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
	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 哪一种的登克方式,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 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 。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。	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 信,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 覆、看用户身份标识是否具有唯一性、核查是否	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 效一次	符合情况:通过用户名口令方式杂度。 符合情况:通过用户名口令专数字。 多大支期为90天: 口令行答情况:通过用户名口令方实度, 可令分符合情况:通过用户名口令分符合情况:通过用户名户。 多字。 一个分子录;字母,数据: 一个大量的一个大量的一个大量的一个大量的一个大量的一个大量的一个大量的一个大量的
身份鉴别	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,设置管理员展大登录失败次数, 一旦该管理员的登录失败次数相可设定数值,系统称 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	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	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)还置并启用了远程登录连接租时并自动退出功能。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: 巴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5次锁定现的,连续登录失败5次锁时自动退力能,连续登录失败5次锁时自动退出措施; 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、HTTPBS等加密协议等方式进行交互式管理	ஐ等班 技术添过WED用态等项目不知添过	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。
	种或两种以上组合的鉴别技术对用户进	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。些鉴别信息,还需要访问者各有鉴别特征,例如采用令原、智能卡等目前主流。集地内鉴别下述证的方式进证的方式进行认证。不过一个专证书认证"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 行两种或两种以上组合的鉴别技术,点击该用户 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。20度1省中于负权限。20成4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	便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 6) 的具体高级。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——对应。 2)如果因为本种原因导致类些多余的、过期的账户 元法被删除,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——对应,是实现共享账户的情况:管理员用户与账户之间——对应,未发现共享账户的情况。但4、5°为多余账户(但4、7000分余账户(万000分分分分分分分分分分分分分分分分分分分分分分分分分分分分分分分分分分
	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。 则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 可以应置安全策略,审计管理项可以与看日志。 可以应置安全策略,审计管理项可以查看日志。 可以在置安全策略,可以查看日志的工程, 可以应数据的最小权限,如禁止对管理用户的权限。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。	部分付合情况,已配置女主官理员S* 、系统管理员S*,但未配置审计管理员;
	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		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; 访问控制力度为功能模块; 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, 据之它表示主客体的安全级别。敏感形记由安全管理 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。	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	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。	
	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。 使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、FIP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		进入管理界面。然后在左侧导航树中选择日志审 计右侧显示各类器,并进入日志源配置界面,查看 爱果日志服务器,并进入日志源配置界面,查看 经机的P。 在日志服务器上,根据P地址选择全机后,便 可对该堡垒机的日志进行核查。确以是否包括 期和时间、用户、事件类型、事件是否成功等相 关的偏息	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:仅有用户信息、登录时间。
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	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P。 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: 已对审时计记录记录进进行保护,审计记录实时传输至止能够进免策争性的上,能够避免受到未预期的删除、修改或覆盖部分符合情况: 已对审计记录记录已报告计设备,并不是有计设备,每十亿年计记事计记录记录日本法等的变级覆盖,然符合情况: 未对审计记录记录记录记录记录记录记录记录记录记录记录记录记录记录记录记录记录记录记录

	d)应对审计进程进行保护,防止未经授权的中断	保护好审计进程, 当安全事件发生时能够及时记录事件发生的详细内容	应测试通过非审计员的其他账户来中断审计进程,验证审计进程是否受到保护	非审计员的其他账户来不能中断审计进程,验 证审计进程是否得到保护	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
	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 像全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地址进范 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。
入侵防范	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		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:定期进行扫描,担 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案。 (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。	此項不适合,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、系统程序、重要配置参数和应用程序的关键执行可信验证、并在应用程序的关键执行环节进行动态可信验证。在传统中,并不可能是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	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:安装引导性。 安装等进程 " 一
松 枯 凸 數 林	据在传输过程中的完整性,包括但不限 干鉴别数据、重要业务数据、重要审计	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,当检测到传 银的完整性通知破坏时应采取恢复指动数据进行恢复。本条款要求对鉴别数据、重要业务数据、重要审计数据、重要配置数据重要规频数据和重要入信息 付数据、重要配置数据重要规频数据和重要入到信息 在传输过程中的完整性进行检测,并在重测到完整性 受到破坏时采取恢复措施,如重传或其它方式	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	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呆 人信息等在传输过程中的完整性受到被坏后呆	信息。 部分符合:系统采取措施对传输

