户既要通过堡垒机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堡垒机	1)进入管理界面。然后在左侧导航树中选择用户管理-用户列表。 2）右侧显示用户列表信息，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“更新”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”。	查看该用户的认证方式应该为“本地口令+证书认证”。	符合情况：通过用户名口令和谷歌验证码方式登录，验证码长度为6位，有效时间为30秒； 不符合情况：通过用户名口令方式登录，未采用两种或两种以上鉴别技术对用户进行身份鉴别。
	a)应对登录的用户分配账户和权限	为了确保堡垒机的安全，需要对登录的用户分配账户，并合理配置账户权限	进入管理界面，然后在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息，点击该用户条目右侧的“更新”图标。 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。	符合情况：已对可登录用户分配账户和权限，相关管理员与职位相对应； 不符合情况：已启用匿名登录模式。
	b)应重命名或删除默认账户，修改默认账户的默认口令	对于堡垒机的默认账户，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	进入管理界面，然后在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 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认口令	堡垒机重命名或删除默认账户，修改默认账户的默认口令	符合情况：已重命名系统默认账户a*为***，且口令修改为复杂口令； 部分符合情况：未重命名系统默认账户a**,已修改口令为复杂口令； 不符合情况：未重命名系统默认账户名，口令为设备出厂默认口令。

访问控制	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	堡垒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，因此应及时清理路由器中的账户，删除或停用多余的账户	进入管理界面，在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1) 应核查堡垒机用户账户列表，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	堡垒机用户账户列表不存在多余或过期账户，不存在共享用户	符合情况：设备中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况; 部分符合情况：管理员用户与账户之间一一对应，未发现共享账户的情况，但a*、s*为多余账户; 不符合情况：可登录账户仅有a*，所有管理员均通过a*登录。
	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	然后在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 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。 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。	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，如禁止对管理用户同时赋予配置管理员和审计管理员权限。	符合情况：已配置安全管理员s*、审计管理员a*、系统管理员s*，授予管理用户所需的最小权限; 部分符合情况：已配置安全管理员s*、系统管理员s*，但未配置审计管理员; 不符合情况：可登录账户仅有a*，未授予管理用户所需的权限分离，实现管理用户的权限分离。
	e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	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。	进入管理界面，然后在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1)应核查是否进行角色划分，确认访问控制策略仅由管理员进行管理。	用户的访问控制规则由管理进行管理;	符合情况：用户的访问控制规则由管理进行管理。 不符合情况：管理员无法配置访问规则。
	f)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、数据库表级	进入管理界面，在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1)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	访问控制规则由管理进行管理,主体为用户账号，客体为功能模块，访问控制力度为功能模块;	符合情况：访问控制规则由管理进行管理,主体为用户账号，客体为功能模块，访问控制力度为功能模块; 不符合情况：所有访问的模块均一致。
	g)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。	进入管理界面，进入管理界面，在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1）查看是否有安全标记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。	查看到具有安全标记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。	符合情况：查看到具有安全标记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。 不符合情况：未设置敏感标记。
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	为了对堡垒机的运行状况、管理记录等进行检测和记录，需要启用日志审计功能，并伴随一些指示性问题或事件的描述信息。 堡垒机的系统日志信息通常输出至各种第三方审计或者日志服务器,在缺省情况下，控制台端口上的日志功能处于启用状态	进入管理界面，在左侧导航树中选择日志审计,右侧显示各类日志信息。 在右侧显示"日志设置"页面，能够查看到登录日志、FTP日志、操作日志、改密日志和批量命令等日志记录。	堡垒机能够正确记录关键用户行为，以及对用户行为记录进行保存。	符合情况：已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户; 不符合情况：无审计模块，无法对重要的用户行为和安全事件进行审计。
	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	对于堡垒机来说，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	进入管理界面。然后在左侧导航树中选择日志审计,右侧显示各类日志信息。 登录日志服务器，并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堡垒机的IP。 在日志服务器上，根据IP地址选择堡垒机后，便可对该堡垒机的日志进行核查，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。	符合情况：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。 部分符合情况：仅有用户信息、登录时间。 不符合情况：无审计模块。
	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	进入管理界面。然后在左侧导航树中选择日志审计,右侧显示各类日志信息。 登录日志服务器，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堡垒机的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，便可实现堡垒机数据的备份和保护。	堡垒机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	符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，并留存半年以上，能够避免受到未预期的删除、修改或覆盖; 部分符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，但审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖; 不符合情况：未对审计记录记录进行保护，审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖。

	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	符合情况：审计进程权限配置合理，仅授权用户可终止审计进程； 不符合情况：审计进程权限配置不合理，部分普通用户可关闭审计进程。
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	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	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，需要对远程管理堡垒机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。	登录设备进行核查。进入管理界面,后在左侧导航树中选择系统管理》配置,查看登录地址限制列表;	设备本地设置访问控制列表限制终端接入范围。	符合情况：已限制终端接入地址范围，仅允许通过10.*.*.*/32地址进行管理; 部分符合：已限制终端接入地址范围，但限制登录地址范围为10.*.*.*/16，可登录地址范围过大; 不符合情况，未限制终端接入方式或网络地址范围，任意地址均可登录。
	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	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	符合情况：定期对安全设备进行漏洞扫描，发现漏洞及时修复，并形成报告。 部分符合情况：定期进行漏洞扫描，但未进行漏洞修复。 不符合情况：未定期进行扫描，且无法及时对漏洞进行修复。
	f)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，或在堡垒机及其他防护设备用入侵检测功能，以检查是否发生了入侵和攻击	此项不适合，该项要求一般在安全设备上实现	此项不适合，该项要求一般在安全设备上实现	此项不适合，该项要求一般在入侵设备上实现
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	1) 应核查是否安装了防恶意代码软件或相应功能的软件，定期进行升级和更新防恶意代码库; 2) 应核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为; 3) 应核查当识别入侵和病毒行为时是否将其有效阻断。	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	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	查看设备是否具有可信根芯片	查看设备是否具有可信根芯片	符合情况：安装了可信根芯片，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。 不符合情况：未安装可信根芯片，无法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。
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复，本条款要求对鉴别数据、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在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；

数据完整性	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能； 部分符合：无部分符合 不符合：系统采集信息非业务必要；

个人信息保护	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用； 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露；

安全计算环境-安全设备-防火墙（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
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括: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://xxx。回车后进入防火墙的登录界面，，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界面对防火墙进行配置管理: 1)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。 2)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	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	符合情况：通过用户名口令方式登录，口令长度8位以上，口令复杂度包含大写字母、小写字母、数字，口令有效期为90天; 部分符合情况：通过用户名口令方式登录，口令长度8位以上，复杂度为小写字母、数字、特殊字符，但未配置口令有效期; 不符合情况：通过用户名口令方式登录，口令长度为6位，复杂度为纯数字，未配置口令有效期，口令为弱口令。
	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	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。 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，。 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，。 2)配置并启用了远程登录连接超时并自动退出功能。 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，: 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，	符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，会话空闲30分钟自动退出; 部分符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，但未配置连接超时自动退出措施; 不符合情况：未配置登录失败处理功能和连接超时自动退出措施。
	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	为避免口令传输过程中别窃取，不应当使用明文传送的Telnet、HTTP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界面管理是否都通过SSL协议进行加密处理	通过WEB界面进行远程管理时，通过SSL协议进行加密处理	符合情况：仅采用https协议进行管理，防止鉴别信息在网络传输过程中被窃听; 不符合情况：仅采用http协议进行管理，无法防止鉴别信息在网络传输过程中被窃听。
	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	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， 2）右侧显示用户列表信息， 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"，。	，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"。	符合情况：通过用户名口令和谷歌验证码方式登录，验证码长度为6位，有效时间为30秒; 不符合情况：通过用户名口令方式登录，未采用两种或两种以上鉴别技术对用户进行身份鉴别。

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	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，。 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	符合情况：已对可登录用户分配账户和权限，相关管理员与职位相对应； 不符合情况：已启用匿名登录模式。
	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	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 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认口令	防火墙重命名或删除默认账户，修改默认账户的默认口令	符合情况：已重命名系统默认账户a*为***，且口令修改为复杂口令； 部分符合情况：未重命名系统默认账户a**,已修改口令为复杂口令； 不符合情况：未重命名系统默认账户名，口令为设备出厂默认口令。
	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	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， 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	符合情况：设备中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况； 部分符合情况：管理员用户与账户之间一一对应，未发现共享账户的情况，但a*、s*为多余账户； 不符合情况：可登录账户仅有a*，所有管理员均通过a*登录。
	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	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， 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 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	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	符合情况：已配置安全管理员s*、审计管理员a*、系统管理员s*，授予管理用户所需的最小权限； 部分符合情况：已配置安全管理员s*、系统管理员s*，但未配置审计管理员； 不符合情况：可登录账户仅有a*，未授予管理用户所需的权限分离，实现管理用户的权限分离。
	e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	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	符合情况：用户的访问控制规则由管理进行管理。 不符合情况：管理员无法配置访问规则。
	f)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	符合情况：访问控制规则由管理进行管理,主体为用户账号，客体为功能模块，访问控制力度为功能模块； 不符合情况：所有访问的模块均一致。
	g)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	符合情况：查看到具有安全标记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。 不符合情况：未设置敏感标记。

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	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， 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，	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	符合情况：已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户； 不符合情况：无审计模块，无法对重要的用户行为和安全事件进行审计。
	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	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，。 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。	符合情况：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。 部分符合情况：仅有用户信息、登录时间。 不符合情况：无审计模块。
	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	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， 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	符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，并留存半年以上，能够避免受到未预期的删除、修改或覆盖； 部分符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，但审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖； 不符合情况：未对审计记录记录进行保护，审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖。
	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	符合情况：审计进程权限配置合理，仅授权用户可终止审计进程； 不符合情况：审计进程权限配置不合理，部分普通用户可关闭审计进程。
	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	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	此项不适合，该项要求一般在服务器上实现

入侵防范	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	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，。 在右侧页面中，应该存在“服务名称”为“webui”，"ssh" 或"telnet'的服务规则。	设备本地设置访问控制列表限制终端接入范围。	符合情况：已限制终端接入地址范围，仅允许通过10.*.*.*/32地址进行管理; 部分符合：已限制终端接入地址范围，但限制登录地址范围为10.*.*.*/16，可登录地址范围过大; 不符合情况，未限制终端接入方式或网络地址范围，任意地址均可登录。
	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	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	符合情况：定期对安全设备进行漏洞扫描，发现漏洞及时修复，并形成报告。 部分符合情况：定期进行漏洞扫描，但未进行漏洞修复。 不符合情况：未定期进行扫描，且无法及时对漏洞进行修复。
	f)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	此项不适合，该项要求一般在入侵设备上实现
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	1) 应核查是否安装了防恶意代码软件或相应功能的软件，定期进行升级和更新防恶意代码库; 2) 应核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为; 3) 应核查当识别入侵和病毒行为时是否将其有效阻断。	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	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	查看设备是否具有可信根芯片	查看设备是否具有可信根芯片	符合情况：安装了可信根芯片，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。 不符合情况：未安装可信根芯片，无法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。

数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；

剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除;
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除;
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能; 部分符合：无部分符合 不符合：系统采集信息非业务必要;
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用; 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露;

安全计算环境-安全设备-日志审计（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
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，日志审计器只有经过授权的合法用户才能访问，一般来说，用户登录日志审计的方式为通过浏览器以WEB方式登录，日志审计为了便于用户管理，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，且需要对用户身份进行鉴别。 日志审计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)以奇安信网神日志审计为例，核查用户在登录时是否采用身份鉴别措施。 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日志审计的URL地址，如https://xx.xx.x.xx/las（默认地址）。回车后进入日志审计的登录界面，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，即可登录到日志审计。登录后，用户就可通过WEB界面对日志审计进行配置管理。 1）输入密码后，回车，即可登录到日志审计。登录后，用户就可使用命令行方式对日志审计进行配置管理。 2)应核查日志审计管理员账户列表，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。 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。	1)日志审计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。	符合情况：通过用户名口令方式登录，口令长度8位以上，口令复杂度包含大写字母、小写字母、数字，口令有效期为90天； 部分符合情况：通过用户名口令方式登录，口令长度8位以上，复杂度为小写字母、数字、特殊字符，但未配置口令有效期； 不符合情况：通过用户名口令方式登录，口令长度为6位，复杂度为纯数字，未配置口令有效期，口令为弱口令。
	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日志审计。	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。	以奇安信网神日志审计为例，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。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。 2)配置并启用了远程登录连接超时并自动退出功能。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。 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。	符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，会话空闲30分钟自动退出； 部分符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，但未配置连接超时自动退出措施； 不符合情况：未配置登录失败处理功能和连接超时自动退出措施。
	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	为避免口令传输过程中别窃取，不应当使用明文传送的Telnet、HTTP服务，而应当采用SSH、HTTPS等加密协议等方式进行交互式管理。	应询问系统管理员采用何种方式对日志审计进行远程管理,核查通过WEB界面管理是否都通过SSL协议进行加密处理。	通过WEB界面进行远程管理时，通过SSL协议进行加密处理。	符合情况：仅采用https协议进行管理，防止鉴别信息在网络传输过程中被窃听； 不符合情况：仅采用http协议进行管理，无法防止鉴别信息在网络传输过程中被窃听。

	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.目前主流日志审计多采用“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，用户既要通过日志审计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日志审计。	以奇安信网神日志审计为例，通过浏览器以WEB方式登录。 1)在登录界面查看是否需要同时输入动态验证码和密码来进行登录。 2)如果需要对用户进行两种或两种以上组合的鉴别技术，需要登录日志审计服务器，查看安装目录\server\ext目录下是否有 pass.txt文件，如果有则启用了“口令+动态验证”。	以奇安信网神日志审计为例，登录日志审计服务器，查看安装目录\server\ext目录下有 pass.txt文件。	符合情况：通过用户名口令和谷歌验证码方式登录，验证码长度为6位，有效时间为30秒； 不符合情况：通过用户名口令方式登录，未采用两种或两种以上鉴别技术对用户进行身份鉴别。
访问控制	a)应对登录的用户分配账户和权限	为了确保日志审计的安全，需要对登录的用户分配账户，并合理配置账户权限。	进入管理界面。然后点击“权限”>>“用户管理”，主页面点击指定用户，查看对应管理员权限。 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。	符合情况：已对可登录用户分配账户和权限，相关管理员与职位相对应； 不符合情况：已启用匿名登录模式。
	b)应重命名或删除默认账户，修改默认账户的默认口令	对于日志审计的默认账户，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。	进入管理界面。然后点击“权限”>>“用户管理”，主页面点击指定用户，查看对应账户权限。 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认口令	日志审计重命名或删除默认账户，修改默认账户的默认口令。	符合情况：已重命名系统默认账户a*为***，且口令修改为复杂口令； 部分符合情况：未重命名系统默认账户a**,已修改口令为复杂口令； 不符合情况：未重命名系统默认账户名，口令为设备出厂默认口令。
	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	日志审计中如果存在多余的、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。	进入管理界面。然后点击“权限”>>“用户管理”，主页面点击指定用户，查看对应账户权限。 1) 应核查日志审计用户账户列表，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。	日志审计用户账户列表不存在多余或过期账户，不存在共享用户。	符合情况：设备中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况； 部分符合情况：管理员用户与账户之间一一对应，未发现共享账户的情况，但a*、s*为多余账户； 不符合情况：可登录账户仅有a*，所有管理员均通过a*登录。
	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。	进入管理界面。然后点击“权限”>>“用户管理”，主页面点击指定用户，查看对应账户。 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。 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。	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。	符合情况：已配置安全管理员s*、审计管理员a*、系统管理员s*，授予管理用户所需的最小权限； 部分符合情况：已配置安全管理员s*、系统管理员s*，但未配置审计管理员； 不符合情况：可登录账户仅有a*，未授予管理用户所需的权限分离，实现管理用户的权限分离。
	e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	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	进入管理界面，然后在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1)应核查是否进行角色划分，确认访问控制策略仅由管理员进行管理。	用户的访问控制规则由管理进行管理；	符合情况：用户的访问控制规则由管理进行管理。 不符合情况：管理员无法配置访问规则。

	f)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	进入管理界面，在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1)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	访问控制规则由管理进行管理,主体为用户账号，客体未功能模块，访问控制力度未功能模块;	符合情况：访问控制规则由管理进行管理,主体为用户账号，客体为功能模块，访问控制力度为功能模块; 不符合情况：所有访问的模块均一致。
	g)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	进入管理界面，在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1）查看是否有安全标记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。	查看到具有安全标记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。	符合情况：查看到具有安全标记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。 不符合情况：未设置敏感标记。
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	为了对日志审计的运行状况、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。 日志审计的系统日志信息通常输出至本地存储，日志审计设备或者日志服务器,在缺省情况下，控制台端口上的日志功能处于启用状态。	以奇安信网神日志审计为例，在登录界面中输入日志审计管理员的用户名口令后，点击“登录”按钮，进入管理界面。然后点击“权限”>>“用户管理”，主页面点击指定用户，查看对应账户。日志审计设备通过报表体现重要用户行为，可以按需进行日志条目筛选。	日志审计设置正确的日志服务器地址、端口、以及日志级别和日志类型等信息。	符合情况：已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户; 不符合情况：无审计模块，无法对重要的用户行为和安全事件进行审计。
	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	对于日志审计来说，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。	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日志审计的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地址选择日志审计后，便可对该日志审计的日志进行核查，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。	符合情况：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。 部分符合情况：仅有用户信息、登录时间。 不符合情况：无审计模块。
	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。	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。 存储在设备本体的，查看设备设备本地记录，能否查询到半年前的日志记录。 存在服务器的，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日志审计的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，便可实现日志审计数据的备份和保护。 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，进而达到备份日志审计日志信息的目的。	日志审计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。	符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，并留存半年以上，能够避免受到未预期的删除、修改或覆盖; 部分符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，但审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖; 不符合情况：未对审计记录记录进行保护，审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖。

	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。	符合情况：审计进程权限配置合理，仅授权用户可终止审计进程； 不符合情况：审计进程权限配置不合理，部分普通用户可关闭审计进程。
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。	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。	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，需要对远程管理日志审计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。	进入管理界面。然后在界面导航栏>>权限>>IP 登陆限制，可以在此功能中，对登陆系统的客户端的 IP 地址进行限制，可以是单个 IP 址或者 IP 地址段；对已经有的限制规则可删除、可修改。	设备本地设置访问控制列表限制终端接入范围。日志审计设备自身有限制指定IP登录功能。	符合情况：已限制终端接入地址范围，仅允许通过10.*.*.*/32地址进行管理； 部分符合：已限制终端接入地址范围，但限制登录地址范围为10.*.*.*/16，可登录地址范围过大； 不符合情况，未限制终端接入方式或网络地址范围，任意地址均可登录。
	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),进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。	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。	符合情况：定期对安全设备进行漏洞扫描，发现漏洞及时修复，并形成报告。 部分符合情况：定期进行漏洞扫描，但未进行漏洞修复。 不符合情况：未定期进行扫描，且无法及时对漏洞进行修复。
	f)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，或在日志审计设备或服务器上，以检查是否发生了入侵和攻击。	此项不适合，该项要求一般在边界防护设备上实现。	此项不适合，该项要求一般在边界防护设备上实现。	此项不适合，该项要求一般在入侵设备上实现
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	1) 应核查是否安装了防恶意代码软件或相应功能的软件，定期进行升级和更新防恶意代 码库; 2) 应核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为; 3) 应核查当识别入侵和病毒行为时是否将其有效阻断。	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	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	查看设备是否具有可信根芯片	查看设备是否具有可信根芯片	符合情况：安装了可信根芯片，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。 不符合情况：未安装可信根芯片，无法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。
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；

	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能； 部分符合：无部分符合 不符合：系统采集信息非业务必要；
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施， 禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用； 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露；