I was the term was our					
	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 排不。证要配置数据、重要观频数据和重要个人信息在 存值要中的灾整性进行检测,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、重要中分数据、重要审计数据、重要审计数据、重要审计数据,重要的完整性。2)尝试修改存储在数据库中的鉴别数据,重要业数据、重要视置数据、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、重要现频数据和重要个人信息等在存储过程中的完整性。 要业务数据、重要审计数据、重要配置数据、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		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 到或嗅媒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		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;
		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)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sha255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 款要来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 沒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—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价、备份策略为每周2,4,6进行备价、备份策略为每周2,4,6进行备价、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		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	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		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多级形态,不成分系统中的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:无彩取措施保证鉴别信息存储空间被释放后得到完全清除;
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 阴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—些鲸信息。 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级对的 零或置空、及时清除7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	部分符合:
	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	 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 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	北江佐田人 1 佐白 川 五 旧 拉 人 1 佐白	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	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;
------------	---------------------------	---------------------------	--	-------------------------------------	--

				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
	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	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。 防火墙不分许配置用户名相同的用户。同时要	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。	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	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
身份鉴别	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,设置管理员成登录失败次数,一旦该管理员的登录失数数过设定数值,系统将对其进行登录失败定,从而防止非法用户通过暴力破解的方式登录到防火墙	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	选下 同級病任 在例的支延性, 可以宣有到 取入豆果 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	能,连续登录失败5次顿定账户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
	必要措施、防止鉴别信息在网	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。
	的鉴别技术对用户进行身份鉴	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	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	,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。

	a)应对登录的用户分配账户和 权限	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	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	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——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:管理员用户与账户的情况:管理员用户与账户的情况,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。
访问控制	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、安全管理员和计管理员三类,其中,安全管理员可以制定安全策略,第计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	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;
	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。
		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	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	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,	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,	防火牆设置正确的服务器地址、端口、以及日志级别	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PP。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P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。 受录日志服务器,并选择管理策略》日志收集源,进入日志源图界面,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库进行备份操作,便可实现防火墙数路各份和保护。在日志服务据上,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",确保存在一类型为"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:已对审计记录进行审计记录进行审计记录实际传输至年的电话的重点 并强有的 删除、修改或覆盖,并留存的,一个不够或覆盖,分符合情况:已录实时传输至录记录记录记录记录记录记录记录记录记录记录记录记录记录记录记录记录记录记录记
	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。
	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	国动物业组	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。
入侵防范	能, 保证通过人机接口输入或	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	在网络边界、 核心等重要节点处部署IDS. IPS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	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、系统程序、系统程序、配置参数和应用程序等进行信验证,并在应用程序的验证,并在应测到其行动态可信验证,在检测到其分解验证结果形成审计记录送至安全管理中心	以由应1.7.000以由以2.7.1以由约1寸	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	符片 然是 的

数据完整性	完整性,包括但不限于鉴别数 据、重要业务数据、重要审计	恢复措施对数据进行恢复。本条款要求对鉴别	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	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	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;
	的完整性,包括但不限于鉴别 数据、重要业务数据、重要审	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	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	。 部分符合:系统诵讨MD5技术对
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	平宗孙安水列金加致佑、里安业分致佑、和里 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		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	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		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 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:不符合:未提供异地实施备份功能;

剩全位		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(如使盘或内存)中的 用户鉴别信息进行及时清除。如系统会对存储或调用	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	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	中的敏感致描述行及的清除,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	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	2)询问系统管理员,系统中采集的用户个人信息是否	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	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:无部分符合:现款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
	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,用户客途,用户对的合法用户对的方式为通过对照户户户对的各式等。日志审计为了重要,但是不是一个,是一个,是一个,是一个,是一个,是一个,是一个,是一个,是一个,是一个,	市计的登录界面,提示用户输入用户名和密码。输入用户名和密码。接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码。 四年,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,测试用户身份核是是有更点,被	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	符合情况:通过用户名口令方式登录、
身份鉴别	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>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。

	两种或两种以上组合的鉴别技术对用户	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。
	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。	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。
访问控制	b)应重命名或删除默认账户,修改默认账户的默认口令	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:管理员用户与账户的情况:管理员用户与账户的自一一对应,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	1分 有利十各岗位细致协调工作 同时仅	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局和审计管理员权限。	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;
	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	定了主体可以对客体进行的操作,访问控制	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。

1		I	T	T	放入峡口,运运场制加则占领型型
	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	沙水,在 炒业小用厂沙水后芯。 沙冷点惊惧笑叹声摇扭声,体出气和黑,点视点之主体	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。
	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。
	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。在缺行,有情况下,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。
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	行状况和网络攻击行为, 因此需要对审计	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。 一个在服务器的,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,查看市的IP。收集到的日志源列表中包含了该日志市的IP。收集到的日志源组会保存在日志系统的数据库中,据的运分制度,这一个人,通过对数据库进行备份操作,便可实现日志审计数据的运动数据库进行备份操作,便可实现日志审计数据的运动。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。这些日志市计日志信息的目的。	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,能够遵复盖;部分符合情况:已对审计记录证录记录证行保护,审计记录证录时传输留存7天,修改合情况:未对审计记录记录形形除、修改合情况:未对审计记录记录进行保护,审计记录仅留存7天,修改合情况:未对审计记录记录进行保护,审计记录仅留存7天,修改查

	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	能性。及时更新系统补了, 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。		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) 应能友现当能仔住的巨为漏洞,并在	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。
	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
账意代码 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		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: 不有情况: 不有情况。
**-10 -> **-14	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、重要视频数据和重要个人信息等	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 报和重要人上信息在任验过程的信息数据	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	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	部分符号: \$3.\$\$\\\\$\\\\$\\\\$\\\\$\\\\$\\\\$\\\\$\\\\$\\\
数据完整性	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	重要审计数据、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	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	、重安代观数据和重安了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	。 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; 仅对奖别数据 未包括业务数据
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	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;

	储过程中的保密性,包括但不限于鉴别	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	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	复功能	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	2)核查备份策略设置是否合理,配置是否则正确	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,备份策略为每周5,46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;
	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	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		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拉处理。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	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	「簡空則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
	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	[八火(XI收血以门)[八山)蚁芯蚁炬处门久时,何你,例	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	随空间做样放冶特到元至清除, 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	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	信息	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	未授权访问和非法使用个人信息,从而保	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
		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。	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:	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,口令复路位以上,口令复度的位以上,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;部分写,面过用户名口令有效明,正是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个
身份鉴别	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如,设置管理员最大登录失败次数,一旦	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	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	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	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 双因子鉴别不仅要求访问者知道一些鉴别 宗用令牌、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"外部口的认证方式应该为"本地口令+证书认证"或者"外部口	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。
	a)应对登录的用户分配账户和权限	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	^{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	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: 巴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	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贮户列表,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; 管理员用户与账户的情况; 管理员用户与账户之间——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	1)应核查是否进行角色划分,审计、配置、管理、系	2)管理用户的权限进行了分离,并为其工作任务	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;

	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	定了主体可以对客体进行的操作。访问控	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。
	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	用尸旨理-用尸列衣,有侧亚小用尸列衣信息。 1) 本手具衣左宫人长\\\ 去声之伏和家伏\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	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。
	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	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。	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。
安全审计		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好备,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,确认是否包括日期可时间、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: 已对审计记录进行保护, 品对审计记录实时传输至日志审计记录实时传输至日的多数 并留存半年以上, 能改 選 盖; 部分符合情况: 已对审计记录记录记录记录记录计行保护, 审计记录实时传输至存7 法够避免 受到未预期的删除、修改够避免等价值况: 未对审计记录记录进行保护, 审计记录记录进行保护, 审计记录记录进入。不符合情况: 未对审计记录记录进行保护, 审计记录以明明,不行保护,审计记录以明明,

	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。
	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。
入侵防范	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供和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	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 器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。