安全计算环境-安全设备-入侵检测（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
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，入侵检测只有经过授权的合法用户才能访问，一般来说，用户登录入侵检测的方式为通过浏览器以WEB方式登录。入侵检测为了便于用户管理，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，需要对用户身份进行鉴别。 入侵检测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)以奇安信IDS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奇安信IDS的URL地址，如https://xx.x.x.x 。回车后进入奇安信IDS的登录界面，，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，即可登录到奇安信IDS。登录后，用户就可通过WEB界面对奇安信IDS进行配置管理 输入用户名，然后回车后，提示用户输入密码： 1）输入密码后，回车，即可登录到奇安信IDS。登录后，用户就可使用命令行方式对奇安信IDS进行配置管理。 2)应核查IDS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。 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	1)入侵检测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	符合情况：通过用户名口令方式登录，口令长度8位以上，口令复杂度包含大写字母、小写字母、数字，口令有效期为90天； 部分符合情况：通过用户名口令方式登录，口令长度8位以上，复杂度为小写字母、数字、特殊字符，但未配置口令有效期； 不符合情况：通过用户名口令方式登录，口令长度为6位，复杂度为纯数字，未配置口令有效期，口令为弱口令。
	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入侵检测	1)应在管理>系统设置里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)应在管理>系统设置里，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	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。 进入管理界面。然后在管理>系统设置，进入在系统设置页面，选择"管理员账号"页签，进入管理员账号页面，点击收缩的下拉栏，可以查看到"最大登录失败次数"的配置。 2)配置并启用了远程登录连接超时并自动退出功能。进入管理界面。管理>系统设置，默认进入基础设置页面，可见WEB页面超时时间版块。在"管理员登录超时时间"后的时间设置文本框中，输入需要设置的Web页面超时时间，系统默认为600秒，时间范围：60-65535秒。	符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，会话空闲30分钟自动退出； 部分符合情况：已配置登录失败处理功能，连续登录失败5次锁定账户30分钟，但未配置连接超时自动退出措施； 不符合情况：未配置登录失败处理功能和连接超时自动退出措施。
	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	为避免口令传输过程中别窃取，不应当使用明文传送的Telnet、HTTP服务，而应当采用SSH、HTTPS等加密协议等方式进行交互式管理	应询问系统管理员采用何种方式对入侵检测进行远程管理,核查通过WEB界面管理是否都通过SSL协议进行加密处理	通过WEB界面进行远程管理时，通过SSL协议进行加密处理。	符合情况：仅采用https协议进行管理，防止鉴别信息在网络传输过程中被窃听； 不符合情况：仅采用http协议进行管理，无法防止鉴别信息在网络传输过程中被窃听。

	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.目前主流入侵检测多采用“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，用户既要通过入侵检测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入侵检测	进入管理界面。 2）右侧显示用户列表信息，： 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”。	以奇安信IDS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”。	符合情况：通过用户名口令和谷歌验证码方式登录，验证码长度为6位，有效时间为30秒; 不符合情况：通过用户名口令方式登录，未采用两种或两种以上鉴别技术对用户进行身份鉴别。
访问控制	a)应对登录的用户分配账户和权限	为了确保入侵检测的安全，需要对登录的用户分配账户，并合理配置账户权限	进入管理界面。用户进入Web管理页面后，在导航栏区域点击管理>系统设置，进入系统设置页面，点击管理员账号，可进入管理员账号配置页面。 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。	符合情况：已对可登录用户分配账户和权限，相关管理员与职位相对应; 不符合情况：已启用匿名登录模式。
	b)应重命名或删除默认账户，修改默认账户的默认口令	对于入侵检测的默认账户，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	进入管理界面。用户进入Web管理页面后，在导航栏区域点击管理>系统设置，进入系统设置页面，点击管理员账号，可进入管理员账号配置页面。点击进入，查看账号的状态为active或block。 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认口令 3）根据实际情况决定是否应该关闭默认账户	入侵检测重命名或删除默认账户，修改默认账户的默认口令。	符合情况：已重命名系统默认账户a*为***，且口令修改为复杂口令; 部分符合情况：未重命名系统默认账户a**,已修改口令为复杂口令; 不符合情况：未重命名系统默认账户名，口令为设备出厂默认口令。
	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	入侵检测中如果存在多余的、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	进入管理界面。用户进入Web管理页面后，在导航栏区域点击管理>系统设置，进入系统设置页面，点击管理员账号，可进入管理员账号配置页面。用户权限等级分为level0-level3四个等级，对应审计、配置、管理、系统四个级别，根据用户需求分配权限等级。 1) 应核查入侵检测用户账户列表，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。	入侵检测用户账户列表不存在多余或过期账户，不存在共享用户。	符合情况：设备中未发现多余或过期的账户，管理员用户与账户之间一一对应，未发现共享账户的情况; 部分符合情况：管理员用户与账户之间一一对应，未发现共享账户的情况，但a*、s*为多余账户; 不符合情况：可登录账户仅有a*，所有管理员均通过a*登录。
	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	进入管理界面。用户进入Web管理页面后，在导航栏区域点击管理>系统设置，进入系统设置页面，点击管理员账号，可进入管理员账号配置页面。 1)应核查是否进行角色划分，审计、配置、管理、系统四个级别，每个管理员有其特定权限和职责。 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。	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。	符合情况：已配置安全管理员s*、审计管理员a*、系统管理员s*，授予管理用户所需的最小权限; 部分符合情况：已配置安全管理员s*、系统管理员s*，但未配置审计管理员; 不符合情况：可登录账户仅有a*，未授予管理用户所需的权限分离，实现管理用户的权限分离。

	e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	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	进入管理界面，然后在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1)应核查是否进行角色划分，确认访问控制策略仅由管理员进行管理。	用户的访问控制规则由管理进行管理;	符合情况：用户的访问控制规则由管理进行管理。 不符合情况：管理员无法配置访问规则。
	f)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	进入管理界面，在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1)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	访问控制规则由管理进行管理,主体为用户账号，客体未功能模块，访问控制力度未功能模块;	符合情况：访问控制规则由管理进行管理,主体为用户账号，客体为功能模块，访问控制力度为功能模块; 不符合情况：所有访问的模块均一致。
	g)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	进入管理界面，进入管理界面，在左侧导航树中选择用户管理-用户列表,右侧显示用户列表信息。 1）查看是否有安全标记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。	查看到具有安全标记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。	符合情况：查看到具有安全标记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。 不符合情况：未设置敏感标记。
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	为了对入侵检测的运行状况、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。 入侵检测的系统日志信息通常输出至本地或日志服务器或日志审计设备,在缺省情况下，控制台端口上的日志功能处于启用状态	进入管理界面。用户进入Web管理页面后，在导航栏区域点击管理>全局配置，单击选择“网关服务器配置”页签，可进行配置和查看网关服务器配置信息。 同时也可通过SNMP协议被日志审计设备采集日志数据。	入侵检测设置正确的日志审计服务器或设备地址、端口、以及日志类别等信息。	符合情况：已开启安全审计功能，可对所有重要的用户行为和重要安全事件进行审计，审计范围覆盖系统内所有用户; 不符合情况：无审计模块，无法对重要的用户行为和安全事件进行审计。
	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	对于入侵检测来说，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	进入管理界面。可视>日志显示，进入日志页面中可查看。 登录日志审计设备，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入侵检测设备的IP。 在日志审计设备上，根据IP地址选择入侵检测后，便可对该入侵检测的日志进行核查，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。	符合情况：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。 部分符合情况：仅有用户信息、登录时间。 不符合情况：无审计模块。
	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	以奇安信IDS为例，该设备日志存储时间决定于设备内存容量，所以需要日志审计设备对入侵检测的日志信息进行定期备份。 登录日志审计设备，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入侵检测设备的IP。 在日志审计设备上，根据IP地址选择入侵检测后，便可对该入侵检测的日志进行核查，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。	入侵检测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	符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，并留存半年以上，能够避免受到未预期的删除、修改或覆盖; 部分符合情况：已对审计记录记录进行保护，审计记录实时传输至日志审计设备，但审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖; 不符合情况：未对审计记录记录进行保护，审计记录仅留存7天，无法够避免受到未预期的删除、修改或覆盖。

	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	符合情况：审计进程权限配置合理，仅授权用户可终止审计进程； 不符合情况：审计进程权限配置不合理，部分普通用户可关闭审计进程。
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	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	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，需要对远程管理入侵检测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	登录设备进行核查。进入管理界面,后在左侧导航树中选择系统管理》配置,查看登录地址限制列表；	设备本地设置访问控制列表限制终端接入范围。	符合情况：已限制终端接入地址范围，仅允许通过10.*.*.*/32地址进行管理； 部分符合：已限制终端接入地址范围，但限制登录地址范围为10.*.*.*/16，可登录地址范围过大； 不符合情况，未限制终端接入方式或网络地址范围，任意地址均可登录。
	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	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	符合情况：定期对安全设备进行漏洞扫描，发现漏洞及时修复，并形成报告。 部分符合情况：定期进行漏洞扫描，但未进行漏洞修复。 不符合情况：未定期进行扫描，且无法及时对漏洞进行修复。
	f)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，以检查息是否发生了入侵和攻击	此项不适合，该项要求一般在安全设备上实现	此项不适合，该项要求一般在安全设备上实现	符合情况：能够对所有的入侵时间进行拦截并记录。 部分符合：设备授权已过期，仅能对已知的攻击行为进行拦截。 不符合情况：设备未接入，无法实现入侵防御行为。
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	1) 应核查是否安装了防恶意代码软件或相应功能的软件，定期进行升级和更新防恶意代 码库； 2) 应核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为； 3) 应核查当识别入侵和病毒行为时是否将其有效阻断。	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	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	查看设备是否具有可信根芯片	查看设备是否具有可信根芯片	符合情况：安装了可信根芯片，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。 不符合情况：未安装可信根芯片，无法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。
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；

	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能； 部分符合：无部分符合 不符合：系统采集信息非业务必要；
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施， 禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用； 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露；

安全计算环境-操作系统- Ubuntu（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
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	Ubuntu系统的用户鉴别过程与其他UNIX系统相同：系统管理员为用户建立一个账户并为其指定一个口令,用户使用指定的口令登录后重新配置自己的自己的口令，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Ubuntu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。 Ubuntu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。 Ubuntu系统具有调用PAM的应用程度认证用户。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。	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rmore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。 [预期结果或主要证据]1)登录需要密码;	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_DAYS 90 #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	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	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	Ubuntu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Ubuntu， 查看文件内容: # cat /ete/pam.d/system -auth或根据Ubuntu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	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	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	Ubuntu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因为其在数据传输过程中，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Ubuntu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	符合情况：采用SSH方式进行远程管理，且已关闭Telnet服务 部分符合情况：采用SSH方式进行远程管理，但未关闭Telnet 不符合情况：采用Telnet进行远程管理，或采用未进行加密处理的远程管理方式
	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	符合情况：采用两种或两种以上组合的鉴别技术，且其中一种鉴别技术在鉴别过程中使用了密码技术 部分符合情况：采用两种或两种以上的鉴别技术，但非密码技术 不符合情况：未采用两种或两种以上组合的鉴别技术
	a)应对登录的用户分配账户和权限	对于Ubuntu中一些重要的文件，应检查Ubuntu系统主要目录的权限设置情况，Ubuntu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Ubuntu,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—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	符合情况：重要文件和目录权限设置合理 部分符合情况：重要文件和目录权限设置未完全合理设置，部分文件和目录权限设置不合理 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	Ubuntu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Ubuntu,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	符合情况：不存在默认的、无用的可登录账户，且已禁止root用户远程登录 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改

访问控制	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	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	符合情况：无多余或过期账户，各类管理员均使用自己分配的特定权限账户登录，不存在共享账户的情况 部分符合情况：无多余或过期账户，但存在共享账户的情况 不符合情况：存在多余或过期账户
	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。Ubuntu, 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Ubuntu, 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Ubuntu, 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	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	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	符合情况：已指定授权主体（一般为安全管理员）对操作系统访问控制权限进行配置 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	f)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	符合情况：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，对于访问控制的粒度达到主体为用户级或进程级，客体为文件级、数据库表级 部分符合情况：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，但访问控制的粒度未完全达到要求，部分文件或目录权限设置不合理 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体为文件、数据库表级
	g)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Ubuntu (Security Enhanced Linux)简称SELinux,是一个Ubuntu内核模块，也是Ubuntu的一个安全子系统。2.6及以上版本的Ubuntu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Ubuntu,使用more查看/etc/selinux/config文件中的SELINUX参数的设定	1) 2) 3)4) Ubuntu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	符合情况：已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：已配置安全标记，但安全标记配置不合理等 不符合情况：未对重要主体或客体设置安全标记
	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	Ubuntu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，Ubuntu 内核就将安全审计信息传递给日志系统。 Ubuntu 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。Ubuntu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Ubuntu, 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Ubuntu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)Ubuntu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	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
	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。 Ubuntu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	1以root身份登录，查看审计日志是否包含必要的要素;默认位置是/var/log/audit/audit.log 2查看是否有第三方审计工具或系统; 3系统审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的准确性。启动NTP服务。	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	符合情况：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 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录

安全审计	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。	1. 询问系统管理员是否采取专用日志服务器等措施，对审计记录进行存储，备份和保护。 2. 在root权限下，查看日志访问权限：ls –la /var/log/audit.d 3. 查看auditd服务的配置文件#cat /etc/audit/auditd.conf 记录全部输出，重点检查mum logs、max log file、max log file action、disk full action、disk error action等字段。 4. 如果配置守护进程向除默认/var/log/audit/外的目录写日志文件时，一定要修改它上面的文件权限。	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	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	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Ubuntu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	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作
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Ubuntu操作系统时，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，为了避免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	访谈：1)访谈系统管理员系统目前是否采取了最小安装原则。 手工检查：1)确认系统目前正在运行的服务：#service --status-all | grep running,查看并确认是否已经关闭危险的网络服务如echo、 shell、login、finger、r命令等。关闭非必需的网络服务如talk 、ntalk、pop-2、Sendmail、Imapd、Pop3d等。 2)访谈补丁升级机制，查看补丁安装情况： # rpm –qa | grep patch 3)记录系统中多余和危险服务，记录系统补丁升级方式和已安装最新的补丁名称。。	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	符合情况：系统安装遵循最小化安装原则，且不存在业务所不需要的组件和应用程序 部分符合情况：无 不符合情况：未遵循最小化安装原则，存在多余的组件或应用程序
	b)应关闭不需要的系统服务、默认共享和高危端口	Ubuntu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）确认系统目前正在运行的服务：#ps -aux | grep running,查看并确认是否已经关闭危险的网络服务如echo、shell、login、fingerr命令等。关闭非必需的网络服务如talk、ntalk、pop-2、Sendmail、Imapd、Pop3d等。 2）使用netstat –tln命令查看已开启的端口，查看是否开启高危端口。	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	符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，不存在系统默认共享 部分符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，但存在系统默认共享 不符合情况：存在系统多余服务、危险服务和进程、未关闭多余端口、存在系统默认共享
	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Ubuntu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	1)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	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	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	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	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） 应核查是否存在高风险漏洞,如漏洞扫描、渗透测试等; 2） 应核查是否在经过充分测试评估后及时修补漏洞。	有运维团队定期进行漏洞扫描，发现安全风险，及时修补。	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
	f) 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，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	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，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）可执行命令：find / -name <daemon name> -print核查是否安装了以下主机入侵检测软件。Dragon Squire by Enterasys Networks、ITA bySymantec、Hostsentry by Psionic Software、Logcheck by PsionicSoftware、RealSecure agent by ISS。 4）询问是否有第三方入侵检测系统，如主机IDS，是否具备报警功能。	1）入侵的重要路径均deny，不存在系统级入侵的可能性; 2）开启主机防火墙等相关配置; 3）安装有基于主机的IDS设备; 4）若主机未部署主机IDS设备，可在网络链路上查看是否是IDS、IPS。 发生入侵事件时，记录报警措施等	符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，并进行报警 部分符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，但不具备报警功能 不符合情况：无入侵检测措施，无法检测到对重要节点进行入侵的行为

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Ubuntu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	查看系统中安装了什么防病毒软件。询问管理员病毒库是否经常更新。查看病毒库的最新版本更新日期是否超过一个星期；访谈管理员并查看实时检测与查杀恶意代码的软件产品是否采有统一的病毒根新策略和查杀策略。	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	符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，且病毒库已更新到最新 部分符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，但病毒库未及时更新 不符合情况：未安装任何防病毒软件，未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
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	符合情况：服务器具有可信根芯片或硬件，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 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心 不符合情况：无可信根芯片或硬件
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1） 系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2） 系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2） 通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2） 通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；

剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能； 部分符合：无部分符合 不符合：系统采集信息非业务必要；
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用； 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露；

安全计算环境-操作系统-AIX（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
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	AIX系或统的用户鉴别过程与其他UNIX系统相同：系统管理员为用户建立一个账户并为其指定一个口令,用户使用指定的口令登录后重新配置自己的自己的口令，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AIX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/security/passwd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，/etc/security/passwd文件是不能被普通用户读取的，只有超级用户才有权读取。 AIX中的/etc/security/user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。	1、检查并记录R族文件的配置，记录主机信任关系。 #find / -name .rhosts 对每个.rhosts文件进行检查 #find / -name .netrc 对.netrc文件进行检查 #more /etc/hosts.equiv 如果不存在信任关系或存在细粒度控制的信任关系，判定结果为符合； 如果存在与任意主机任意用户的信任关系，判定结果为不符合。 2、查看系统是否存在空口令用户 # more /etc/security/passwd检查空口令帐号 /etc/security/passwd中所有密码位不为空，判定结果为符合； /etc/security/passwd中所存在密码位为空，判定结果为不符合。 3、检查系统账号密码策略 执行以下命令: #more /etc/security/user记录Default规则,以及各用户配置的规则，重点关注: minlen口令最短长度 minalpha口令中最少包含字母字符个数 minother口令中最少包含非字母数字字符个数 loginretries 连续登录失败后锁定用户 4、检查系统中是否存在空口令或者是弱口令 利用扫描工具进行查看 询问管理员系统中是否存在弱口令 手工尝试密码是否与用户名相同 5、检查系统账户 执行以下命令: #cat /etc/passwd #cat /etc/security/passwd #cat /etc/group 查看UID是否唯一 查看系统是否分别建立了系统专用管理帐号，以及帐号的属组情况。	1、不存在信任关系或存在细粒度控制的信任关系； 2、不存在空口令用户 /etc/security/passwd中所有密码位不为空； 3、 Minlen 8 口令最短长度8 Minalpha 2口令中最少包含字母字符个数 Minother2口令中最少包含非字母数字字符个数 loginretries 5 连续登录失败后锁定用户 4、建立了系统专用管理账号	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	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	AIX系统中需要查看/etc/security/user（口令复杂度）记 录 Default 规 则 , 和 /etc/security/login.cfg （ 系 统 Banner）内容，/etc/sshd_config（远程登陆)等来查看登陆失败处理功能是否配置。	1、检查系统账号登录失败处理策略 执行以下命令 #more /etc/security/user记录Default规则,以及各用户配置的规则 检查loginretries 值 #more /etc/security/login.cfg 检查loginreenable值（端口锁定解锁时间） logindelay （失败登录后延迟时间） 2、如果启用了ssh远程登录，则检查ssh远程用户登录失败处理策略 执行以下命令 cat /etc/sshd_config 查看MaxAuthTries 等参数。 LoginGraceTime 1m 帐号锁定时间（建议为30 分钟） PermitRootLogin no MaxAuthTries 3 帐号锁定阀值（建议5 次） 3、检查系统是否设置了超时退出 执行以下命令: cat /etc/profile | grep TMOUT 查看输出结果	1、loginretries 值为5 2、loginreenable值 300s 3、ogindelay 300s（失败登录后延迟时间） 2、如果启用了ssh远程登录 cat /etc/sshd_config 查看MaxAuthTries 等参数。 LoginGraceTime 1m 帐号锁定时间（建议为30 分钟） PermitRootLogin no MaxAuthTries 3 帐号锁定阀值（建议5 次） 3、系统设置了超时退出 执行以下命令: cat /etc/profile | grep TMOUT tmout=300s	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	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	AIX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。!因为其在数据传输过程中，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	1、询问系统管理员，并查看开启的服务中是否包含了不安全的远程管理方式，如telnet, ftp,ssh,VNC 等。 执行：#ps –ef 查看开启的远程管理服务进程 执行：#netstat -a 查看开启的远程管理服务端口 2、系统采用了安全的远程管理方式，如ssh；且关闭了如telnet、ftp 等不安全的远程管理方式，判定结果为符合； 系统的开启了telnet、ftp 等不安全的远程管理方式，判定结果为不符合。	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	符合情况：采用SSH方式进行远程管理，且已关闭Telnet服务 部分符合情况：采用SSH方式进行远程管理，但未关闭Telnet 不符合情况：采用Telnet进行远程管理，或采用未进行加密处理的远程管理方式