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: 不有情况: 不有情况。
**-10 -> **-14	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、重要视频数据和重要个人信息等	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 报和重要人上信息在任验过程的信息数据	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	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	部分符号: \$3.\$\$\\\\$\\\\$\\\\$\\\\$\\\\$\\\\$\\\\$\\\\$\\\
数据完整性	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	重要审计数据、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	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	、重安代观数据和重安了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	。 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; 仅对奖别数据 未包括业务数据
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	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;

	储过程中的保密性,包括但不限于鉴别	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	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	复功能	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	2)核查备份策略设置是否合理,配置是否则正确	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,备份策略为每周5,46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;
	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	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		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拉处理。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	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	「簡空則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
	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	[八火(XI收血以门)[八山)蚁芯蚁炬处门久时,何你,例	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	随空间做样放冶特到元至清除, 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	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	信息	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	未授权访问和非法使用个人信息,从而保	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
	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系統的用户鉴别过程与其他UNIX系統相同:系统管理员为用户建立一个账户并为其指定一个口令用户使用指定的口今登录后重新配置自己的自己的口令。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、组标识等自意sword文件中的口令字段使用一个"火"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-auth里的设置为准,也就是说/etc/pam.d/system-auth区的运用程度认证用户。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 Centos和后处不是一个重要的文件使是etc/pam.d/system-auth(在kedhat Centos和后的不是一)。/etc/pam.d/system-auth《teckedhat Centos和Fedora系上)。/etc/pam.d/system-auth《teckedhat Centos和Fedora系上)。/etc/pam.d/system-auth《teckedhat Centos和Fedora系上)。/etc/pam.d/system-auth《teckedhat Centos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、	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。	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: 7ASS 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 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	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,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
身份鉴别	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,瞬锁时间等。 看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	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	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,但未设置登录组时锁定参数。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。因为其在教据传输过程中,账户与密码均明文传输,这是非常危险的。黑客通过一些网络对嗅探工是能够轻易地的窃取网络中明文传输的账户与密码,因此不建议通过Telnet的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	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 servicestatus-all grep running, 查看是否存在Telnet服 务	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,Telner默认不符合 2)通过抓包工具,截获信息为密文,无法读取,协 设为加密 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
		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		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	以有相应权限的另份总承进入UDUNIU,使用 15-1人件右 叩 - 本套重更文件和日景权限设置具不合理 加·#1。1	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 - r - r - : 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合理理设置,部分文件和目录权限设置不合理现资。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	/etc/shadow文件,查看文件中的用户,是否存在adm、		符合情况: 不存在默认的、无用的可登录账户,且已禁止foot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	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	2)各类管理员均使用自己分配的特定权限账户登	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: 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	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
访问控制	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
	级或进程级,客体为文件、数据库	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		,] 切凹控制束畸, 刈合尖义件和数据库衣级进行访问。	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
	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,实现强制访问注制。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。26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	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。 4 3)应测试是否依据主体、客体安全标记控制主体对客体访 间的强制访问控制策略	SELINUX有三种工作模式,分别是: f 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。	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
	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进程用来记录宏统中的各种信息,如硬件报管和软件日志。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	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	[root@localhost april]# service auditd status auditd (pid 1656) is running [root@localhost april]# service rsyslog status syslogd (pid 1681) is running	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
	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	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;	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都分符合情况: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	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	计记录进行存储,备份和保护。 2. 在 root 权限: Is - Ia /var/log/audit.d 3. 查看auditd服务的配置文件#cat /etc/audit/auditd.conf记录全部輸出,重点检查mum logs、max log file、mat log file action、disk full action、disk error action等字段。	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		访问权限是否设置合理。	3) 部署有第三方审计工具, 可实时记录审计日志,	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	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	则。 手工检查: 1)确认系统目前正在运行的服务: #servicestatus-all grep running,查看并确认是否已经 关闭危险的网络服务如cho、shell、login、finger、r态 今等。关闭非必需的网络服务如talk、ntalk、pop-2、 Sendmail、lmapd、Pop3d等。2)访谈补丁升级机制,查	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	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	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。	 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P对本机服务的访问。其中/etc/hosts.allow控制可以访问本机的P地址,/etc/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	请求;在/etc/hosts.allow中,是否有如下配置(举例):	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	限制等 部分符合情况:通过网路地址范围对终端接入方式
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	 立核查是否存在高风险漏洞,如漏洞扫描、渗透测试等; 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
	密的。妾雖扩系统女王,必侵威胁分外部渗透、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,入侵行为分为物理入侵、系统入侵和远程入侵三种。此成中,关注的操作系统所面对的入侵成协可能包含了三种造成入侵威的的人侵人情力主要是系统入侵加证在人侵两种。系统入侵,指入侵者还没有及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于程序,那么拥有低级限的用户就可能利用系统漏洞海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漏洞海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漏沟海环境、新闻和设计、计划、	1) が欧井皇有八皮極測的指加。 知 2 年 通过知 「 中 で 宣	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;	符合情况:具备入侵检测的措施,可以检测到对重要市点进行入侵的行为,并进行报警部分符合情况:具备入侵检测的措施,可以检测到对重要专选进行入侵的行为,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
	份,避免受到未预期的删除、修改或覆盖等 d)应对审计进程进行保护,防止未经授权的中断 a)应遵循最小安装的原则仅安装需要的组件和应用程序 b)应关闭不需要的系统服务、默认共享和高危端口 c)应通过设定终端接入方式或网络绝理终端进行限制 d)应进供数据有效性检验功能。信接口输入的内容符合系统设定要求 e)应能发现可能存在的已知,属阴,并在经过充分测试评估后,及时修补漏洞 f) 应能够检测到对重要节点,进导条件	C)应从用证证来进行体护。产物或覆盖等 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或覆盖等 成现人健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或覆盖等。 《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是目志守护进程保护好审计进程,当事件发生的,能够及时记录事件发生的详细内容。在Ubuntu操件系统时,应试循最小化安装原则,即不需要的各条的的变量性,当事件发生的,能够及时记录事件发生的详细内容。在安装Ubuntu操件系统时,应试循最小化安装原则,即不需要的包系统的安全性。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。 Ubuntu聚认安装时会开启许多不必要的系统服务,默认共享和高危端口是操作系统使用过程中,为了避免由于多余组件和应用程序。 Ubuntu聚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需求安全风险。通常可以将其关闭。通过查看监听端程序和的安全性。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。 Ubuntu聚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需要的通过发定终端接入方式或网络地是时间,通常更多处理,对比不是操作系统度和通过通行。 在Ubuntu系统中在在/ctc/hosts.allow和和/etc/hosts.deny两个文件。它的该经通进行限制。 D)应是供数据有效性检验功能,保证人类的证据,主要验证证或长度是多级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,则上个结份的表现有一个文件的配置并中央,以不是心态或是不要处于多级过入机接口的程序的界面的入次通过通信接口输入循环或长度是互构分系统设定要求,则上个别用产输入需形数提高可数系统出插如5cU注入攻击等,人而影响系统和正常使用甚至危害系统的安全。这就是对于不能是成为关键方式,是不是交别致非常系统中存在的已知漏洞,并在经过充分测试评估后,及时参加设在一个设施的上级,是有是不是不是一个关键,并不是是一个不会更多处,是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	计正是进行保护、验明保护。	□が共産計画を表示性態。 変数 の、重要を実示機能的制度、更な の、重要を実示機能的制度、更な の、重要を実示機能的制度、更な の、企業が非常に表示性の重要を使用、重要を使用、重要を対す機能的機能を改 に重要を使用して表示性の関する。 に関する。 のには、ののでは、では、では、では、では、では、では、では、では、では、では、では、では、で

		I			1
恶意代码防范		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台期是否超过一 个星期: 访谈管理员并查看实时检测与查条责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。	恶意代码的统-管理个	符合情况:系统中已安装部署防病毒软件,可对病毒人侵进行及时阻断,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变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、重要配置并在 原本原序等进行可信验证。 和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,并验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攻行为能被发现,并报警便于后续的处置动作		1) 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	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
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、重要配置数据、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	完整性	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	个人信息。 部分符合:系统采取措施对传输中的数据进行 宗整性校验:仅包括业务数据
		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	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		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,那成传输过程中的数据,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	部分符合:系统通过https协议对传输过程中的
XXIV.III		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	2000年安里方数2007年安	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)核查证期恢复测试记录,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) 完全量备份) 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	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		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	(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信	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,以及对存用户鉴别信息的临时文件进行删除或内容清除等	部分符合:无部分符合
初示旧心体扩	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	间间系统管理页,应用系统定台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	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。 好清除B/S系统中的Session和Cookie信息,以及对 存用户鉴别信息的临时文件进行删除或内容清除 等	后得到完全清除; 部分符合 无部分符合
	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	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	身份证号、电话等个人信息	NG: 不知以来来用户姓石, 电记, 用了 XXXXXXX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	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	0.1 控权工法分词和使用用点的人工信息	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
	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系或統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。ett/password文件中记录用户的属性信息。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"来"代替,将/etc/security/password文件是不能被普通用户读取的,只有超级用户才有戏课的,是一个被一次有数通用户读取的,只有超级用户才有效课的。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、检查并记录床放文件的配置,记录主机信任关系。 #find / -name .nestro 对.netro文件进行检查 #find / -name .nestro 对.netro文件进行检查 #find / -name .nestro 对.netro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中所有密码位不为空,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口令中最少包含字母字符个数 loginetries 连续登录失败后锁定用户 4、检查系统账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可令。 专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/passwd #cat /etc/passwd #cat /etc/passwd #cat /etc/passwd #cat /etc/group 查看UD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、检查系统账号奇类失败处理策略	1、不存在信任关系或存在细粒度控制的信任关系; 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,并已设置口令复录度要求。且当前口令符合口令复杂度要求,并定期更执口令。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,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
身份鉴别	置并启用结束会话、限制非法登录	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。	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	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, 且设置登录据时锁定参数 部分符合情况: 已配置登录失败处理功能相关参数, 的工作工作。 部次符合情况: 已配置登录失败处理功能相关参数, 但未设置登录集员 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, 未设置登录经时锁定参数, 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	录时使用SSH协议。其原理跟Telnet类似,只是其具	telnet, ftp,ssh,VNC 等。 执行: #ps -ef 查看开启的远程管理服务进程 执行: #nestat -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。	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	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士术等两种或两种以上组合的鉴别,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		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		重点查看以下文件和目录权限是否设置合理。 —rwx	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roat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、过期的贮户; 别宁 方面,也会出现多个系统管理员或用户使用同一 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 有用其进行非线件的风险,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
访问控制	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,避免现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
		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:访问控制的故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目开下生成的记,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	3、 位皇本が申り別形定台介启 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:	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
	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	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
	份,避免受到未预期的删除、修改	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: Is -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 # Is 查看申口文件的权限或访问控制是否合理 例如 Is -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。无对审计进行进行保护,非授权人员可申断审计进程、可随意对审计日志进行更改、删除等操作