	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，如口令数字证书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	符合情况：采用两种或两种以上组合的鉴别技术，且其中一种鉴别技术在鉴别过程中使用了密码技术 部分符合情况：采用两种或两种以上的鉴别技术，但非密码技术 不符合情况：未采用两种或两种以上组合的鉴别技术
访问控制	a)应对登录的用户分配账户和权限	对于AIX中一些重要的文件，应检查AIX系统主要目录的权限设置情况，AIX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AIX,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—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	符合情况：重要文件和目录权限设置合理 部分符合情况：重要文件和目录权限设置未完全合理设置，部分文件和目录权限设置不合理 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	AIX操作系统本身安装后提供各种账号，如agames, news，gopher，ftp,lp,halt，shutdown，reboot 、who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。	执行: # cat /etc/passwd或者/etc/security/passwd 查看不需要的账号games, news, gopher, ftp 、lp是否被删除 查看不需要的特权账号halt, shutdown, reboot 、who是否被删除	不存在默认无用的账户	符合情况：不存在默认的、无用的可登录账户，且已禁止root用户远程登录 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改
	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	访谈系统管理员，是否存在无用的多余帐号。同时执行以下命令: cat /etc/passwd或 cat /etc/security/passwd	禁用或删除了无用账户 各类管理员均使用自己分配的特定权限账户登录，不存在多余过期用户。	符合情况：无多余或过期账户，各类管理员均使用自己分配的特定权限账户登录，不存在共享账户的情况 部分符合情况：无多余或过期账户，但存在共享账户的情况 不符合情况：存在多余或过期账户
	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。	询问管理员系统定义了哪些管理用户角色，是否仅授予管理用户所需的最小权限 # SMIT 查看用户角色的授权	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 管理权限仅分配root用户	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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	符合情况：已指定授权主体（一般为安全管理员）对操作系统访问控制权限进行配置 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	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	符合情况：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，对于访问控制的粒度达到主体为用户级或进程级，客体为文件级、数据库表级 部分符合情况：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，但访问控制的粒度未完全达到要求，部分文件或目录权限设置不合理 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体为文件、数据库表级
	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	明确/etc/security/user文件的umask值	检查访问控制颗粒度。	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。	符合情况：已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：已配置安全标记，但安全标记配置不合理等 不符合情况：未对重要主体或客体设置安全标记

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	AIX使用audit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，AIX内核就将安全审计信息传递给日志系统。 AIX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；系统自动在/audit目录下生成bin1、bin2、trail三个文件,bin1、bin2是两个循环日志，交替使用，其内容定期刷新内容到trail文件中,AIX操作系统在安全审计配置文件/etc/security/audit/config中配置安全事件审计规则	1、检查系统日志是否开启 执行 #ps -ef |grep syslogd 查看系统是否运行syslogd进程 询问并查看是否有第三方审计工具或系统 2、查看选择的被审计用户 执行 # audsys （或者输入sam启动系统管理菜单GUI，点击“审计和安全”，点击“用户”查看被审计的用户，点击“事件”查看审计的事件，“system calls”查看被审计的系统调用。） #more /etc/rc.config.d./auditing 中的auditing字段值(=1 已开启) #audusr 3、检查系统审计功能是否开启 执行 # /usr/sbin/audit query 显示审计系统的当前状态 # more /etc/security/audit/config 查看选择的被审计用户 4、检查系统日志审计策略配置 执行: #cat /etc/syslog.conf 查看系统日志配置 syslog.conf 配置文件设置合理，对大多数系统行为、用户行为进行了纪录，并存储在指定的文档中，syslong.conf 中至少应包括: local0.crit /dev/console local0.info /usr/es/adm/cluster.log user.notice /usr/es/adm/cluster.log; 5、检查系统审计策略配置 执行: #more /etc/security/audit/objects	1、syslogd进程运行 #more /etc/rc.config.d./auditing 中的auditing字段值(=1 已开启) 执行: #cat /etc/syslog.conf 查看系统日志配置 syslog.conf 配置文件设置合理，对大多数系统行为、用户行为进行了纪录，并存储在指定的文档中，syslong.conf 中至少应包括: local0.crit /dev/console local0.info /usr/es/adm/cluster.log user.notice /usr/es/adm/cluster.log; 2、具有审计信息。	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
	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。	审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等 执行: #more /usr/es/adm/cluster.log #last 查看系统历史日志信息 #auditpr -v –hhelrtRpPTc 获取所有审计的信息	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	符合情况：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 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录
	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。	1、查看日志审计文件权限设置 执行: ls –la /etc/syslog.conf /usr/es/adm/cluster.log /var/adm 查看系统历史日志文件的权限或访问控制是否合理 2、查看审计文件权限设置 执行: #more /etc/security/audit/config 查看日志模式，例如 binmode = on streammode = off # ls 查看申日文件的权限或访问控制是否合理 例如 ls –l /audit/bin1 bin2 = /audit/bin2	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	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	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。 。	针对审计进程的权限设置。	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	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作

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AIX操作系统时，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、检查操作系统是否开启了与业务无关的服务 执行以下命令: ps –ef 执行#more /etc/inetd.conf|grep -v "#"记录系统开启的服务 #more /etc/rc.nfs #more /etc/rc.tcpip 2、检查操作系统是否开启了与业务无关的网络端口 执行以下命令: netstat –an netstat –a 3、检查系统版本和补丁升级情况 执行以下命令，查看AIX 内核版本: 版本信息：#oslevel： #oslevel –q: 补丁安装情况#instfix –i |grep ML	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	符合情况：系统安装遵循最小化安装原则，且不存在业务所不需要的组件和应用程序 部分符合情况：无 不符合情况：未遵循最小化安装原则，存在多余的组件或应用程序
	b)应关闭不需要的系统服务、默认共享和高危端口	AIX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	检查操作系统是否开启了与业务无关的网络端口 执行以下命令: netstat –an netstat –a	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	符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，不存在系统默认共享 部分符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，但存在系统默认共享 不符合情况：存在系统多余服务、危险服务和进程、未关闭多余端口、存在系统默认共享
	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AIX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	1、检查系统是否有网络访问控制策略 访谈系统管理员，是否制定了严格的访问控制策略，包括是否限制登录用户，对远程登录的IP 是否有限制，采用哪种远程登录方式等。 查看hosts.allow、hosts.deny 是否对某些服务，某些IP 进行了限制。 #cat hosts.allow #cat hosts.deny #cat /etc/ftpusers #cat /etc/ftpaccess	1、hosts.allow中有如下类似配置 Sshd: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、堡垒机、安全域、防火墙等运维方式实现对终端接入方式的限制。	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	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	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	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	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
	f)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，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	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，查看网络上是否部署了网络入侵检测系统，如IDS	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	符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，并进行报警 部分符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，但不具备报警功能 不符合情况：无入侵检测措施，无法检测到对重要节点进行入侵的行为
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AIX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	AIX系统是否安装恶意代码防护软件	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	符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，且病毒库已更新到最新 部分符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，但病毒库未及时更新 不符合情况：未安装任何防病毒软件，未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

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	符合情况：服务器具有可信根芯片或硬件，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 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心 不符合情况：无可信根芯片或硬件
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能； 部分符合：无部分符合 不符合：系统采集信息非业务必要；

个人信息保护	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用； 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露；

安全计算环境-操作系统-centos（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
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系或统的用户鉴别过程与其他UNIX系统相同：系统管理员为用户建立一个账户并为其指定一个口令,用户使用指定的口令登录后重新配置自己的自己的口令，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 。/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。	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_DAYS 90 #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	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	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，centos5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	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	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。l因为其在数据传输过程中，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	符合情况：采用SSH方式进行远程管理，且已关闭Telnet服务 部分符合情况：采用SSH方式进行远程管理，但未关闭Telnet 不符合情况：采用Telnet进行远程管理，或采用未进行加密处理的远程管理方式
	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	符合情况：采用两种或两种以上组合的鉴别技术，且其中一种鉴别技术在鉴别过程中使用了密码技术 部分符合情况：采用两种或两种以上的鉴别技术，但非密码技术 不符合情况：未采用两种或两种以上组合的鉴别技术
	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—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	符合情况：重要文件和目录权限设置合理 部分符合情况：重要文件和目录权限设置未完全合理设置，部分文件和目录权限设置不合理 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	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	符合情况：不存在默认的、无用的可登录账户，且已禁止root用户远程登录 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改

访问控制	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	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	符合情况：无多余或过期账户，各类管理员均使用自己分配的特定权限账户登录，不存在共享账户的情况 部分符合情况：无多余或过期账户，但存在共享账户的情况 不符合情况：存在多余或过期账户
	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。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	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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	符合情况：已指定授权主体（一般为安全管理员）对操作系统访问控制权限进行配置 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	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	符合情况：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，对于访问控制的粒度达到主体为用户级或进程级，客体为文件级、数据库表级 部分符合情况：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，但访问控制的粒度未完全达到要求，部分文件或目录权限设置不合理 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体为文件、数据库表级
	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	符合情况：已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：已配置安全标记，但安全标记配置不合理等 不符合情况：未对重要主体或客体设置安全标记
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	centos5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	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
	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	符合情况：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 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录

	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	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	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	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作
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操作系统时，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	符合情况：系统安装遵循最小化安装原则，且不存在业务所不需要的组件和应用程序 部分符合情况：无 不符合情况：未遵循最小化安装原则，存在多余的组件或应用程序
	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Linux, 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Linux,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,Linux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	符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，不存在系统默认共享 部分符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，但存在系统默认共享 不符合情况：存在系统多余服务、危险服务和进程、未关闭多余端口、存在系统默认共享
	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	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	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	此项不适合，该项要求一般在应用层面上核查
	f) 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? 3)访谈补丁升级机制，查看补丁安装情况：#rpm -qa grep patch	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）更新补丁时间为最近，对补丁进行控制和管理	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
	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，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	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，查看网络上是否部署了网络入侵检测系统，如IDS	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	符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，并进行报警 部分符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，但不具备报警功能 不符合情况：无入侵检测措施，无法检测到对重要节点进行入侵的行为

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	符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，且病毒库已更新到最新 部分符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，但病毒库未及时更新 不符合情况：未安装任何防病毒软件，未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
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	符合情况：服务器具有可信根芯片或硬件，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 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心 不符合情况：无可信根芯片或硬件
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；

剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能； 部分符合：无部分符合 不符合：系统采集信息非业务必要；
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用； 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露；

安全计算环境-操作系统-linux（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
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系或统的用户鉴别过程与其他UNIX系统相同：系统管理员为用户建立一个账户并为其指定一个口令,用户使用指定的口令登录后重新配置自己的自己的口令，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。	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_DAYS 90 #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	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	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	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	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。l因为其在数据传输过程中，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	符合情况：采用SSH方式进行远程管理，且已关闭Telnet服务 部分符合情况：采用SSH方式进行远程管理，但未关闭Telnet 不符合情况：采用Telnet进行远程管理，或采用未进行加密处理的远程管理方式
	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	符合情况：采用两种或两种以上组合的鉴别技术，且其中一种鉴别技术在鉴别过程中使用了密码技术 部分符合情况：采用两种或两种以上的鉴别技术，但非密码技术 不符合情况：未采用两种或两种以上组合的鉴别技术
	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—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	符合情况：重要文件和目录权限设置合理 部分符合情况：重要文件和目录权限设置未完全合理设置，部分文件和目录权限设置不合理 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	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	符合情况：不存在默认的、无用的可登录账户，且已禁止root用户远程登录 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改

访问控制	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	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	符合情况：无多余或过期账户，各类管理员均使用自己分配的特定权限账户登录，不存在共享账户的情况 部分符合情况：无多余或过期账户，但存在共享账户的情况 不符合情况：存在多余或过期账户
	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。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	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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	符合情况：已指定授权主体（一般为安全管理员）对操作系统访问控制权限进行配置 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	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	符合情况：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，对于访问控制的粒度达到主体为用户级或进程级，客体为文件级、数据库表级 部分符合情况：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，但访问控制的粒度未完全达到要求，部分文件或目录权限设置不合理 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体为文件、数据库表级
	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	符合情况：已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：已配置安全标记，但安全标记配置不合理等 不符合情况：未对重要主体或客体设置安全标记
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	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
	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	符合情况：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 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录

	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	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	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	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作
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操作系统时，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	符合情况：系统安装遵循最小化安装原则，且不存在业务所不需要的组件和应用程序 部分符合情况：无 不符合情况：未遵循最小化安装原则，存在多余的组件或应用程序
	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Linux, 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Linux,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,Linux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	符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，不存在系统默认共享 部分符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，但存在系统默认共享 不符合情况：存在系统多余服务、危险服务和进程、未关闭多余端口、存在系统默认共享
	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	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	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	此项不适合，该项要求一般在应用层面上核查
	f) 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? 3)访谈补丁升级机制，查看补丁安装情况：#rpm -qa grep patch	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）更新补丁时间为最近，对补丁进行控制和管理	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
	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，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	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，查看网络上是否部署了网络入侵检测系统，如IDS	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	符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，并进行报警 部分符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，但不具备报警功能 不符合情况：无入侵检测措施，无法检测到对重要节点进行入侵的行为

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	符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，且病毒库已更新到最新 部分符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，但病毒库未及时更新 不符合情况：未安装任何防病毒软件，未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
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	符合情况：服务器具有可信根芯片或硬件，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 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心 不符合情况：无可信根芯片或硬件
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；

剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能； 部分符合：无部分符合 不符合：系统采集信息非业务必要；
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用； 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露；

安全计算环境-操作系统-Redhat（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
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系或统的用户鉴别过程与其他UNIX系统相同：系统管理员为用户建立一个账户并为其指定一个口令,用户使用指定的口令登录后重新配置自己的自己的口令，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 。/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。	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_DAYS 90 #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	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	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	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	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。l因为其在数据传输过程中，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	符合情况：采用SSH方式进行远程管理，且已关闭Telnet服务 部分符合情况：采用SSH方式进行远程管理，但未关闭Telnet 不符合情况：采用Telnet进行远程管理，或采用未进行加密处理的远程管理方式
	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	符合情况：采用两种或两种以上组合的鉴别技术，且其中一种鉴别技术在鉴别过程中使用了密码技术 部分符合情况：采用两种或两种以上的鉴别技术，但非密码技术 不符合情况：未采用两种或两种以上组合的鉴别技术
	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—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	符合情况：重要文件和目录权限设置合理 部分符合情况：重要文件和目录权限设置未完全合理设置，部分文件和目录权限设置不合理 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	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	符合情况：不存在默认的、无用的可登录账户，且已禁止root用户远程登录 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改

访问控制	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	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	符合情况：无多余或过期账户，各类管理员均使用自己分配的特定权限账户登录，不存在共享账户的情况 部分符合情况：无多余或过期账户，但存在共享账户的情况 不符合情况：存在多余或过期账户
	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。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	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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	符合情况：已指定授权主体（一般为安全管理员）对操作系统访问控制权限进行配置 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	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	符合情况：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，对于访问控制的粒度达到主体为用户级或进程级，客体为文件级、数据库表级 部分符合情况：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，但访问控制的粒度未完全达到要求，部分文件或目录权限设置不合理 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体为文件、数据库表级
	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	符合情况：已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：已配置安全标记，但安全标记配置不合理等 不符合情况：未对重要主体或客体设置安全标记
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	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
	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	符合情况：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 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录

	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	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	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	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作
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操作系统时，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	符合情况：系统安装遵循最小化安装原则，且不存在业务所不需要的组件和应用程序 部分符合情况：无 不符合情况：未遵循最小化安装原则，存在多余的组件或应用程序
	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Linux, 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Linux,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,Linux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	符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，不存在系统默认共享 部分符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，但存在系统默认共享 不符合情况：存在系统多余服务、危险服务和进程、未关闭多余端口、存在系统默认共享
	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	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	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	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	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? 3)访谈补丁升级机制，查看补丁安装情况：#rpm -qa grep patch	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）更新补丁时间为最近，对补丁进行控制和管理	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
	f)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，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	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，查看网络上是否部署了网络入侵检测系统，如IDS	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	符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，并进行报警 部分符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，但不具备报警功能 不符合情况：无入侵检测措施，无法检测到对重要节点进行入侵的行为

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	符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，且病毒库已更新到最新 部分符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，但病毒库未及时更新 不符合情况：未安装任何防病毒软件，未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
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	符合情况：服务器具有可信根芯片或硬件，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 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心 不符合情况：无可信根芯片或硬件
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；

剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能； 部分符合：无部分符合 不符合：系统采集信息非业务必要；
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用； 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露；

安全计算环境-操作系统-windows（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
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	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	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	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 需要说明的是，如果系统按上面的方法合理的设置了密码策略，此项要求就不是很重要了，因为任何攻击者都不能在一段合理的时间内猜出密码。在仅使用大小写字母与数字，用户不使用词典单词并仅附加一个数字的情况下，如果每次猜测需要半秒钟时间，猜到密码要花3，461，760年。由于密码会定期更改，攻击者猜到密码的可能性非常小。事实上，如果每隔70天更改密码，攻击者将需要相当于52,000条T3传入被攻击系统的线路,才能在密码过期前猜到一个随机的密码(当然，需要假定该容码不是词典单词)换句话说，如果密码很弱，攻击者能在十次尝话内猜到，那么何题并不是在照户锁定策略，而是弱到极点的密码	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	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	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， Windows Server 2003 SP1中针对远程桌面提供了SSL加密功能，它可以基于SSL来实现以下两个功能:对RDP客户端提供终端服务器的服务器身份验证、加密和RDP客户端的通信。要使用远程桌面的SSL加密功能，远程桌面必须使用RDP的版本是5.2或以上，即所远行的操作累统必须是Windows Server 2003 SPI或其后版本	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	符合情况：采用RDP远程桌面方式进行远程管理，且已关闭Telnet服务 部分符合情况：采用RDP远程桌面方式进行远程管理，但未关闭Telnet 不符合情况：采用Telnet进行远程管理，或采用未进行加密处理的远程管理方式
	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	查看和询问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 记录系统管理员在登录操作系统使用的身份鉴别方法，同时记录使用密码的鉴别方法	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	符合情况：采用两种或两种以上组合的鉴别技术，且其中一种鉴别技术在鉴别过程中使用了密码技术 部分符合情况：采用两种或两种以上的鉴别技术，但非密码技术 不符合情况：未采用两种或两种以上组合的鉴别技术

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%\windows\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	符合情况：重要文件和目录权限设置合理 部分符合情况：重要文件和目录权限设置未完全合理设置，部分文件和目录权限设置不合理 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	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，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	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	符合情况：不存在默认的、无用的可登录账户，已禁用guest账户 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改，未禁用guest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	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	符合情况：无多余或过期账户，各类管理员均使用自己分配的特定权限账户登录，不存在共享账户的情况 部分符合情况：无多余或过期账户，但存在共享账户的情况 不符合情况：存在多余或过期账户
	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	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	在命令行输入"secpol.msc" ,弹出“本地安全策略”窗口，查看“安全设置->本地策略>用户权限分配”中的相关项目。右侧的详细信息窗口即显示可配署的用户权限策略设置	设置系统管理员、安全员、审计员角色,根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限，角色的权限之间相互制约	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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,能够配置访问控制策略的用户 2)查看重点目录的权限配置，是否依据安全策略配置访问规则	1)由安全管理员授权设置规则 2)配置主体对客体的访问控制规则，并统一管理	符合情况：已指定授权主体（一般为安全管理员）对操作系统访问控制权限进行配置 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	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	选择%systemdrive%\program files、%systemdrive% \system32等重要的文件夹，以及%systemdrive%\Windows \system32\conf ig、%systemdrive%\Windows\system32\secpol等重要的文件，右键选择“属性”>“安全”，查看访问权限设置	users权限设置合理,用户依据访问控制策略，对各类文件和数据库表级进行访问	符合情况：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，对于访问控制的粒度达到主体为用户级或进程级，客体为文件级、数据库表级 部分符合情况：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，但访问控制的粒度未完全达到要求，部分文件或目录权限设置不合理 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体为文件、数据库表级