			1 - 松木場佐茗公旦不正百フトルタエ子的叩々		
	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操件系统时,应试循最小化安装原则,即不需要的包不进行安装。安装的包越多,面临的风险起大,系统瘦身有利于提高系统的安全性。在操作系统使用过程中,为了避象由于多余组件和应用程序带来的安全风险。通常遵循最小安装原则,仅安装需要的组件和应用程序	1、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.conflgrep -v "#"记录系统开启的服务 #more /etc/rc.rfs #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 -a1 s. 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	执行以下命令: netstat –an	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: 已关闭多余端口, 他的服务和进程, 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 经端进行限制	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	#cat hosts dony	2、对终端接入力式、网络地址范围寺条件进	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制等的符合情况: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5QL 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	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离种。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	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.</daemonname>	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DS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 部份符合情况:具备入侵的行为,相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/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/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	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	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	1) 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	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
	括但不限于鉴别数据、重要业务数	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 性遭到破坏的定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 进行检测。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,重要被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 数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	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	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	包括但不限于鉴别数据、重要业务	中的完整性进行检测,并在检测到完整性受到破坏时采取	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。重要规频数据和重要个人信息等在存储过程中的完整性 2.完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	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	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
数据保密性		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)通过现保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	数据和重要个人信息进行了保密性处理	部分符合:系统通过https协议对传输过程中的
		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;包括鉴别数据,未对业务数据和个人信息。
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	2)核查备份策略设置是否合理,配置是否则正确	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, 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)中的用户鉴别信息地进行及时清除。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IS/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
初水 信态体护	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	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	加付到元主用陈, 如从佐人·工如从佐人
	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	 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: 使用个人信息,从而保护个人信息	ti 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: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		
	a)应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定期更换	Linux系或統的用户鉴别过程与其他UNIX系統相同:系统管理员为用户建立一个账户并为其指定一个口令用户使用指定的口今登录后重新配置自己的自己的口令。这样用户就具备一个私有口令。ett/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"米宋代替,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,又有超级用户才有权读取。Linux中的经记/ogin.des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型的设置为件,也就是说/etc/pam.d/system-auth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的配置优先级高于/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。	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 着/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	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 #登录密码量短修改时间,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	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,或口令未定期更换不符合口令复杂度要求,或口令不符合情况:存在空口令或弱口令账户、可绕过身份鉴别措施进行登录		
身份鉴别	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、起时时间,瞬锁时间等。 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	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	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。因为其在教据传输过程中,账户与密码均明文传输,这是非常危险的。黑客通过一些网络对嗅探工是能够轻易地的窃取网络中明文传输的账户与密码,因此不建议通过Telnet协议帮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)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 Telnat 方式进行远程管理 servicestatus-all grep running,查看是否存在Telnet服务	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		
		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		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		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 数字表示为744 - rwr-w-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., gopthor tp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		