	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。敏感标记是由强认证的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。 当操作系统具备了能对信息资源设置敏感标记的功能前提下，应该严格按照安全策略来控制用户对相关资源的操作	1)查看操作系统功能手册或相关文档，确认操作系统是否具备能对信息资源设置敏感 2)询问管理员是否对重要信息资源设置敏感标记 3)询问或查看目前的敏感标记策略的相关设置，如:如何划分敏感标记分类，如何设定访问权限等	1)系统中有敏感数据，不同层面人员设置强制访问控制策略，若无敏感数据，本条N/A 2)3)在主客体层面分别设置不同的敏感标记，并在基于这些标记上，由管理员设置访问控制路径，是否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。部署第三方主机加固系统，可设置对主客体安全标记，并控制主体对客体的访问路径	符合情况：已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：已配置安全标记，但安全标记配置不合理等 不符合情况：未对重要主体或客体设置安全标记
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	安全审计通过关注系统和网络日志文件、目录和文件中不期望的改变、程序执行中的不期望行为、物理形式的入侵信息等，用以检查和防止虚假数据和欺骗行为，是保障计算机系统本地安全和网络安全的重要技术，对审计信息的分析可以为计算机系统的脆弱性评估、责任认定、损失评估、系统恢复提供关键性信息，所以审计覆盖范围必须要覆盖到每个操作系统用户。 Windows操作系统通过配置开启安全审计功能，合理地配置安全审计内容，对重要的用户行为和重要安全事件进行审计，能够及时准确地了解和判断安全事件的内容和性质，并且可以极大地节省系统资源	1)查看系统是否开启了安全审计功能 在命令行输入“”secpol.msc”,弹出“本地安全策略”窗口，查看“安全设置->本地策略->审计策略”中的相关项目。右侧的详细信息窗格即显示审计策略的设置情况。 2)询问并查看是否有第三方审计工具或系统	1)结果如下: a)审核策略更改:成功，失败 b)审核登录事件:成功，失败 c)审核对象访问：成功，失败 d)审核进程跟踪:成功，失败 e)以审核目录服务访问:失败 f)审核特权使用:失败 g)审核系统事件:成功，失败 h)审核账户登录事件:成功，失败 i)审核账户管理:成功，失败 2)部署第三方审计工具，实现对用户的全覆盖，主要针对用户操作行为的审计	符合情况：已开启安全审计功能，且所有审计策略均已开启， 部分符合情况：已开启安全审计功能，但审计策略未全部开启 不符合情况：未开启安全审计功能
	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。	查看审计记录是否包含要求的信息 1)在命令行输入”eventvwr.msc”，弹出“事件查看器”窗口，“事件查看器(本地)->Windows日志”下包括“应用程序”、“安全”、“设置”、“系统”几类记录事件类型，点击任意类型事件，查看日志文件是否满足此项要求 2) 如果安装了第三方审计工具，则:查看审计记录是否包括日期、时间，类型、主体标识、客体标识和结果	1) Windows操作系统事件查看器中的审计记录默认满足 2)第三方审计工具中，查看审计记录，审计信息包含日期、主客体、类型等信息	符合情况：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 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录
	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	1)如果日志数据本地保存，则询问审计记录备份周期，有无异地备份。在命令行输入“eventvwr. msc”,弹出“事件查看器”窗口，“事件查看器(本地)->Windows 日志”下包括“应用程序”、”安全”、“设置”、“系统”几类记录事件类型，右键点击类型事件，选择下拉菜单中的“属性”，查看日志存储策略 2)如果日志数据存放在日志服务器上并且审计策略合理,则该要求为符合	1)日志本地存储，可查看存储目录，周期和相关策略等 2)若部署有日志服务器，可查看存储路径等	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	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，当事件发生时，能够及时记录事件发生的详细内容。Windows系统具备了在审计进程自我保护方面功能	1)访谈是否有第三方方审计进程监控和保护的措施 2)在命令行输入”secpol.msc”，弹出“本地安全策略”窗口，点击“安全设置->本地策略->用户权限分配”，右键点击策略中的“管理审核和安全日志”，查看是否只有系统审计员或系统审计员所在的用户组	1)默认符合 2)其他非审计人员不可登录和操作日志，有专人负责审计日志的管理	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作

	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默认安装时会安装许多不必要的组件和应用程序，为了避免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等。有些操作系统中运行的多余服务和应用程序，如:在一台只提供下载服务的FTP服务器上还启用了邮件服务，则该"邮件服务"对于此主机来说属于多余服务；一台文件服务器上安装了游戏软件，这些游戏软件则属于多余的应用程序	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	符合情况：系统安装遵循最小化安装原则，且不存在业务所不需要的组件和应用程序 部分符合情况：无 不符合情况：未遵循最小化安装原则，存在多余的组件或应用程序
	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	符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，不存在系统默认共享 部分符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，但存在系统默认共享 不符合情况：存在系统多余服务、危险服务和进程、未关闭多余端口、存在系统默认共享

入侵防范	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	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网络地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	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	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	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	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描

	f)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，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	1)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 2)查看网络拓扑图，查看网络上是否部署了网络入侵检测系统，如IDS	1)暂无安装主机入侵检测系统 2)网络上有IDS、IPS软件 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	符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，并进行报警 部分符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，但不具备报警功能 不符合情况：无入侵检测措施，无法检测到对重要节点进行入侵的行为
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)询问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	符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，且病毒库已更新到最新 部分符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，但病毒库未及时更新 不符合情况：未安装任何防病毒软件，未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
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	I）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	符合情况：服务器具有可信根芯片或硬件，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 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心 不符合情况：无可信根芯片或硬件
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1） 系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2） 系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；

	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能； 部分符合：无部分符合 不符合：系统采集信息非业务必要；

个人信息保护	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用； 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露；

安全计算环境-操作系统-windows（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
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	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	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	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 需要说明的是，如果系统按上面的方法合理的设置了密码策略，此项要求就不是很重要了，因为任何攻击者都不能在一段合理的时间内猜出密码。在仅使用大小写字母与数字，用户不使用词典单词并仅附加一个数字的情况下，如果每次猜测需要半秒钟时间，猜到密码要花3，461，760年。由于密码会定期更改，攻击者猜到密码的可能性非常小。事实上，如果每隔70天更改密码，攻击者将需要相当于52,000条T3传入被攻击系统的线路,才能在密码过期前猜到一个随机的密码(当然，需要假定该容码不是词典单词)换句话说，如果密码很弱，攻击者能在十次尝话内猜到，那么何题并不是在照户锁定策略，而是弱到极点的密码	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	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	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， Windows Server 2003 SP1中针对远程桌面提供了SSL加密功能，它可以基于SSL来实现以下两个功能:对RDP客户端提供终端服务器的服务器身份验证、加密和RDP客户端的通信。要使用远程桌面的SSL加密功能，远程桌面必须使用RDP的版本是5.2或以上，即所远行的操作累统必须是Windows Server 2003 SPI或其后版本	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	符合情况：采用RDP远程桌面方式进行远程管理，且已关闭Telnet服务 部分符合情况：采用RDP远程桌面方式进行远程管理，但未关闭Telnet 不符合情况：采用Telnet进行远程管理，或采用未进行加密处理的远程管理方式
	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	查看和询问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 记录系统管理员在登录操作系统使用的身份鉴别方法，同时记录使用密码的鉴别方法	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	符合情况：采用两种或两种以上组合的鉴别技术，且其中一种鉴别技术在鉴别过程中使用了密码技术 部分符合情况：采用两种或两种以上的鉴别技术，但非密码技术 不符合情况：未采用两种或两种以上组合的鉴别技术

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%\windows\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	符合情况：重要文件和目录权限设置合理 部分符合情况：重要文件和目录权限设置未完全合理设置，部分文件和目录权限设置不合理 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	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，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	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	符合情况：不存在默认的、无用的可登录账户，已禁用guest账户 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改，未禁用guest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	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	符合情况：无多余或过期账户，各类管理员均使用自己分配的特定权限账户登录，不存在共享账户的情况 部分符合情况：无多余或过期账户，但存在共享账户的情况 不符合情况：存在多余或过期账户
	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	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	在命令行输入"secpol.msc" ,弹出“本地安全策略”窗口，查看“安全设置->本地策略>用户权限分配”中的相关项目。右侧的详细信息窗口即显示可配署的用户权限策略设置	设置系统管理员、安全员、审计员角色,根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限，角色的权限之间相互制约	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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,能够配置访问控制策略的用户 2)查看重点目录的权限配置，是否依据安全策略配置访问规则	1)由安全管理员授权设置规则 2)配置主体对客体的访问控制规则，并统一管理	符合情况：已指定授权主体（一般为安全管理员）对操作系统访问控制权限进行配置 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	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	选择%systemdrive%\program files、%systemdrive% \system32等重要的文件夹，以及%systemdrive%\Windows \system32\conf ig、%systemdrive%\Windows\system32\secpol等重要的文件，右键选择“属性”>“安全”，查看访问权限设置	users权限设置合理,用户依据访问控制策略，对各类文件和数据库表级进行访问	符合情况：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，对于访问控制的粒度达到主体为用户级或进程级，客体为文件级、数据库表级 部分符合情况：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，但访问控制的粒度未完全达到要求，部分文件或目录权限设置不合理 不符合情况：访问控制的粒度未达到主体为用户级或进程级，客体为文件、数据库表级

	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。敏感标记是由强认证的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。 当操作系统具备了能对信息资源设置敏感标记的功能前提下，应该严格按照安全策略来控制用户对相关资源的操作	1)查看操作系统功能手册或相关文档，确认操作系统是否具备能对信息资源设置敏感 2)询问管理员是否对重要信息资源设置敏感标记 3)询问或查看目前的敏感标记策略的相关设置，如:如何划分敏感标记分类，如何设定访问权限等	1)系统中有敏感数据，不同层面人员设置强制访问控制策略，若无敏感数据，本条N/A 2)3)在主客体层面分别设置不同的敏感标记，并在基于这些标记上，由管理员设置访问控制路径，是否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。部署第三方主机加固系统，可设置对主客体安全标记，并控制主体对客体的访问路径	符合情况：已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：已配置安全标记，但安全标记配置不合理等 不符合情况：未对重要主体或客体设置安全标记
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	安全审计通过关注系统和网络日志文件、目录和文件中不期望的改变、程序执行中的不期望行为、物理形式的入侵信息等，用以检查和防止虚假数据和欺骗行为，是保障计算机系统本地安全和网络安全的重要技术，对审计信息的分析可以为计算机系统的脆弱性评估、责任认定、损失评估、系统恢复提供关键性信息，所以审计覆盖范围必须要覆盖到每个操作系统用户。 Windows操作系统通过配置开启安全审计功能，合理地配置安全审计内容，对重要的用户行为和重要安全事件进行审计，能够及时准确地了解和判断安全事件的内容和性质，并且可以极大地节省系统资源	1)查看系统是否开启了安全审计功能 在命令行输入“”secpol.msc”,弹出“本地安全策略”窗口，查看“安全设置->本地策略->审计策略”中的相关项目。右侧的详细信息窗格即显示审计策略的设置情况。 2)询问并查看是否有第三方审计工具或系统	1)结果如下: a)审核策略更改:成功，失败 b)审核登录事件:成功，失败 c)审核对象访问：成功，失败 d)审核进程跟踪:成功，失败 e)以审核目录服务访问:失败 f)审核特权使用:失败 g)审核系统事件:成功，失败 h)审核账户登录事件:成功，失败 i)审核账户管理:成功，失败 2)部署第三方审计工具，实现对用户的全覆盖，主要针对用户操作行为的审计	符合情况：已开启安全审计功能，且所有审计策略均已开启， 部分符合情况：已开启安全审计功能，但审计策略未全部开启 不符合情况：未开启安全审计功能
	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。	查看审计记录是否包含要求的信息 1)在命令行输入”eventvwr.msc”，弹出“事件查看器”窗口，“事件查看器(本地)->Windows日志”下包括“应用程序”、“安全”、“设置”、“系统”几类记录事件类型，点击任意类型事件，查看日志文件是否满足此项要求 2) 如果安装了第三方审计工具，则:查看审计记录是否包括日期、时间，类型、主体标识、客体标识和结果	1) Windows操作系统事件查看器中的审计记录默认满足 2)第三方审计工具中，查看审计记录，审计信息包含日期、主客体、类型等信息	符合情况：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 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录
	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	1)如果日志数据本地保存，则询问审计记录备份周期，有无异地备份。在命令行输入“eventvwr. msc”,弹出“事件查看器”窗口，“事件查看器(本地)->Windows 日志”下包括“应用程序”、”安全”、“设置”、“系统”几类记录事件类型，右键点击类型事件，选择下拉菜单中的“属性”，查看日志存储策略 2)如果日志数据存放在日志服务器上并且审计策略合理,则该要求为符合	1)日志本地存储，可查看存储目录，周期和相关策略等 2)若部署有日志服务器，可查看存储路径等	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	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，当事件发生时，能够及时记录事件发生的详细内容。Windows系统具备了在审计进程自我保护方面功能	1)访谈是否有第三方方审计进程监控和保护的措施 2)在命令行输入”secpol.msc”，弹出“本地安全策略”窗口，点击“安全设置->本地策略->用户权限分配”，右键点击策略中的“管理审核和安全日志”，查看是否只有系统审计员或系统审计员所在的用户组	1)默认符合 2)其他非审计人员不可登录和操作日志，有专人负责审计日志的管理	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作

	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默认安装时会安装许多不必要的组件和应用程序，为了避免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等。有些操作系统中运行的多余服务和应用程序，如:在一台只提供下载服务的FTP服务器上还启用了邮件服务，则该"邮件服务"对于此主机来说属于多余服务；一台文件服务器上安装了游戏软件，这些游戏软件则属于多余的应用程序	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	符合情况：系统安装遵循最小化安装原则，且不存在业务所不需要的组件和应用程序 部分符合情况：无 不符合情况：未遵循最小化安装原则，存在多余的组件或应用程序
	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	符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，不存在系统默认共享 部分符合情况：已关闭系统多余服务、危险服务和进程，已关闭多余端口，但存在系统默认共享 不符合情况：存在系统多余服务、危险服务和进程、未关闭多余端口、存在系统默认共享

入侵防范	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	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网络地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	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	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	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	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描

	f)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，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	1)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 2)查看网络拓扑图，查看网络上是否部署了网络入侵检测系统，如IDS	1)暂无安装主机入侵检测系统 2)网络上有IDS、IPS软件 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	符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，并进行报警 部分符合情况：具备入侵检测的措施，可以检测到对重要节点进行入侵的行为，但不具备报警功能 不符合情况：无入侵检测措施，无法检测到对重要节点进行入侵的行为
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)询问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	符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，且病毒库已更新到最新 部分符合情况：系统中已安装部署防病毒软件，可对病毒入侵进行及时阻断，但病毒库未及时更新 不符合情况：未安装任何防病毒软件，未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
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	I）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	符合情况：服务器具有可信根芯片或硬件，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 部分符合情况：具有可信根芯片或硬件，但未将验证结果形成审计记录送至安全管理中心 不符合情况：无可信根芯片或硬件
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1） 系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2） 系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；

	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；
	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能； 部分符合：无部分符合 不符合：系统采集信息非业务必要；

个人信息保护	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用； 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露；

安全计算环境（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
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，口令复杂(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令复杂度相关配置: 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	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	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	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	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	符合情况：采用的远程管理方式启用了SSL连接特性，采取SSH隧道加密连接远程管理通信 部分符合情况：无 不符合情况：采用未进行加密处理的远程管理方式
	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运维服务器。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	符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，且在硬件Ukey中使用了加密算法 部分符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，但采用加密算法 不符合情况：未部署堡垒机，未通过堡垒机管理服务器来实现双因素身份验证
	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	符合情况：已创建不同账户，并且根据用户所需为其分配相应的权限 部分符合情况：已创建不同的用户，但未进行权限的划分 不符合情况：未对登录的用户分配账户和权限
	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	符合情况：不存在默认的、无用的可登录账户，已删除或禁用默认账户 部分符合情况：存在默认账户，但已修改默认账户默认口令 不符合情况：存在默认账户，且默认账户口令也未修改

访问控制	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	符合情况：不存在默认的、无用的可登录账户， 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改
	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MySQL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	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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	符合情况：已指定授权主体（一般为安全管理员）对数据库访问控制权限进行配置，且授权主体为用户，客体未数据库表 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	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	符合情况：在数据库所在操作系统上，已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：在数据库所在操作系统上，已配置安全标记，但安全标记配置不合理等 不符合情况：未在数据库所在操作系统上对重要主体或客体设置安全标记
	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	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能

安全审计	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	符合情况：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 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录
	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份，根据《网络安全法》要求，日志应至少保存6个月以上	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	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	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	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作
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	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	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	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
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	符合情况：已提供重要数据处理系统的热冗余，如热备、集群、负载均衡等高可用方式 部分符合情况：无 不符合情况：未提供重要数据处理系统的热冗余

	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	符合情况：已提供异地数据备份功能，实时将数据备份至异地备份机房 部分符合情况：已提供异地数据备份功能，但未实时将数据备份至异地机房 不符合情况：未提供异地数据备份功能
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该数据库的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）数据库提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）数据库检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合情况：已采用校验技术或密码技术保障重要数据在传输过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在传输过程中的完整性
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问数据库管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)数据库采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)数据库可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合情况：已采用校验技术或密码技术保障重要数据在存储过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在存储过程中的完整性
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)数据库管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合情况：已采用密码技术保障重要数据在传输过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在传输过程中的保密性
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合情况：已采用密码技术保障重要数据在存储过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在存储过程中的保密性
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	数据库将用户的鉴别信息所在的存储空间完全清理后才能分配	询问数据库管理员，数据库是否采取措施保证对存储介质防止其他用户非授权获取该用户的鉴别信息	数据库采取措施保证对存储介质中的用户鉴别信息进行及时清除。	符合情况：数据库已采取措施保证对存储介质中的用户鉴别信息进行及时清除 部分符合情况：无 不符合情况：数据库未采取措施保证对存储介质中的用户鉴别
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	数据库应将敏感数据所在的存储空间清除后才能分配给其他用户	询问数据库管理员，数据库是否采取措施保证对存储介质中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	数据库采取了措施保证对存储介质中的敏感数据进行及时清除，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：数据库采取了措施保证对存储介质中的敏感数据进行及时清除，以及对存有用户鉴别信息的临时文件进行删除或内容清除信息进行及时清除 部分符合情况：无 不符合情况：数据库未采取措施保证对存储介质中的敏感数据进行及时清除，以及对存有用户鉴别信息的临时文件进行删除或内容清除
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	保护个人信息，不采集业务不需要的个人数据	1)询问数据库管理员,该系统采集了用户的哪些个人信息 2)询问数据库管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录数据库所存储的个人信息。如数据库存储了用户身份证号、电话等个人信息 2)记录数据库哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合情况：数据库所存储的用户个人信息均为业务所必需的，不存在非必要用户个人信息 部分符合情况：无 不符合情况：数据库违规保存非业务必需的用户个人信息
	b)应禁止未授权访问和非法使用用户个人信息	数据库应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问数据库管理员，哪些数据库账户可以访问个人信息，且数据库采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了数据库账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合情况：系统已采取措施限制了数据库账户对个人信息的访问，非授权用户无法访问和使用用户的个人信息，且已制定相关个人信息保护制度 部分符合情况：无 不符合情况：未对用户个人信息的访问和使用进行严格的管理，未采取措施来禁止非授权访问和非法使用个人信息

安全计算环境（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
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，口令复杂(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	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	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= 'DEFAULT and resource name= 'IDLE_ TIME'	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	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	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 _AUTHENT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	符合情况：采用的远程管理方式启用了SSL连接特性，采取SSH隧道加密连接远程管理通信 部分符合情况：无 不符合情况：采用未进行加密处理的远程管理方式
	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	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、指纹等，是否有一种鉴别方法使用密码技术	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	符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，且在硬件Ukey中使用了加密算法 部分符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，但采用加密算法 不符合情况：未部署堡垒机，未通过堡垒机管理服务器来实现双因素身份验证
	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	符合情况：已创建不同账户，并且根据用户所需为其分配相应的权限 部分符合情况：已创建不同的用户，但未进行权限的划分 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	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	符合情况：不存在默认的、无用的可登录账户，已删除或禁用默认账户 部分符合情况：存在默认账户，但已修改默认账户默认口令 不符合情况：存在默认账户，且默认账户口令也未修改

访问控制	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 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	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	符合情况：不存在默认的、无用的可登录账户， 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改
	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	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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	符合情况：已指定授权主体（一般为安全管理员）对数据库访问控制权限进行配置，且授权主体为用户，客体未数据库表 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	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	符合情况：在数据库所在操作系统上，已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：在数据库所在操作系统上，已配置安全标记，但安全标记配置不合理等 不符合情况：未在数据库所在操作系统上对重要主体或客体设置安全标记
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。	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
	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	符合情况：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 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录

	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	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	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	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作
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	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	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	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
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)询问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	符合情况：已提供重要数据处理系统的热冗余，如热备、集群、负载均衡等高可用方式 部分符合情况：无 不符合情况：未提供重要数据处理系统的热冗余
	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	符合情况：已提供异地数据备份功能，实时将数据备份至异地备份机房 部分符合情况：已提供异地数据备份功能，但未实时将数据备份至异地机房 不符合情况：未提供异地数据备份功能
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该数据库的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）数据库提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）数据库检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合情况：已采用校验技术或密码技术保障重要数据在传输过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在传输过程中的完整性
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问数据库管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)数据库采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)数据库可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合情况：已采用校验技术或密码技术保障重要数据在存储过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在存储过程中的完整性
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)数据库管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合情况：已采用密码技术保障重要数据在传输过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在传输过程中的保密性
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询间数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合情况：已采用密码技术保障重要数据在存储过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在存储过程中的保密性

剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	数据库将用户的鉴别信息所在的存储空间完全清理后才能分配	询问数据库管理员，数据库是否采取措施保证对存储介质防止其他用户非授权获取该用户的鉴别信息	数据库采取措施保证对存储介质中的用户鉴别信息进行及时清除。	符合情况：数据库已采取措施保证对存储介质中的用户鉴别信息进行及时清除 部分符合情况：无 不符合情况：数据库未采取措施保证对存储介质中的用户鉴别
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	数据库应将敏感数据所在的存储空间清除后才能分配给其他用户	询问数据库管理员，数据库是否采取措施保证对存储介质中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	数据库采取了措施保证对存储介质中的敏感数据进行及时清除，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：数据库采取了措施保证对存储介质中的敏感数据进行及时清除，以及对存有用户鉴别信息的临时文件进行删除或内容清除信息进行及时清除 部分符合情况：无 不符合情况：数据库未采取措施保证对存储介质中的敏感数据进行及时清除，以及对存有用户鉴别信息的临时文件进行删除或内容清除
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	保护个人信息，不采集业务不需要的个人数据	1)询问数据库管理员,该系统采集了用户的哪些个人信息 2)询问数据库管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录数据库所存储的个人信息。如数据库存储了用户身份证号、电话等个人信息 2)记录数据库哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合情况：数据库所存储的用户个人信息均为业务所必需的，不存在非必要用户个人信息 部分符合情况：无 不符合情况：数据库违规保存非业务必需的用户个人信息
	b)应禁止未授权访问和非法使用用户个人信息		1)询问数据库管理员，哪些数据库账户可以访问个人信息，且数据库采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了数据库账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合情况：系统已采取措施限制了数据库账户对个人信息的访问，非授权用户无法访问和使用用户的个人信息，且已制定相关个人信息保护制度 部分符合情况：无 不符合情况：未对用户个人信息的访问和使用进行严格的管理，未采取措施来禁止非授权访问和非法使用个人信息

安全计算环境（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
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Sql server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，口令复杂(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）展开服务器组，编辑SQL Server注册属性，查看身份认证方式；或者直接登录SQL Server企业管理器，试图连接数据库，查看系统是否出现用户和密码的输入框。 3）1）询问是否在安装时立刻修改sa口令，用该用户和常见密码试图登录数据库系统，查看是否成功。 4）2）在SQL 查询分析器中执行命令: use master select * from syslogins where password is null 查看是否有空口令用户。 5）询问口令的管理要求，如口令的长度、口令复杂性和口令更新周期等方面的管理要求。	1）选中“使用SQL Server身份认证”，并且选中“总是提示输入用户名和密码”。 2）提示用户输入密码。 3）sa用户的口令不是常见口令。 4）无空口令用户。	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	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	访谈管理员是否启用登录失败处理功能：是否限制用户尝试登录次数、登录尝试失败次数超过一定次数后数据库对用户的处理策略。	1）如果没有采用第三方工具或对SQL Server2000安全功能进行增强，则该项要求为不符合。	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	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）询问是否能对数据库进行远程管理; 2）在服务器网络实用工具中查看是否启用“强制协议加密(C)”。	如果能够对数据库进行远程管理，则应选中“强制协议加密(C)”，并对其进行配置。	符合情况：采用的远程管理方式启用了SSL连接特性，采取SSH隧道加密连接远程管理通信 部分符合情况：无 不符合情况：采用未进行加密处理的远程管理方式
	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	Sql server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	访谈系统管理员并核查系统除用户名+口令外有无其他身份鉴别方法，如有没有令牌、数字证书和生物技术等，且其中一种鉴别技术至少应使用密码技术来实现。	采用除用户口令外另一种密码技术，可调用密码机制或使用SM1-SM4密码技术	符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，且在硬件Ukey中使用了加密算法 部分符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，但采用加密算法 不符合情况：未部署堡垒机，未通过堡垒机管理服务器来实现双因素身份验证
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	1）在“企业管理器”-）“安全性”中，选中每个登录用户，在右键菜单中选择“属性”，查看是否为每个用户指定了角色和能够对每个数据库的访问权限。	为每个登录用户指定了角色，并限定了每个角色的访问权限。	符合情况：已创建不同账户，并且根据用户所需为其分配相应的权限 部分符合情况：已创建不同的用户，但未进行权限的划分 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	SQL Server中的默认账户是sa账户，是在安装数据库时，初始化设置时设置的密码，sa账户是可以重命名或者删除的，至于默认口令，sa是不存在的，一般就是修改一下sa的名称	1）询问并验证sa用户的密码是否是空口令或弱口令; 2）现场让用户登录一次进行测试，验证用户的密码是否与描述一致。	管理用户sa的密码不是空口令和弱口令。	符合情况：不存在默认的、无用的可登录账户，已删除或禁用默认账户 部分符合情况：存在默认账户，但已修改默认账户默认口令 不符合情况：存在默认账户，且默认账户口令也未修改
	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	访谈并核查数据库表中用户是否存在多余的、过期的账户，并询问管理员账户是否与自然人做到一一对应，不存在多人共用一个账户的情况。	不存在多余过期和共享账户。	符合情况：不存在默认的、无用的可登录账户， 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改
	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	数据库的权限划分跟业务多少有非常大的关系，一般是有多少业务就有多少数据库，有多少数据库就有多少用户管理，我们给数据库划分权限，也最好按照数据库来划分	1）在“企业管理器”-）“安全性”中，选中每个登录用户，在右键菜单中选择“属性”，查看每个登录用户的角色和权限，是否是该管理用户所需的最小权限。	为每个登录用户授予所需的最小权限。	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理

	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)	访谈管理员数据库使用的访问控制模型是否通过访问控制策略控制主体对客体的访问控制规则。。	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	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	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	符合情况：已指定授权主体（一般为安全管理员）对数据库访问控制权限进行配置，且授权主体为用户，客体未数据库表 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	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	SQL Server本身并不具备这项功能，要想达到这一要求，就必须借助第三方软件了，这就需要根据被测评方所使用的的软件具体分析	1） 查看操作系统功能手册或相关文档，确认操作系统是否具备能对信息资源设置安全标记功能； 2） 询问管理员是否对重要信息资源设置安全标记。 3） 询问或查看目前的安全标记策略的相关设置，如：如何划分敏感标记分类，如何设定访问权限等。	1）主要数据库管理系统对重要信息资源设置敏感标记；2）强制访问控制的覆盖范围包括与重要信息资源直接相关的所有主体、客体及它们之间的操作。	符合情况：在数据库所在操作系统上，已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：在数据库所在操作系统上，已配置安全标记，但安全标记配置不合理等 不符合情况：未在数据库所在操作系统上对重要主体或客体设置安全标记
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）在“企业管理器”-〉右键单击注册名称-〉点击“属性”-〉“安全性”，查看审核级别。 2）访谈数据库管理员，了解是否采取第三方工具增强SQL Server的日志功能。	审核级别为“全部”。	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
	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）访谈数据库数据库管理员，了解是否采取第三方工具增强SQL Server的日志功能。 2）如果有第三方工具，则查看审计记录内容是否包括日期和时间、类型、主体标识、客体标识、事件的结果等。	有第三方工具且审计记录内容包括日期和时间、类型、主体标识、客体标识、事件的结果等。	符合情况：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 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录
	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Sqlserver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	1）访谈操作系统管理员，了解对SQL Server2000的日志记录采取的保护措施。	操作系统提供相关保护措施，不能被非授权破坏；通过备份审计记录文档避免未预期的覆盖。	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	d)应对审计进程进行保护，防止未经授权的中断	sqlserver数据库审计进程系统默认开启，无法停止	默认符合	默认符合	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作
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	Sqlserver数据库限制远程连接IP地址	在防火墙上做配置，只允许特定的IP地址建立1433通讯	已做限制符合	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	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	1） 应核查是否不存在高风险漏洞,如漏洞扫描、渗透测试等; 2） 应核查是否在经过充分测试评估后及时修补漏洞。	1、有运维团队定期进行漏洞扫描，发现安全风险、及时修补 2、更新补丁时间为最近，对补丁进行控制和管理	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
数据备份恢	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)询问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	符合情况：已提供重要数据处理系统的热冗余，如热备、集群、负载均衡等高可用方式 部分符合情况：无 不符合情况：未提供重要数据处理系统的热冗余

数据备份恢复	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	符合情况：已提供异地数据备份功能，实时将数据备份至异地备份机房 部分符合情况：已提供异地数据备份功能，但未实时将数据备份至异地机房 不符合情况：未提供异地数据备份功能
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该数据库的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）数据库提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）数据库检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合情况：已采用校验技术或密码技术保障重要数据在传输过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在传输过程中的完整性
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问数据库管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)数据库采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)数据库可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合情况：已采用校验技术或密码技术保障重要数据在存储过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在存储过程中的完整性
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)数据库管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合情况：已采用密码技术保障重要数据在传输过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在传输过程中的保密性
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合情况：已采用密码技术保障重要数据在存储过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在存储过程中的保密性
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	数据库将用户的鉴别信息所在的存储空间完全清理后才能分配	询问数据库管理员，数据库是否采取措施保证对存储介质防止其他用户非授权获取该用户的鉴别信息	数据库采取措施保证对存储介质中的用户鉴别信息进行及时清除。	符合情况：数据库已采取措施保证对存储介质中的用户鉴别信息进行及时清除 部分符合情况：无 不符合情况：数据库未采取措施保证对存储介质中的用户鉴别
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	数据库应将敏感数据所在的存储空间清除后才能分配给其他用户	询问数据库管理员，数据库是否采取措施保证对存储介质中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	数据库采取了措施保证对存储介质中的敏感数据进行及时清除，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：数据库采取了措施保证对存储介质中的敏感数据进行及时清除，以及对存有用户鉴别信息的临时文件进行删除或内容清除信息进行及时清除 部分符合情况：无 不符合情况：数据库未采取措施保证对存储介质中的敏感数据进行及时清除，以及对存有用户鉴别信息的临时文件进行删除或内容清除
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	保护个人信息，不采集业务不需要的个人数据	1)询问数据库管理员,该系统采集了用户的哪些个人信息 2)询问数据库管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录数据库所存储的个人信息。如数据库存储了用户身份证号、电话等个人信息 2)记录数据库哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合情况：数据库所存储的用户个人信息均为业务所必需的，不存在非必要用户个人信息 部分符合情况：无 不符合情况：数据库违规保存非业务必需的用户个人信息
	b)应禁止未授权访问和非法使用用户个人信息	数据库应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问数据库管理员，哪些数据库账户可以访问个人信息，且数据库采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了数据库账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合情况：系统已采取措施限制了数据库账户对个人信息的访问，非授权用户无法访问和使用用户的个人信息，且已制定相关个人信息保护制度 部分符合情况：无 不符合情况：未对用户个人信息的访问和使用进行严格的管理，未采取措施来禁止非授权访问和非法使用个人信息

安全计算环境-网络设备-cisco（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
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	1、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 核查是否使用口令鉴别机制对登录用户进行身份标识和鉴别，用户标识是否唯一，是否存在密码为空的用户。 2、访谈管理员口令复杂度，并查看管理员登录过程验证；访谈管理员口令更换周期，并查看口令更改记录。 口令组成:应由数字、字母、特殊字符组成 口令长度:应大于8位 口令更换周期:口令一般三个月换一次	1）采取用户名口令进行身份鉴别; 2）身份标识具有唯一性; 3）用户口令8位以上由数字字母符号组成; 4）定期（90天以内）更换用户口令。	符合情况：采用了一种及以上的身份鉴别方式，身份标识具备唯一性，用户口令8位及以上，口令组成由大小写字母、数字和字符组成，口令每90天进行一次更换。 部分符合情况：预期结果1,2,3,4满足一部分为部分符合。 不符合情况：未采取身份鉴别方式，用户口令8位以下，且口令组成未采用大小写字母、数字和特殊字符，未定期进行口令更换。
	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.默认登陆3次失败断开连接，不会锁定。检查登录失败锁定情况，分两种情况: a、telnet管理: 存在如下配置：login block-for 20 attempts 3 within 60 b、SSH管理: show ip ssh 查看如下配置 %Please create RSA keys (of atleast 768 bits size) to enable SSH v2. Authentication timeout: 120 secs; Authentication retries: 3 2、查看空闲超时时间：show running-config，查看VTY口下如下配置：exec-timeout X（分） X（秒）。 3、尽量争取测试验证。	1）启用了登录失败处理功能; 2）非法登录达到一定次数后将账户锁定; 3）配置了连接超时自动退出功能，超时时间不大于30分钟。	符合情况：启用了登录失败处理功能，且非法登录达到一定次数后进行限制，配置了连接自动退出功能。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：未配置登录失败处理功能，未配置非法登录限制措施，未配置登录连接自动超时退出功能。
	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	核查远程管理采用何种协议， 输入show run命令，查看如下类似配置: line vty 0 4 exec-timeout 5 0 privilege level 15 password 7 05080F1C2243 transport input ssh	1）采用SSH、HTTPS等加密或其他的安全方式进行远程管理。	符合情况：采用SSH或HTTPS的加密方式进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：采用telnet、http的方式进行远程管理。
	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	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	1、访谈身份鉴别过程采用哪几种鉴别技术，并查看管理员登录过程验证; 2、检查鉴别机制中是否采用了密码技术，如调用了密码机或采取SM1- SM4等算法	1）同时采用两种或两种以上组合的鉴别方式对用户身份进行鉴别; 2）其中一种方式采用密码技术。	符合情况：同时采用两种或两种以上的身份鉴别方式，且其中一种鉴别方式采用了密码技术。 部分符合情况：采用了两种及两种以上的身份鉴别方式，但未包含密码技术。 不符合情况：未同时采用两种或两种以上的身份鉴别方式。
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、核查用户账户和权限设置情况，输入show run命令，查看如下配置: username XXXXXXXX privilege xx password XXXXXXXX 2、访谈各帐户权限是否与相关管理人员职位相对应。	1）各帐户权限设置与实际业务需求一致。	符合情况：对登录的用户分配了不同的账户，且分配了不同的权限。 部分符合情况：无部分符合情况。 不符合情况：未对登录的用户分配不同的账户，且未分配相关的权限。
	b)应重命名或删除默认账户，修改默认账户的默认口令	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、输入show run命令，查看如下配置: username XXXXXXXX privilege xx password XXXXXXXX 核查是否存在默认帐户，如username为cisco、Cisco的帐户; 2、访谈管理是否修改默认口令，查看登录过程验证。	1）重命名默认账户、禁用或删除默认账户; 2）修改了默认帐户的默认口令。	符合情况：已重命名或删除默认账户，且已修改默认账户的默认口令。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未重命名或删除默认账户，且使用默认口令登录。
	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	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、输入show run命令，查看如下配置: username XXXXXXXX privilege xx password XXXXXXXX 确认各个账户是否必要。 2、是否存在不同管理员使用同一账户。	1）不存在多余或过期账户; 2）不存在共用账户。	符合情况：通过show running未发现多余、过期账户存在，且管理员用户与账户之间一一对应，无共享账户存在。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：设备存在多余、过期账户，且存在共享账户。
	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。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、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 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。	1）合理角色划分，管理用户的权限是否已进行分离（如管理员、审计员、操作员）; 2）各用户权限为其工作任务所需的最小权限。	符合情况：创建有系统管理员、审计管理员、安全管理员等账户通过LEVEL进行等级划分，并赋予去角色权限，各账户仅分配最小的权限。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未创建系统管理员、审计管理员、安全管理员等账户角色，各账户均具备相同的管理员权限。
	e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	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	×	×
	f)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	×	×
	g)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	×	×
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	查看日志开启情况：show logging查看如下配置: Console logging（控制台日志）: level debugging, 0 messages logged, xml disabled,filtering disabled Monitor logging（监控日志）: level debugging, 0 messages logged, xml disabled, filtering disabled Buffer logging（缓冲区日志）：enabled, xml disabled, filtering disabled	1）开启了日志审计功能; 2）对重要的用户行为和重要安全事件进行了审计。	符合情况：设备已开启log日志功能，审计范围能覆盖到每个用户，并对每个重要安全事件进行审计。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：设备未开启日志功能，未能审计到每个用户行为以及重要安全事件。
	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	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	1)查看具体日志：show loggin buffer，查看如下配置 %Oct 30 08:15:06:588 2015 HZ7503E-S OPTMOD/4/MODULE_IN:GigabitEthernet0/0/1: The transceiver is 1000_BASE_SX_SFP. 查看记录是否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。 2)查看设备时间是否与当前日期相符，确认日志的有效性：show clock *0:0:22.653 UTC Mon Mar 1 1993;	1）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; 2）系统时间正确。	符合情况：审计记录能覆盖到具体的日期和时间、用户、事件类型、事件是否成功及审计相关信息，系统时间正确。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未开启审计功能，审计记录未包含日期和时间、用户、事件类型、事件是否成功及其他审计信息。
	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	1）输入命令"show run",查看如下配置：logging host 192.168.100.252；核查是否将日志发送至日志服务器或第三方日志管理平台; 2）访谈采用哪些日志备份方式，查看备份的日志记录。	1）采取技术措施对审计记录进行保护; 2）将日志发送到日志服务器或综合安全审计系统保存; 3）定期备份设备审计记录。	符合情况：部署有第三方日志审计系统，设备日志上传至第三方审计平台进行保护，日志保存时间长达6个月。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：未部署第三方日志审计系统，未对审计记录进行保护，日志保存时间不满足6个月。
	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	1）核查非审计员的其他账户是否能中断审计进程; 2）核查是否通过堡垒机进行管理，远程管理地址是否限制为堡垒机。	1）非审计员的其他账户不能中断审计进程; 2）通过堡垒机对设备进行管理，且远程管理地址限制为堡垒机。	符合情况：非审计管理员的其他账户不能中断审计进程。 部分符合情况：无部分符合情况。 不符合情况：非审计管理员的其他账户能中断审计进程。
	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	×	×