	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、10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	2)各类管理员均使用自己分配的特定权限账户登	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	是否实现管理用户的权限分离	o) 禁用 只 把 四 /0 /1 和	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
访问控制	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投权工作,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 不用户或某个进程,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"Is -1文件名"命令,查看重要文件和目录权限设置是否合理、如:#Is -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	部分符合情况: 由管理用户进行用户访问权限分配
	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(读一写、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		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。	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待语况: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	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syslog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 -eflgrep 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 例以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	[root@localhost april]# service auditd status auditd (pid 1656) is running	符合情况:已开启安全审计功能,且审计覆盖到每
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	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	100ddy , X 1 , 63 <u>H</u> X II 11 11 109, X II	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 总部分符合情况: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。		3) 部署有第三方审计工具, 可实时记录审计日志,	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:无 不符合情况:未对审计进行进行保护,非授权人员可书审计进程,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	在安装Linux操件系统时,应试循最小化安装原则,即不需要的包不进行安装。安装的包越多,面临的风险起大,系统瘦身有利于提高系统的安全性。在操作系统使用过程中,为了避象由于多余组件和应用程序带来的安全风险,通常遵循最小安装原则,仅安装需要的组件和应用程序	1)访谈安装系统时是否遵循最小化安装原则,查看安装操作手册 2)使用命令'yum list installed" 查看操作系统中已安装的程序包,询问是否有目前不需要的组件和应用程序	1)系统安装遵循最小化安装原则 2)不存在业务所不需要的组件和应用程序	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獻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	务	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、上关闭多余端口,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P对本机服务的访问。其中/etc/hosts.dlow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)是否采用了从防火塘设置了对接入终端的限制	限制IP及其访问方式,如(举例): ssbd; 192. 168. 1.10/255.255 255.0	限制等 部分符合情况:通过网路地址范围对终端接入方式
入侵防范	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	时补修	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。如果假设曾常在会受到攻击,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,入侵不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所负人侵成人侵两种。系统入侵者在损人侵者在拥有取时,进行的破坏活动。通常,如果和用系统系更新更新发行级账号权限下进行的破坏活动。通常,如果和用系统系更新更新取分低的计程符。远程入侵,指入风者通过网络渗透和影响,现在不是不是不是不是不是不是不是不是不是不是不是不是不是不是不是不是不是不是不是	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</daemonname>	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	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

	•	I		T	
恶意代码防范		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变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,并在和应用程序等进行可信验证,并在加度用程序的关键执行环节进行动态可信验证,在检测到其构验证结果形成环行进行报警,并验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攻行为能被发现,并报警便于后续的处置动作		1) 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	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
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、重要配置数据、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	完整性	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	个人信息。 部分符合:系统采取措施对传输中的数据进行 宗整性校验:仅包括业务数据
XXXXIII II		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、重要业务数据、重要更重要的发展。 1	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		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	部分符合:系统通过https协议对传输过程中的
数据保密性		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	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		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;