控制点 安全要求 要求解读 测评方法 预期结果或主要证据

入侵防范	b)应关闭不需要的系统服务、默认共享和高危端口	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	输入show run命令。根据实际网络环境参考是否关闭不必要服务: 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	1）已关闭非必要的系统服务。	符合情况：已关闭不需要的系统服务、默认共享和高危端口等。 部分符合情况：无部分符合情况。 不符合情况：存在多余系统服务ftp, telnet等，存在高危端口和共享端口等。
	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)	输入show run命令，查看如下类似配置: access-list 10 access-list 10 permit 192.168.0.1 access-list 10 deny any line vty 0 4 access-class 10 in 核查是否对设备远程管理地址进行了限制，限制范围是否仅管理终端或堡垒机。	1）仅允许管理终端或堡垒机远程登录设备。	符合情况：通过策略限制设备仅通过某地址或地址段可进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：未采取措施对远程管理设备的地址进行限制。
	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	×	×
	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）访谈是否定期进行漏洞扫描，查看漏洞扫描报告; 2）是否对已发现的漏洞在经过充分测试评估后及时修补。	1）定期（至少每年一次，测评扫的不算）进行漏洞扫描，并生成漏洞扫描报告; 2）及时修补漏洞或经过测试评估后充分说明漏洞不进行修补。	符合情况：定期对设备进行漏洞扫描，且针对发现的漏洞经过测试评估后及时进行修补。 部分符合情况：无部分符合情况。 不符合情况：未定期对设备进行漏洞扫描，且未进对发现的漏洞进行测评评估后及时进行修补。
	f)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	×	×
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	×	×
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 (2.3)	1)计算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)	符合情况：计算设备均部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。 部分符合情况：预期结果1，2，3，4点满足一部分为部分符合。 不符合情况：未采取措施计算设备部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能;
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别信息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除;
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除;
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能; 部分符合：无部分符合 不符合：系统采集信息非业务必要;
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用; 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露;

安全计算环境-网络设备-H3C（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
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	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"即【dis cu】命令；检查是否存在如下配置： # telnet server enable【登录通道】 # user-interface vty 0 15 authentication-mode scheme user-role network-admin user-role network-operator # local-user user1【用户名】 class manage service-type telnet【用户登录方式】 authorization-attribute user-role level-9【用户权限】 password-control aging 1【口令老化时间1天】 password-control length 24【长度24个字符】 password-control composition type-number 4 type-length 5【复杂度：4种字符每种长度5个字符】 # 或者"display password-control super【用户名】"，检查是否存在以下配置： Super password control configurations: Password aging: Enabled (30 days) Password length: Enabled (10 characters) Password composition: Enabled (3 types, 5 characters per type) 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）采取一种或以上身份鉴别措施; 2）身份标识具有唯一性; 3）用户口令8位以上由数字字母符号组成; 4）定期（90天以内）更换用户口令。	符合情况：采用了一种及以上的身份鉴别方式，身份标识具备唯一性，用户口令8位及以上，口令组成由大小写字母、数字和字符组成，口令每90天进行一次更换。 部分符合情况：预期结果1,2,3,4满足一部分为部分符合。 不符合情况：未采取身份鉴别方式，用户口令8位以下，且口令组成未采用大小写字母、数字和特殊字符，未定期进行口令更换。
	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.网络设备默认启用登录失败处理功能。 2.网络设备设置的登录失败处理功能： H3C:输入 display password-control 存在如下配置： password-control login-attempt 3 exceed locktime 360 华为/H3C路由器: 输入display current-configuration命令,存在如下类似配置 idle-timeout 20	1）启用并配置了登录失败处理功能; 2）非法登录达到一定次数后将账户锁定; 3）配置了连接超时自动退出功能，超时时间不大于30分钟。	符合情况：启用了登录失败处理功能，且非法登录达到一定次数后进行限制，配置了连接自动退出功能。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：未配置登录失败处理功能，未配置非法登录限制措施，未配置登录连接自动超时退出功能。
	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	1、直接对设备进行远程管理时，华为H3C:输入【diSplay curent-configuration】命令，查看是否存在如下类似配置： 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 如果service-type 后的参数为明文传输协议则不符合要求。 2、网络设备通过堡垒机进行远程管理参照1、执行。	1）采用SSH、HTTPS等加密或其他的安全方式进行远程管理。	符合情况：采用SSH或HTTPS的加密方式进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：采用telnet、http的方式进行远程管理。
	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	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	1、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	1）同时采用两种或两种以上组合的鉴别方式对用户身份进行鉴别，且其中一种方式采用密码技术。	符合情况：同时采用两种或两种以上的身份鉴别方式，且其中一种鉴别方式采用了密码技术。 部分符合情况：采用了两种及两种以上的身份鉴别方式，但未包含密码技术。 不符合情况：未同时采用两种或两种以上的身份鉴别方式。
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)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 华为H3C交换机输入【diSplay curent-configuration】查看设备中存在的账号，与管理员核对一下配置中的账号对应的管理人员和权限设置情况； # user-interface vty 0 15 authentication-mode scheme user-role network-operator 【network-operator为默认权限名】 # role name network-operator rule 1 permit read write execute feature aaa rule 2 permit read write execute feature device --------------------------------------- 进一步查看用户权限【dispaly role name network-operator（权限名称）】 配置参考如下： <Switch> display role name role1 Role: role1 Description: VLAN policy: permit (default) Interface policy: permit (default) VPN instance policy: permit (default) --- Rule Perm Type Scope Entity --- 1 permit RWX feature aaa 2 permit RWX feature device R:Read W:Write X:Execute	1）各帐户权限设置与实际业务需求一致。	符合情况：对登录的用户分配了不同的账户，且分配了不同的权限。 部分符合情况：无部分符合情况。 不符合情况：未对登录的用户分配不同的账户，且未分配相关的权限。
	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、使用默认账户和默认口令无法登录路由器 2、华为H3C交换机不存在默认账户admin, huawei 华为H3C交换机输入"display local-user"确认存在的用户	1）重命名默认账户、禁用或删除默认账户; 2）修改了默认帐户的默认口令。	符合情况：已重命名或删除默认账户，且已修改默认账户的默认口令。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未重命名或删除默认账户，且使用默认口令登录。
	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	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、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 2、与管理员确认账号的使用人员，分析是否存在共享账户、过期多余账户。	1）不存在多余或过期账户; 2）管理员用户与账户之间一一对应。	符合情况：通过display current-configuration未发现多余、过期账户存在，且管理员用户与账户之间一一对应，无共享账户存在。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：设备存在多余、过期账户，且存在共享账户。
	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。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、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、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	1）合理角色划分，管理用户的权限是否已进行分离（如管理员、审计员、操作员）; 2）各用户权限为其工作任务所需的最小权限。	符合情况：创建有系统管理员、审计管理员、安全管理员等账户通过LEVEL进行等级划分，并赋予去角色权限，各账户仅分配最小的权限。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未创建系统管理员、审计管理员、安全管理员等账户角色，各账户均具备相同的管理员权限。
	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	×	×	×
	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，	×	×	×
	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。	×	×	×
	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、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	1）开启了日志审计功能; 2）审计范围覆盖到每个用户; 3）对重要的用户行为和重要安全事件进行了审计。	符合情况：设备已开启log日志功能，审计范围能覆盖到每个用户，并对每个重要安全事件进行审计。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：设备未开启日志功能，未能审计到每个用户行为以及重要安全事件。

控制点　安全要求　要求解读　测评方法　预期结果或主要证据

安全审计	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	1、华为/H3C:网络设备配置的日志策略，通过输入"display logging"或"display logbuffer"命令，存在如下类似配置： %Jan 31 00:38:22:216 2019 Spine ACL/6/PFILTER_STATIS_INFO: -MDC=1-Chassis=1-Slot=1; GigabitEthernet1/1/0/42 (inbound): Packet-filter 3333 rule 2 permit icmp source 192.168.1.10 0 logging counting 7 packet(s).	1）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； 2）系统时间正确。	符合情况：审计记录能覆盖到具体的日期和时间、用户、事件类型、事件是否成功及审计相关信息，系统时间正确。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未开启审计功能，审计记录未包含日期和时间、用户、事件类型、事件是否成功及其他审计信息。
	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，历正未授权修改、删除和破坏	1、华为/H3C:网络设备配置的日志策略，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	1）部署了综合安全审计系统； 2）采取技术措施对审计记录进行保护； 3）定期备份设备审计记录。	符合情况：部署有第三方日志审计系统，设备日志上传至第三方审计平台进行保护，日志保存时间长达6个月。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：未部署第三方日志审计系统，未对审计记录进行保护，日志保存时间不满足6个月。
	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	×	1）非审计员的其他账户不能中断审计进程。	符合情况：非审计管理员的其他账户不能中断审计进程。 部分符合情况：无部分符合情况。 不符合情况：非审计管理员的其他账户能中断审计进程。
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	×	×	×
	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	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	1）已关闭非必要的系统服务。	符合情况：已关闭不需要的系统服务、默认共享和高危端口等。 部分符合情况：无部分符合情况。 不符合情况：存在多余系统服务ftp，telnet等，存在高危端口和共享端口等。
	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)	检查配置信息中存在类似如下配置信息: acl number 2001 rule 10 permit source 10.1.100.0.0.0.0.255 user-interface vty 0 4 acl 2001 inbound authentication-mode scheme user privilege level 1	1）仅允许管理主机远程登录设备。	符合情况：通过策略限制设备仅通过某地址或地址段可进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：未采取措施对远程管理设备的地址进行限制。
	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	×	×	×
	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）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。	符合情况：定期对设备进行漏洞扫描，且针对发现的漏洞经过测试评估后及时进行修补。 部分符合情况：无部分符合情况。 不符合情况：未定期对设备进行漏洞扫描，且未进对发现的漏洞进行测评评估后及时进行修补。
	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，以检查是否发生了入侵和攻击	×	×	×
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	×	×	×
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(2.3)	1)计算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)	符合情况：计算设备均部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。 部分符合情况：预期结果1，2，3，4点满足一部分为部分符合。 不符合情况：未采取措施计算设备部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别信息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除；

个人信息保护	a)应仅采集和保存业务必需的用户个人信息	系统是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务必用必需的	1）记录系统所采集的个人信息，如系统采集了身份证号、电话等个人信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名、电话，用于XXX,XXX功能; 部分符合：无部分符合 不符合：系统采集信息非业务必需。
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)检查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息重点界面进行了脱敏处理，防止个人信息的非法使用。 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到。 且相关人员未签署保密协议，防止个人信息泄露;

安全计算环境-网络设备-华为（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
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	1)输入diplay current-configuration命令,查看是否存在如下类似配置: local-user netadmin password irreversible-cipher xxxxx 核查用户在登录时是否采用了身份签别措施，是否存在密码为空的用户。 2)访谈管理员口令复杂度，并查看管理员登录过程验证；访谈管理员口令更换周期，并查看口令更改记录。 口令组成:应由数字、字母、特殊字符组成 口令长度:应大于8位 口令更换周期:口令一般三个月换一次 PS:策略检查: 3）输入"display current-configuration"即【dis cu】命令；检查是否存在如下配置: set password min-length 6 4）（华为设备没有配置复杂度功能，但有的版本系统出厂自带了，因此需要）新建测试帐户，设置口令时测试是否可以设置简单口令。	1）采取一种或以上身份鉴别措施; 2）身份标识具有唯一性; 3）用户口令8位以上由数字字母符号组成; 4）定期（90天以内）更换用户口令。	符合情况：采用了一种及以上的身份鉴别方式，身份标识具备唯一性，用户口令8位及以上，口令组成由大小写字母、数字和字符组成，口令每90天进行一次更换。 部分符合情况：预期结果1,2,3,4满足一部分为部分符合。 不符合情况：未采取身份鉴别方式，用户口令8位以下，且口令组成未采用大小写字母、数字和特殊字符，未定期进行口令更换。
	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）默认登陆3次失败断开连接，不会锁定。检查登录失败锁定情况，输入"display current-configuration"；检查是否存在如下配置: local-aaa-user wrong-password retry-interval 5 retry-time 3 block-time 8 2）查看空闲超时时间设置情况：输入"display current-configuration"； line vty 0 4 idle-timeout 20	1）启用并配置了登录失败处理功能; 2）非法登录达到一定次数后将账户锁定; 3）配置了连接超时自动退出功能，超时时间不大于30分钟。	符合情况：启用了登录失败处理功能，且非法登录达到一定次数后进行限制，配置了连接自动退出功能。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：未配置登录失败处理功能，未配置非法登录限制措施，未配置登录连接自动超时退出功能。
	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	访谈管理员管理方式（本地管理/远程管理），核查远程管理采用何种协议，输入"display current-configuration"检查如下配置: # telnet server enable ssh server enable dhcp enable # 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	1）采用SSH、HTTPS等加密或其他的安全方式进行远程管理; 2）本地管理。	符合情况：采用SSH或HTTPS的加密方式进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：采用telnet、http的方式进行远程管理。
	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	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	1、访谈身份鉴别过程采用哪几种鉴别技术，并查看管理员登录过程验证; 2、检查鉴别机制中是否采用了密码技术，如调用了密码机或采取SM1- SM4等算法	1）同时采用两种或两种以上组合的鉴别方式对用户身份进行鉴别，且其中一种方式采用密码技术。	符合情况：同时采用两种或两种以上的身份鉴别方式，且其中一种鉴别方式采用了密码技术。 部分符合情况：采用了两种及两种以上的身份鉴别方式，但未包含密码技术。 不符合情况：未同时采用两种或两种以上的身份鉴别方式。
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、核查用户账户和权限设置情况，输入：dis local-user，查看如下配置: -- User-name State AuthMask AdminLevel -- admin A TMSH 15 guest A TS 1 test123 A S 1 2、访谈各帐户权限是否与相关管理人员职位相对应。	1）各帐户权限设置与实际业务需求一致。	符合情况：对登录的用户分配了不同的账户，且分配了不同的权限。 部分符合情况：无部分符合情况。 不符合情况：未对登录的用户分配不同的账户，且未分配相关的权限。
	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、核查用户账户设置情况，输入：dis local-user，查看如下配置，确定设备中的用户: -- User-name State AuthMask AdminLevel -- admin A TMSH 15 guest A TS 1 test123 A S 1 查看是否存在帐户; 2、若存在默认帐户，访谈管理是否修改默认口令，查看登录过程验证。	1）重命名默认账户、禁用或删除默认账户; 2）修改了默认帐户的默认口令。	符合情况：已重命名或删除默认账户，且已修改默认账户的默认口令。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未重命名或删除默认账户，且使用默认口令登录。
	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	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、命令同上; 2、核查网络管理员、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	1）不存在多余或过期账户; 2）管理员用户与账户之间一一对应。	符合情况：通过display current-configuration未发现多余、过期账户存在，且管理员用户与账户之间一一对应，无共享账户存在。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：设备存在多余、过期账户，且存在共享账户。
	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。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、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、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"；检查是否存在如下配置: # telnet server enable【登录通道】 # user-interface vty 0 15 authentication-mode scheme user-role network-admin user-role network-operator # local-user user1【用户名】 class manage service-type telnet【用户登录方式】 authorization-attribute user-role level-9【用户权限】 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	1）合理角色划分，管理用户的权限是否已进行分离（如管理员、审计员、操作员）; 2）各用户权限为其工作任务所需的最小权限。	符合情况：创建有系统管理员、审计管理员、安全管理员等账户通过LEVEL进行等级划分，并赋予去角色权限，各账户仅分配最小的权限。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未创建系统管理员、审计管理员、安全管理员等账户角色，各账户均具备相同的管理员权限。
	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	×	×	×
	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,	×	×	×
	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。	×	×	×
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	查看日志开启情况：display logbuffer Logging buffer configuration and contents : enabled Allowed max buffer size : 1024 Actual buffer size : 512 Channel number : 4 , Channel name : logbuffer Dropped messages : 0 Overwritten messages : 0 Current messages : 1 Oct 6 2016 09:55:43-08:00 Huawei %%01GTL/4/STATECHANGED(l)[0]:License state changed from Default to Default.	1）开启了日志审计功能; 2）审计范围覆盖到每个用户; 3）对重要的用户行为和重要安全事件进行了审计。	符合情况：设备已开启log日志功能，审计范围能覆盖到每个用户，并对每个重要安全事件进行审计。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：设备未开启日志功能，未能审计到每个用户行为以及重要安全事件。
	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	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	1、查看日志内容是否完整：输入display logbuffer Logging buffer configuration and contents : enabled Allowed max buffer size : 1024 Actual buffer size : 512 Channel number : 4 , Channel name : logbuffer Dropped messages : 0 Overwritten messages : 0 Current messages : 1 Oct 6 2016 09:55:43-08:00 Huawei %%01GTL/4/STATECHANGED(l)[0]:License state changed from Default to Default. 2、查看系统时间，对当前时间对比是否正确：输入dis clock,查看如下配置 2019-09-29 11:21:25 Time Zone(DefaultZoneName) : UTC	1）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; 2）系统时间正确。	符合情况：审计记录能覆盖到具体的日期和时间、用户、事件类型、事件是否成功及审计相关信息，系统时间正确。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未开启审计功能，审计记录未包含日期和时间、用户、事件类型、事件是否成功及其他审计信息。
	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	1、查看日志是否发送至第三方保存，输入"display current-configuration"，查看是否存在如下配置: info-center loghost 10.1.8.1 2、访谈采用哪些日志备份方式，查看备份的日志记录。	1）部署了综合安全审计系统; 2）采取技术措施对审计记录进行保护; 3）定期备份设备审计记录。	符合情况：部署有第三方日志审计系统，设备日志上传至第三方审计平台进行保护，日志保存时间长达6个月。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：未部署第三方日志审计系统，未对审计记录进行保护，日志保存时间不满足6个月。

控制点 安全要求 要求解读 测评方法 预期结果或主要证据

	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	1）核查非审计员的其他账户是否能中断审计进程; 2）核查是否通过堡垒机进行管理，远程管理地址是否限制为堡垒机。	1）非审计员的其他账户不能中断审计进程; 2）通过堡垒机对设备进行管理，且远程管理地址限制为堡垒机。	符合情况：非审计管理员的其他账户不能中断审计进程。 部分符合情况：无部分符合情况。 不符合情况：非审计管理员的其他账户能中断审计进程。
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	×	×	×
	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	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: http shutdown	1）已关闭非必要的系统服务。	符合情况：已关闭不需要的系统服务、默认共享和高危端口等。 部分符合情况：无部分符合情况。 不符合情况：存在多余系统服务ftp，telnet等，存在高危端口和共享端口等。
	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)	输入命令""dis cu"，检查配置信息中存在类似如下配置信息: acl number 2001 rule 10 permit source 10.1.100.0.0.0.0.255 user-interface vty 0 4 acl 2001 inbound authentication-mode scheme user privilege level 1 核查是否对设备远程管理地址进行了限制，限制范围是否仅管理终端或堡垒机。	1）仅允许管理主机远程登录设备。	符合情况：通过策略限制设备仅通过某地址或地址段可进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：未采取措施对远程管理设备的地址进行限制。
	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	×	×	×
	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）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。	符合情况：定期对设备进行漏洞扫描，且针对发现的漏洞经过测试评估后及时进行修补。 部分符合情况：无部分符合情况。 不符合情况：未定期对设备进行漏洞扫描，且未进对发现的漏洞进行测评评估后及时进行修补。
	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，以检查是否发生了入侵和攻击	×	×	×
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	×	×	×
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 (2.3)	1)计算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)	符合情况：计算设备均部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。 部分符合情况：预期结果1，2，3，4点满足一部分为部分符合。 不符合情况：未采取措施计算设备部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份; 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份;
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份, 部分符合：无部分符合 不符合：未提供异地实施备份功能;
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除;
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除;
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能; 部分符合：无部分符合 不符合：系统采集信息非业务必要;
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用; 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露;

安全计算环境-中间件（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
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	1)应核查用户在登录时是否采用了身份鉴别措施; 2)应核查用户列表确认用户身份标识是否具有唯一性; 3)应核查用户配置信息或测试验证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)cat /login.defs (查看口令可用天数、修改口令间隔天数、口令最小长度) 2)cat /etc/security/pwquality.conf (查看口令复杂度)	1)身份标识具有唯一性 2)采取身份鉴别措施（如通过用户名加口令方式进行身份鉴别） 3)当前口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换（更换周期3个月以内） 4)强制口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换（更换周期3个月以内）	符合情况：需同时保证身份标识唯一性、存在身份鉴别措施、口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换、更换口令时校验口令复杂度达到8位以上，至少三种字符类型组成。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	1)应核查是否配置并启用了登录失败处理功能; 2)应核查是否配置并启用了限制非法登录功能，非法登录达到一定次数后采取特定动作，如账户锁定等; 3)应核查是否配置并启用了登录连接超时及自动退出功能。	1)cat /pam.d/system-auth (查看登陆失败处理次数和限制时间)　　2)cat /etc/profile | grep TMOUT (查看登陆超时自动退出策略--本地) 3)cat /etc/ssh/sshd_config | grep Client（查看登陆超时自动退出策略--通过ssh链接的登录）	1)启用登录失败功能，登录失败X（不超过10）次，锁定账户X（不超过60）分钟 2)启用登录超时策略，登录超时X（30分钟以内）分钟自动退出	符合情况：启用登录失败功能和登录连接超时策略。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	中间件是否采用加密等安全方式对系统进行远程管理，能否防止鉴别信息在网络传输过程中被窃听;	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;	采用HTTPS加密传输方式	符合情况：采用安全加密协议进行传输。 不符合情况：未采用安全加密协议无法保证数据在传输过程中的完整性。
	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	中间件是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别;	1)应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别; 2)应核查其中一种鉴别技术是否使用密码技术来实现。	1)采用双因子认证（短信验证码不算） 2)其中一种必须要有密码技术，并记录采用何种算法（如Google Authenticator 动态口令使用OTP-HMAC密码技术）	符合情况：采用双因子认证方式，并且其中一种有密码技术。 不符合情况：未采用双因子认证方式。
访问控制	a)应对登录的用户分配账户和权限	1)中间件是否对用户账户和权限进行相关设置; 2)是否限制默认账户的访问权限。	1)应核查是否为用户分配了账户和权限及相关设置情况; 2)应核查是否已禁用或限制匿名、默认账户的访问权限。	1)为管理员分配相应账户 2)为账户分配管理员所需的权限 3)禁用或限制匿名、默认账户的权限	符合情况：为管理员分配相应账户和所需的权限并且禁用或限制匿名、默认账户的权限。 不符合情况：未分配相应账户和权限，或者直接使用默认账户对设备进行管理。
	b)应重命名或删除默认账户，修改默认账户的默认口令	默认账户和默认口令是否已修改;	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。	1)默认账户已重命名或者删除默认账户 2)默认账户的默认口令已进行修改	符合情况：默认账户已重命名或者删除默认账户并且默认口令已进行修改。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	管理员和账户一一对应;	1)应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对应; 2)应测试验证多余的、过期的账户是否被删除或停用。	1)不存在多余或者无效的账户 2)一个管理员一个账户	符合情况：不存在多余或者无效的账户并且一个管理员一个账户不存在共享账户。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	账户进行权限划分;	1)应核查是否进行角色划分; 2)应核查管理用户的权限是否已进行分离; 3)应核查管理用户权限是否为其工作任务所需的最小权限。	1)账户角色进行划分 2)账户权限进行三权分立 3)账户所需的权限为工作所需最小权限	符合情况：账户角色进行划分，部署三权分立，分配账户所需的权限为工作所需最小权限。 不符合情况：未划分相应账户的权限。
	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	1)应核查是否由授权主体（如管理用户）负责配置访问控制策略; 2)应核查授权主体是否依据安全策略配置了主体对客体的访问规则; 3)应测试验证用户是否有可越权访问情形。	1)ls -l /etc/passwd（记录不同账户下的该文件夹权限） 2)ls -l /etc/shadow 3)ls -l/etc/profile	1)管理用户负责配置访问控制策略，管理用户为账户分配不同的角色，每个角色分配不同的功能权限，当账户与角色关联时，该账户就具备与角色相关联的功能操作 2)非管理用户不能访问权限管理相关的功能	符合情况：配置访问控制策略，非管理用户不能访问权限管理相关的功能。 不符合情况：未配置访问控制策略。

	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	主体和客体的访问控制策略；	应核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级；	访问控制策略的控制粒度主体为登录账户，客体为功能权限以及功能权限关联的数据库表	符合情况：配置访问控制策略，控制粒度主体达到用户级或进程级，客体为功能权限以及功能权限关联的数据库表。 不符合情况：未配置访问控制策略，不存在控制主客体粒度。
	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	1)应核查是否对主体、客体设置了安全标记； 2)应测试验证是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。	getenforce （查看当前selinux运行状态--Enforcing强制、Permissive宽容、Disabled关闭）	1)安全策略对重要账户和重要信息设置了安全标记 2)安全标记控制了账户对有安全标记信息资源的访问	符合情况：依据安全策略对重要账户和重要信息设置了安全标记。 不符合情况：重要账户和重要信息未设置安全标记。
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	1)应核查是否开启了安全审计功能； 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。	1)在Apache的配置文件httpd.conf中查看是否开启error_log和access_log。 2)在Apache安装目录中查看是否有：/logs/error_log和/logs/access_log。	1)启用了安全审计功能。建立了日志审计模块。 2)安全审计范围覆盖每个用户 3)对重要的用户行为和重要安全事件提供了审计	符合情况：启用了安全审计功能。建立了日志审计模块，安全审计范围覆盖到每个用户，对重要的用户行为和重要安全事件提供了审计。 不符合情况：未开启安全审计功能，不存在日志审计模块，无法对重要的用户行为和重要安全事件提供审计。
	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；	1)查看error_log文件记录内容，查看是否包括：错误发生的日期、时间、错误等级、IP地址、内容等。 2)查看access_log文件内容，查看是否包括：客户端连接的日期、时间、IP地址、状态代码、浏览器信息等。	审计记录至少包括事件日期，时间，发起者信息(如用户名、IP地址等)、类型、描述和结果(是否成功等)等内容	符合情况：启用了安全审计功能。建立了日志审计模块，审计记录至少包括事件日期，时间，发起者信息(如用户名、IP地址等)、类型、描述和结果(是否成功等)等内容。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计记录。
	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	1)应核查是否采取了保护措施对审计记录进行保护； 2)应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。	1)查看日志在本地保存的周期和权限。查看日志轮转周期；查看日志的权限，确保操作系统普通用户无删除、修改权限。 2)查看日志是否进行异地备份，保存周期，查看操作系统中是否发送日志到备份系统、日志审计系统；若操作系统为虚拟机，查看是否通过创建快照的方式对日志进行保护。	1)日志本地存储，可查看存储目录，周期和相关策略等 2)日志无法被删除和篡改	符合情况：启用了安全审计功能。建立了日志审计模块，日志无法被删除和篡改，日志信息保存6个月以上。对日志信息进行定期备份策略。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计记录。
	d)应对审计进程进行保护，防止未经授权的中断	通过非审计管理员的其他账户能否中断审计进程，验证审计进程是否受到保护；	Apache审计进程与httpd服务相关联，无法单独中断。 检查方法：使用操作系统普通用户中断审计进程，查看是否成功。	非授权不能中断审计进程或关闭审计功能	符合情况：启用了安全审计功能。建立了日志审计模块，非授权不能中断审计进程或关闭审计功能。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计进程。
入侵防范	a)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),从而影响系统的正常使用甚至危害系统的安全	1)应核查设计文档的内容是否包括数据有效性检验功能的内容； 2)应测试验证是否对人机接口或通信接口输入的内容进行有效性检验	应具备软件容错能力，提供对输入数据的长度、格式等进行检查和验证的功能，通过限制特定关键字的输入等防护措施防止SQL注入等攻击	符合情况：系统具备软件容错能力，提供对输入数据的长度、格式等进行检查和验证的功能，通过限制特定关键字的输入等防护措施防止SQL注入等攻击。 不符合情况：系统不具备软件容错能力。
	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	攻击者可能利用中间件存在的安全漏洞进行攻击，应对中间件漏洞扫描，及时发现存在的已知漏洞，并在经过充分测试评估后更新补丁，.避免遭受漏洞带的风险	1)应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞； 2)应核查是否在经过充分测试评估后及时修补漏洞	1)中间件经过漏洞扫描或者渗透测试后不存在高风险漏洞，若存在，则经过充分测试评估后及时修补漏洞 2)放弃扫描情况下，客户自身定期进行漏扫或者安全评估等	符合情况：经过漏洞扫描或者渗透测试后不存在高风险漏洞，若存在，则经过充分测试评估后及时修补漏洞。放弃扫描情况下，客户自身定期进行漏扫或者安全评估等。 不符合情况：客户自身未定期进行漏扫或者安全评估。经过漏洞扫描或者渗透测试之后存在相应风险的漏洞信息。

数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1）应核查设计文档，重要审计数据、重要配置数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性; 2）应测试验证在传输过程中对重要审计数据、重要配置数据和重要个人信息等进行篡改,查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。	1)通过HTTPS方式保证鉴别数据、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在传输过程中的完整性 2)HTTPS协议中TSL/SSL版本为1.2以上	符合情况：通过HTTPS方式保证鉴别数据、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在传输过程中的完整性，HTTPS协议中TSL/SSL版本为1.2以上。 不符合情况：未配置HTTPS方式无法保证鉴别数据、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在传输过程中的完整性。
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)应核查设计文档，是否采用了校验技术或密码技术保证鉴别数据、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在存储过程中的完整性; 2)应核查是否采用技术措施保证鉴别数据、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在存储过程中的完整性; 3)应测试验证在存储过程中对鉴别数据、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等进行篡改，是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。	1)采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性 2)可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合情况：系统采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性。 不符合情况：系统未采用校验技术或密码技术无法保证鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性。
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)应核查设计文档，重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性; 2)应通过嗅探等方式抓取传输过程中的数据包,查看重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。	1)通过HTTPS方式保证鉴别数据、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在传输过程中的保密性 2)HTTPS协议中TSL/SSL版本为1.2以上	符合情况：通过HTTPS方式保证鉴别数据、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在传输过程中的保密性，HTTPS协议中TSL/SSL版本为1.2以上。 不符合情况：未配置HTTPS方式无法保证鉴别数据、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在传输过程中的保密性。
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1）应核查是否采用密码技术保证重要业务数据和重要个人信息等在存储过程中的保密性; 2）应核查是否采用技术措施（如数据安全保护系统等）保证重要业务数据和重要个人信息等在存储过程中的保密性; 3）应测试验证是否对指定的数据进行加密处理。	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合情况：系统采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的保密性。 不符合情况：系统未采用校验技术或密码技术无法保证鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的保密性。
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	要求用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户)	应核查相关配置信息或系统设计文档，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除	中间件采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进行及时清理。
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	要求用户的敏感数据所在的存储空间(如硬盘清除后才能分配给其他用户)	应核查相关配置信息或系统设计文档，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除	中间件采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进行及时清理。

数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1） 系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2） 系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2） 通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1:00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；

剩余信息保护	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除;
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能; 部分符合：无部分符合 不符合：系统采集信息非业务必要;
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用; 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露;

安全计算环境-中间件（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
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	1)应核查用户在登录时是否采用了身份鉴别措施; 2)应核查用户列表确认用户身份标识是否具有唯一性; 3)应核查用户配置信息或测试验证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)cat /login.defs (查看口令可用天数、修改口令间隔天数、口令最小长度) 2)cat /etc/security/pwquality.conf (查看口令复杂度)	1)身份标识具有唯一性 2)采取身份鉴别措施（如通过用户名加口令方式进行身份鉴别） 3)当前口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换（更换周期3个月以内） 4)强制口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换（更换周期3个月以内）	符合情况：需同时保证身份标识唯一性、存在身份鉴别措施、口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换、更换口令时校验口令复杂度达到8位以上，至少三种字符类型组成。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	1)应核查是否配置并启用了登录失败处理功能; 2)应核查是否配置并启用了限制非法登录功能，非法登录达到一定次数后采取特定动作，如账户锁定等; 3)应核查是否配置并启用了登录连接超时及自动退出功能。	1)cat /pam.d/system-auth (查看登陆失败处理次数和限制时间) 2)cat /etc/profile | grep TMOUT (查看登陆超时自动退出策略--本地) 3)cat /etc/ssh/sshd_config | grep Client（查看登陆超时自动退出策略--通过ssh链接的登录）	1)启用登录失败功能，登录失败X（不超过10）次，锁定账户X（不超过60）分钟 2)启用登录超时策略，登录超时X（30分钟以内）分钟自动退出	符合情况：启用登录失败功能和登录连接超时策略。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	中间件是否采用加密等安全方式对系统进行远程管理，能否防止鉴别信息在网络传输过程中被窃听;	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;	采用HTTPS加密传输方式	符合情况：采用安全加密协议进行传输。 不符合情况：未采用安全加密协议无法保证数据在传输过程中的完整性。
	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	中间件是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别;	1)应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别; 2)应核查其中一种鉴别技术是否使用密码技术来实现。	1)采用双因子认证（短信验证码不算） 2)其中一种必须要有密码技术，并记录采用何种算法（如Google Authenticator 动态口令使用OTP-HMAC密码技术）	符合情况：采用双因子认证方式，并且其中一种有密码技术。 不符合情况：未采用双因子认证方式。
访问控制	a)应对登录的用户分配账户和权限	1)中间件是否对用户账户和权限进行相关设置; 2)是否限制默认账户的访问权限。	1)应核查是否为用户分配了账户和权限及相关设置情况; 2)应核查是否已禁用或限制匿名、默认账户的访问权限。	1)为管理员分配相应账户 2)为账户分配管理员所需的权限 3)禁用或限制匿名、默认账户的权限	符合情况：为管理员分配相应账户和所需的权限并且禁用或限制匿名、默认账户的权限。 不符合情况：未分配相应账户和权限，或者直接使用默认账户对设备进行管理。
	b)应重命名或删除默认账户，修改默认账户的默认口令	默认账户和默认口令是否已修改;	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。	1)默认账户已重命名或者删除默认账户 2)默认账户的默认口令已进行修改	符合情况：默认账户已重命名或者删除默认账户并且默认口令已进行修改。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	管理员和账户一一对应;	1)应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对应; 2)应测试验证多余的、过期的账户是否被删除或停用。	1)不存在多余或者无效的账户 2)一个管理员一个账户	符合情况：不存在多余或者无效的账户并且一个管理员一个账户不存在共享账户。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	账户进行权限划分;	1)应核查是否进行角色划分; 2)应核查管理用户的权限是否已进行分离; 3)应核查管理用户权限是否为其工作任务所需的最小权限。	1)账户角色进行划分 2)账户权限进行三权分立 3)账户所需的权限为工作所需最小权限	符合情况：账户角色进行划分，部署三权分立，分配账户所需的权限为工作所需最小权限。 不符合情况：未划分相应账户的权限。
	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	1)应核查是否由授权主体（如管理用户）负责配置访问控制策略; 2)应核查授权主体是否依据安全策略配置了主体对客体的访问规则; 3)应测试验证用户是否有可越权访问情形。	1)ls -l /etc/passwd（记录不同账户下的该文件夹权限） 2)ls -l /etc/shadow 3)ls -l/etc/profile	1)管理用户负责配置访问控制策略，管理用户为账户分配不同的角色，每个角色分配不同的功能权限，当账户与角色关联时，该账户就具备与角色相关联的功能操作 2)非管理用户不能访问权限管理相关的功能	符合情况：配置访问控制策略，非管理用户不能访问权限管理相关的功能。 不符合情况：未配置访问控制策略。

	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	主体和客体的访问控制策略；	应核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级；	访问控制策略的控制粒度主体为登录账户，客体为功能权限以及功能权限关联的数据库表	符合情况：配置访问控制策略，控制粒度主体达到用户级或进程级，客体为功能权限以及功能权限关联的数据库表。 不符合情况：未配置访问控制策略，不存在控制主客体粒度。
	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	1)应核查是否对主体、客体设置了安全标记； 2)应测试验证是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。	getenforce （查看当前selinux运行状态--Enforcing强制、Permissive宽容、Disabled关闭）	1)安全策略对重要账户和重要信息设置了安全标记 2)安全标记控制了账户对有安全标记信息资源的访问	符合情况：依据安全策略对重要账户和重要信息设置了安全标记。 不符合情况：重要账户和重要信息未设置安全标记。
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	1)应核查是否开启了安全审计功能； 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。	在IIS中点击站点->双击日志，查看是否启用W3C日志。	1)启用了安全审计功能。建立了日志审计模块。 2)安全审计范围覆盖每个用户 3)对重要的用户行为和重要安全事件提供了审计	符合情况：启用了安全审计功能。建立了日志审计模块，安全审计范围覆盖到每个用户，对重要的用户行为和重要安全事件提供了审计。 不符合情况：未开启安全审计功能，不存在日志审计模块，无法对重要的用户行为和重要安全事件提供审计。
	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；	打开日志，查看日志包括日期、时间、浏览器信息、IP地址、端口等。	审计记录至少包括事件日期，时间，发起者信息(如用户名、IP地址等)、类型、描述和结果(是否成功等)等内容	符合情况：启用了安全审计功能。建立了日志审计模块，审计记录至少包括事件日期，时间，发起者信息(如用户名、IP地址等)、类型、描述和结果(是否成功等)等内容。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计记录。
	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	1)应核查是否采取了保护措施对审计记录进行保护； 2)应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。	1)查看日志在本地保存的周期和权限。查看日志轮转周期；查看日志的权限，确保操作系统普通用户无删除、修改权限。 2)查看日志是否进行异地备份，保存周期，查看操作系统中是否发送日志到备份系统、日志审计系统；若操作系统为虚拟机，查看是否通过创建快照的方式对日志进行保护。	1)日志本地存储，可查看存储目录，周期和相关策略等 2)日志无法被删除和篡改	符合情况：启用了安全审计功能。建立了日志审计模块，日志无法被删除和篡改，日志信息保存6个月以上。对日志信息进行定期备份策略。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计记录。
	d)应对审计进程进行保护，防止未经授权的中断	通过非审计管理员的其他账户能否中断审计进程，验证审计进程是否受到保护；	IIS的审计进程受到Windows操作系统保护。 检查方法：使用操作系统普通用户中断审计进程，查看是否成功。	非授权不能中断审计进程或关闭审计功能	符合情况：启用了安全审计功能。建立了日志审计模块，非授权不能中断审计进程或关闭审计功能。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计进程。
入侵防范	a)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),从而影响系统的正常使用甚至危害系统的安全	1)应核查设计文档的内容是否包括数据有效性检验功能的内容； 2)应测试验证是否对人机接口或通信接口输入的内容进行有效性检验	应具备软件容错能力，提供对输入数据的长度、格式等进行检查和验证的功能，通过限制特定关键字的输入等防护措施防止SQL注入等攻击	符合情况：系统具备软件容错能力，提供对输入数据的长度、格式等进行检查和验证的功能，通过限制特定关键字的输入等防护措施防止SQL注入等攻击。 不符合情况：系统不具备软件容错能力。
	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	攻击者可能利用中间件存在的安全漏洞进行攻击，应对中间件漏洞扫描，及时发现存在的已知漏洞，并在经过充分测试评估后更新补丁，.避免遭受漏洞带的风险	1)应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞； 2)应核查是否在经过充分测试评估后及时修补漏洞	1)中间件经过漏洞扫描或者渗透测试后不存在高风险漏洞，若存在，则经过充分测试评估后及时修补漏洞 2)放弃扫描情况下，客户自身定期进行漏扫或者安全评估等	符合情况：经过漏洞扫描或者渗透测试后不存在高风险漏洞，若存在，则经过充分测试评估后及时修补漏洞。放弃扫描情况下，客户自身定期进行漏扫或者安全评估等。 不符合情况：客户自身未定期进行漏扫或者安全评估。经过漏洞扫描或者渗透测试之后存在相应风险的漏洞信息。

数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1）应核查设计文档，重要审计数据、重要配置数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性; 2）应测试验证在传输过程中对重要审计数据、重要配置数据和重要个人信息等进行篡改,查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。	1)通过HTTPS方式保证鉴别数据、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在传输过程中的完整性 2)HTTPS协议中TSL/SSL版本为1.2以上	符合情况：通过HTTPS方式保证鉴别数据、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在传输过程中的完整性，HTTPS协议中TSL/SSL版本为1.2以上。 不符合情况：未配置HTTPS方式无法保证鉴别数据、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在传输过程中的完整性。
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)应核查设计文档，是否采用了校验技术或密码技术保证鉴别数据、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在存储过程中的完整性; 2)应核查是否采用技术措施保证鉴别数据、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在存储过程中的完整性; 3)应测试验证在存储过程中对鉴别数据、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等进行篡改，是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。	1)采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性 2)可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合情况：系统采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性。 不符合情况：系统未采用校验技术或密码技术无法保证鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性。
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)应核查设计文档，重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性; 2)应通过嗅探等方式抓取传输过程中的数据包,查看重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。	1)通过HTTPS方式保证鉴别数据、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在传输过程中的保密性 2)HTTPS协议中TSL/SSL版本为1.2以上	符合情况：通过HTTPS方式保证鉴别数据、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在传输过程中的保密性，HTTPS协议中TSL/SSL版本为1.2以上。 不符合情况：未配置HTTPS方式无法保证鉴别数据、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在传输过程中的保密性。
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1）应核查是否采用密码技术保证重要业务数据和重要个人信息等在存储过程中的保密性; 2）应核查是否采用技术措施（如数据安全保护系统等）保证重要业务数据和重要个人信息等在存储过程中的保密性; 3）应测试验证是否对指定的数据进行加密处理。	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合情况：系统采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的保密性。 不符合情况：系统未采用校验技术或密码技术无法保证鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的保密性。
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	要求用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户)	应核查相关配置信息或系统设计文档，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除	中间件采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进行及时清理。
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	要求用户的敏感数据所在的存储空间(如硬盘清除后才能分配给其他用户)	应核查相关配置信息或系统设计文档，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除	中间件采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进行及时清理。

数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1） 系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2） 系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2） 通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；

剩余信息保护	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除;
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能; 部分符合：无部分符合 不符合：系统采集信息非业务必要;
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用; 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露;

安全计算环境-中间件（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
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	1)应核查用户在登录时是否采用了身份鉴别措施; 2)应核查用户列表确认用户身份标识是否具有唯一性; 3)应核查用户配置信息或测试验证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)cat /login.defs (查看口令可用天数、修改口令间隔天数、口令最小长度) 2)cat /etc/security/pwquality.conf (查看口令复杂度)	1)身份标识具有唯一性 2)采取身份鉴别措施（如通过用户名加口令方式进行身份鉴别） 3)当前口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换（更换周期3个月以内） 4)强制口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换（更换周期3个月以内）	符合情况：需同时保证身份标识唯一性、存在身份鉴别措施、口令复杂度达到8位以上，至少三种字符类型组成，并且定期更换、更换口令时校验口令复杂度达到8位以上，至少三种字符类型组成。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	1)应核查是否配置并启用了登录失败处理功能; 2)应核查是否配置并启用了限制非法登录功能，非法登录达到一定次数后采取特定动作，如账户锁定等; 3)应核查是否配置并启用了登录连接超时及自动退出功能。	1)cat /pam.d/system-auth (查看登陆失败处理次数和限制时间) 2)cat /etc/profile | grep TMOUT (查看登陆超时自动退出策略--本地) 3)cat /etc/ssh/sshd_config | grep Client（查看登陆超时自动退出策略--通过ssh链接的登录）	1)启用登录失败功能，登录失败X（不超过10）次，锁定账户X（不超过60）分钟 2)启用登录超时策略，登录超时X（30分钟以内）分钟自动退出	符合情况：启用登录失败功能和登录连接超时策略。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	中间件是否采用加密等安全方式对系统进行远程管理，能否防止鉴别信息在网络传输过程中被窃听;	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;	采用HTTPS加密传输方式	符合情况：采用安全加密协议进行传输。 不符合情况：未采用安全加密协议无法保证数据在传输过程中的完整性。
	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	中间件是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别;	1)应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别; 2)应核查其中一种鉴别技术是否使用密码技术来实现。	1)采用双因子认证（短信验证码不算） 2)其中一种必须要有密码技术，并记录采用何种算法（如Google Authenticator 动态口令使用OTP-HMAC密码技术）	符合情况：采用双因子认证方式，并且其中一种有密码技术。 不符合情况：未采用双因子认证方式。
访问控制	a)应对登录的用户分配账户和权限	1)中间件是否对用户账户和权限进行相关设置; 2)是否限制默认账户的访问权限。	1)应核查是否为用户分配了账户和权限及相关设置情况; 2)应核查是否已禁用或限制匿名、默认账户的访问权限。	1)为管理员分配相应账户 2)为账户分配管理员所需的权限 3)禁用或限制匿名、默认账户的权限	符合情况：为管理员分配相应账户和所需的权限并且禁用或限制匿名、默认账户的权限。 不符合情况：未分配相应账户和权限，或者直接使用默认账户对设备进行管理。
	b)应重命名或删除默认账户，修改默认账户的默认口令	默认账户和默认口令是否已修改;	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。	1)默认账户已重命名或者删除默认账户 2)默认账户的默认口令已进行修改	符合情况：默认账户已重命名或者删除默认账户并且默认口令已进行修改。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	管理员和账户一一对应;	1)应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对应; 2)应测试验证多余的、过期的账户是否被删除或停用。	1)不存在多余或者无效的账户 2)一个管理员一个账户	符合情况：不存在多余或者无效的账户并且一个管理员一个账户不存在共享账户。 部分符合情况：至少满足以上一点，但未全部满足。 不符合情况：未符合以上所有情况。
	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	账户进行权限划分;	1)应核查是否进行角色划分; 2)应核查管理用户的权限是否已进行分离; 3)应核查管理用户权限是否为其工作任务所需的最小权限。	1)账户角色进行划分 2)账户权限进行三权分立 3)账户所需的权限为工作所需最小权限	符合情况：账户角色进行划分，部署三权分立，分配账户所需的权限为工作所需最小权限。 不符合情况：未划分相应账户的权限。
	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	1)应核查是否由授权主体（如管理用户）负责配置访问控制策略; 2)应核查授权主体是否依据安全策略配置了主体对客体的访问规则; 3)应测试验证用户是否有可越权访问情形。	1)ls -l /etc/passwd（记录不同账户下的该文件夹权限） 2)ls -l /etc/shadow 3)ls -l/etc/profile	1)管理用户负责配置访问控制策略，管理用户为账户分配不同的角色，每个角色分配不同的功能权限，当账户与角色关联时，该账户就具备与角色相关联的功能操作 2)非管理用户不能访问权限管理相关的功能	符合情况：配置访问控制策略，非管理用户不能访问权限管理相关的功能。 不符合情况：未配置访问控制策略。

	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	主体和客体的访问控制策略；	应核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级；	访问控制策略的控制粒度主体为登录账户，客体为功能权限以及功能权限关联的数据库表	符合情况：配置访问控制策略，控制粒度主体达到用户级或进程级，客体为功能权限以及功能权限关联的数据库表。 不符合情况：未配置访问控制策略，不存在控制主客体粒度。
	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	1)应核查是否对主体、客体设置了安全标记； 2)应测试验证是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。	getenforce （查看当前selinux运行状态--Enforcing强制、Permissive宽容、Disabled关闭）	1)安全策略对重要账户和重要信息设置了安全标记 2)安全标记控制了账户对有安全标记信息资源的访问	符合情况：依据安全策略对重要账户和重要信息设置了安全标记。 不符合情况：重要账户和重要信息未设置安全标记。
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	1)应核查是否开启了安全审计功能； 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。	1)在Nginx的配置文件nginx.conf中查看是否开启error_log和access_log。 2)在Nginx安装目录中查看是否有：/logs/error_log和/logs/access_log。	1)启用了安全审计功能。建立了日志审计模块。 2)安全审计范围覆盖每个用户 3)对重要的用户行为和重要安全事件提供了审计	符合情况：启用了安全审计功能。建立了日志审计模块，安全审计范围覆盖到每个用户，对重要的用户行为和重要安全事件提供了审计。 不符合情况：未开启安全审计功能，不存在日志审计模块，无法对重要的用户行为和重要安全事件提供审计。
	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；	1)查看error_log文件记录内容，查看是否包括：错误发生的日期、时间、错误等级、IP地址、内容等。 2)查看access_log文件内容，查看是否包括：客户端连接的日期、时间、IP地址、状态代码、浏览器信息等。	审计记录至少包括事件日期，时间，发起者信息(如用户名、IP地址等)、类型、描述和结果(是否成功等)等内容	符合情况：启用了安全审计功能。建立了日志审计模块，审计记录至少包括事件日期，时间，发起者信息(如用户名、IP地址等)、类型、描述和结果(是否成功等)等内容。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计记录。
	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	1)应核查是否采取了保护措施对审计记录进行保护； 2)应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。	1)查看日志在本地保存的周期和权限。查看日志轮转周期；查看日志的权限，确保操作系统普通用户无删除、修改权限。 2)查看日志是否进行异地备份，保存周期，查看操作系统中是否发送日志到备份系统、日志审计系统；若操作系统为虚拟机，查看是否通过创建快照的方式对日志进行保护。	1)日志本地存储，可查看存储目录，周期和相关策略等 2)日志无法被删除和篡改	符合情况：启用了安全审计功能。建立了日志审计模块，日志无法被删除和篡改，日志信息保存6个月以上。对日志信息进行定期备份策略。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计记录。
	d)应对审计进程进行保护，防止未经授权的中断	通过非审计管理员的其他账户能否中断审计进程，验证审计进程是否受到保护；	Nginx审计进程与nginx服务相关联，无法单独中断。 检查方法：使用操作系统普通用户中断审计进程，查看是否成功。	非授权不能中断审计进程或关闭审计功能	符合情况：启用了安全审计功能。建立了日志审计模块，非授权不能中断审计进程或关闭审计功能。 不符合情况：未开启安全审计功能，不存在日志审计模块，不存在日志审计进程。
入侵防范	a)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),从而影响系统的正常使用甚至危害系统的安全	1)应核查设计文档的内容是否包括数据有效性检验功能的内容； 2)应测试验证是否对人机接口或通信接口输入的内容进行有效性检验	应具备软件容错能力，提供对输入数据的长度、格式等进行检查和验证的功能，通过限制特定关键字的输入等防护措施防止SQL注入等攻击	符合情况：系统具备软件容错能力，提供对输入数据的长度、格式等进行检查和验证的功能，通过限制特定关键字的输入等防护措施防止SQL注入等攻击。 不符合情况：系统不具备软件容错能力。
	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	攻击者可能利用中间件存在的安全漏洞进行攻击，应对中间件漏洞扫描，及时发现存在的已知漏洞，并在经过充分测试评估后更新补丁，.避免遭受漏洞带的风险	1)应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞； 2)应核查是否在经过充分测试评估后及时修补漏洞	1)中间件经过漏洞扫描或者渗透测试后不存在高风险漏洞，若存在，则经过充分测试评估后及时修补漏洞 2)放弃扫描情况下，客户自身定期进行漏扫或者安全评估等	符合情况：经过漏洞扫描或者渗透测试后不存在高风险漏洞，若存在，则经过充分测试评估后及时修补漏洞。放弃扫描情况下，客户自身定期进行漏扫或者安全评估等。 不符合情况：客户自身未定期进行漏扫或者安全评估。经过漏洞扫描或者渗透测试之后存在相应风险的漏洞信息。

数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1）应核查设计文档，重要审计数据、重要配置数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性; 2）应测试验证在传输过程中对重要审计数据、重要配置数据和重要个人信息等进行篡改,查看是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。	1)通过HTTPS方式保证鉴别数据、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在传输过程中的完整性 2)HTTPS协议中TSL/SSL版本为1.2以上	符合情况：通过HTTPS方式保证鉴别数据、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在传输过程中的完整性，HTTPS协议中TSL/SSL版本为1.2以上。 不符合情况：未配置HTTPS方式无法保证鉴别数据、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在传输过程中的完整性。
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)应核查设计文档，是否采用了校验技术或密码技术保证鉴别数据、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在存储过程中的完整性; 2)应核查是否采用技术措施保证鉴别数据、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在存储过程中的完整性; 3)应测试验证在存储过程中对鉴别数据、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等进行篡改，是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。	1)采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性 2)可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合情况：系统采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性。 不符合情况：系统未采用校验技术或密码技术无法保证鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的完整性。
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)应核查设计文档，重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性; 2)应通过嗅探等方式抓取传输过程中的数据包,查看重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。	1)通过HTTPS方式保证鉴别数据、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在传输过程中的保密性 2)HTTPS协议中TSL/SSL版本为1.2以上	符合情况：通过HTTPS方式保证鉴别数据、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在传输过程中的保密性，HTTPS协议中TSL/SSL版本为1.2以上。 不符合情况：未配置HTTPS方式无法保证鉴别数据、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在传输过程中的保密性。
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1）应核查是否采用密码技术保证重要业务数据和重要个人信息等在存储过程中的保密性; 2）应核查是否采用技术措施（如数据安全保护系统等）保证重要业务数据和重要个人信息等在存储过程中的保密性; 3）应测试验证是否对指定的数据进行加密处理。	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合情况：系统采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的保密性。 不符合情况：系统未采用校验技术或密码技术无法保证鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等在存储过程中的保密性。
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	要求用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户)	应核查相关配置信息或系统设计文档，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除	中间件采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进行及时清理。
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	要求用户的敏感数据所在的存储空间(如硬盘清除后才能分配给其他用户)	应核查相关配置信息或系统设计文档，敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除	中间件采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合情况：采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除系统中的剩余信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等。 不符合情况：未对剩余信息进行及时清理。

数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1） 系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2） 系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2） 通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；
数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份； 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份；
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份， 部分符合：无部分符合 不符合：未提供异地实施备份功能；
	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除； 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除；

剩余信息保护	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除;
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能; 部分符合：无部分符合 不符合：系统采集信息非业务必要;
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用; 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露;

安全计算环境-应用（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	预期结果
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、 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在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该系统的鉴别数据、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在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、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进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1） 系统提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2） 系统检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合：系统通过https协议对传输过程中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统采取措施对传输中的数据进行完整性校验；仅包括业务数据。 不符合：系统未采取措施对传输中的数据进行完整性校验；
	b） 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	本条款要求对鉴别数据、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在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问系统管理员，是否采用校验技术或密码技术保证鉴别数据、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在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、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，查看系统反应	1)系统采用校验技术或密码技术保证了鉴别数据、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在存储过程中的完整性 2)系统可检测到存储在数据库中的鉴别数据、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被修改的行为，并具备恢复措施	符合：系统通过MD5技术对存储中的数据进行完整性校验；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过MD5技术对存储中的数据进行完整性校验；仅对鉴别数据，未包括业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行完整性校验；
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	本条款要求对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2） 通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)系统管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2） 通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过https协议对传输过程中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对传输中的数据进行加密；
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	本条款要求对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询间系统管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据、业务数据和个人信息。 部分符合：系统通过sha256对存储中的数据进行加密；包括鉴别数据，未对业务数据和个人信息。 不符合：系统未采取措施对存储中的数据进行加密；

数据备份和恢复	a)应提供重要数据的本地数据备份与恢复功能	对数据进行备份，是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式和形式等，保证系统重要数据在发生破坏后能够恢复。本条款要求对应用系统的重要数据提供本地数据备份与恢复功能	1)询问数据库管理员，数据库的备份和恢复策略是什么 2)核查备份策略设置是否合理，配置是否则正确 3)核查备份结果是否与备份策略一致 4)核查近期恢复测试记录，查看是否能够进行正常的数据恢复	1)提供数据的每天全量备份《(或每天增量备份，定期全量备份) 2)近期数据库的恢复测试记录显示，能够使用备份文件进行数据恢复	符合：系统通过快照形式对应用程序进行备份，备份策略为每周2，4，6进行备份，备份保存7天，数据每天凌晨1：00全量备份; 部分符合：提供数据备份能力、未提供数据恢复功能。 不符合：系统未对应用程序及数据进行备份;
	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(如火灾)不可恢复时,利用异地保存的数据对系统数据能进行恢复	询问数据库管理员，是否提供异地实时备份功能，并通过网络将重要配置数据，重要业务数据实时备份至备份场地	提供异地实时备份功能，并通过网络将重要配置数据、重要业务数据实时备份至备份场地	符合：系统每周对应用程序及数据进行异地备份, 部分符合：无部分符合 不符合：未提供异地实施备份功能;
剩余信息保护	a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统将用户的鉴别信息所在的存储空间(如硬盘清除后才能分配给其他用户），例如:有的应用系统将用户的鉴别借息放在内存中进行处理，处理完成后没有及时清除等，这样其他的用户通过一些非正常手段就有可能获取该用户的鉴别信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信息	应用系统采取措施保证对存储介质(如硬盘或内存)中的用户鉴别信息进行及时清除。如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证鉴别信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证鉴别信息存储空间被释放后得到完全清除;
	b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除	本条款要求应用系统应将敏感数据所在的存储空间(如硬盘或内存)清除后才能分配给其他用户，例如:有的应用系统在使用过程中可能会产生-些临时文件，这些临时文件中可能会记录一些敏感信息，当将这些资源分配给其他用户时，其他用户就有可能获取这些敏感信息	询问系统管理员，应用系统是否采取措施保证对存储介质(如硬盘或内存)中的敏感数据进行及时清除，防止其他用户非授权获取敏感数据	应用系统采取了措施保证对存储介质(如硬盘或内存入中的敏感数据进行及时清除，如系统会对存储或调用过鉴别信息的函数或变量及时写零或置空，及时清除B/S系统中的Session和Cookie信息，以及对存有用户鉴别信息的临时文件进行删除或内容清除等	符合：采取措施保证敏感信息存储空间被释放后得到完全清除; 部分符合：无部分符合 不符合：未采取措施保证敏感信息存储空间被释放后得到完全清除;
个人信息保护	a)应仅采集和保存业务必需的用户个人信息	条款是为保护个人信息，不采集业务不需要的个人数据	1)询问系统管理员,该系统采集了用户的哪些个人信息 2)询问系统管理员,系统中采集的用户个人信息是否是业务应用必需的	1）记录系统所采集的个人信息。如系统采集了用户身份证号、电话等个人 信息 2)记录应用系统哪个功能模块使用哪些用户个人信息，以及所使用个人信息的必要性	符合：系统仅采集用户姓名，电话，用于XXX,XXX功能; 部分符合：无部分符合 不符合：系统采集信息非业务必要;
	b)应禁止未授权访问和非法使用用户个人信息	本条款要求应用系统应采取措施，禁止未授权访问和非法使用个人信息，从而保护个人信息	1)询问系统管理员，哪些系统账户可以访问个人信息，且系统采取了什么措施控制可访问个人信息的系统账户对个人信息的访问 2)核查相关措施是否有效的限制了相关账户对个人信息的访问和使用	1)系统采取了措施控制了系统账户对个人信息的访问，如权限控制等 2)未授权无法访问和使用用户的个人信息	符合：系统对个人信息显示界面进行了脱敏处理，防止个人信息的非法使用; 部分符合：无部分符合 不符合：系统未对个人信息进行处理，可直接在系统界面中查看到，且相关人员未签署保密协议，防止个人信息泄露;