剥余信息保护	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	(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信	应用系統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,以及对存用户鉴别信息的临时文件进行删除或内容清除等	部分符合:无部分符合
初示旧心体扩	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	间间系统管理页,应用系统定台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	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。 好清除B/S系统中的Session和Cookie信息,以及对 存用户鉴别信息的临时文件进行删除或内容清除 等	后得到完全清除; 部分符合 无部分符合
	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	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	身份证号、电话等个人信息	NG: 不知以本来用户姓石, 屯山, 用」 XXXXXXX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	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	0.1 控权工法分词和使用用点的人工信息	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-持	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
	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	/etc/pam.d/system-auth 文 件 主 有 怕 问 的 远 坝 , 则 以	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	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 #登录密码量短修改时间,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/位	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、不存在空口向口令和弱口令账户,但未设置口令复杂度要求,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
身份鉴别		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,瞬锁时间等。 看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	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	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
	的三进行近往管理时,应未取必委捐施、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。因为其在教据传输过程中,账户与密码均明文传输,这是非常危险的。黑客通过一些网络对嗅探工是能够轻易地的窃取网络中明文传输的账户与密码,因此不建议通过Telnet协议对服务器进行选程管理。针对Telnet协议不安全这种情况,则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)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 servicestatus-all grep running, 查看是否存在Telnet服务	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
		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		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	以有怕应权限的身份包求进入LINUX,使用 1S-1X件名 命	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 数字表示为744 - rwr-w- r 数字表示为665 drw-xx-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合理理设置,部分文件和目录权限设置不合理理设置,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
	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 fp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		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	1)应核查是否不存在多余或过期账户,如查看games、news、ftp、10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	2)各类管理员均使用自己分配的特定权限账户登	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	是否实现管理用户的权限分离	o) 禁用 只 把 四 /0 /1 和	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
访问控制	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 不用户或某个进程,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"Is -1文件名"命令,查看重要文件和目录权限设置是否合理、如:#Is -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	部分符合情况: 由管理用户进行用户访问权限分配
	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(读一写、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		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。	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待语况: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	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	否正常 # ps =efgrep 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以以root身份登录进入Linux查看安全事件配置: #aerep'	[root@localhost april]# service auditd status auditd (pid 1656) is running	符合情况:已开启安全审计功能,且审计覆盖到每
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	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	100ddy , X 1 , 63 <u>H</u> X H 1 110g, X H 2 ddi 20	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 总部分符合情况: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。		3) 部署有第三方审计工具, 可实时记录审计日志,	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:无 不符合情况:未对审计进行进行保护,非授权人员可书审计进程,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	在安装Linux操件系统时,应试循最小化安装原则,即不需要的包不进行安装。安装的包越多,面临的风险起大,系统瘦身有利于提高系统的安全性。在操作系统使用过程中,为了避象由于多余组件和应用程序带来的安全风险,通常遵循最小安装原则,仅安装需要的组件和应用程序	1)访谈安装系统时是否遵循最小化安装原则,查看安装操作手册 2)使用命令'yum list installed" 查看操作系统中已安装的程序包,询问是否有目前不需要的组件和应用程序	1)系统安装遵循最小化安装原则 2)不存在业务所不需要的组件和应用程序	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獻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	务	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、上关闭多余端口,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P对本机服务的访问。其中/etc/hosts.dlow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)是否采用了从防火塘设置了对接入终端的限制	限制IP及其访问方式,如(举例): ssbd; 192. 168. 1.10/255.255 255.0	限制等 部分符合情况:通过网路地址范围对终端接入方式
入侵防范	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	时补修	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。如果假设曾常在会受到攻击,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,入侵不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所负人侵成人侵两种。系统入侵者在损人侵者在拥有取时,进行的破坏活动。通常,如果和用系统系更新更新发行级账号权限下进行的破坏活动。通常,如果和用系统系更新更新取分低的计程符。远程入侵,指入风者通过网络渗透和影响,现在不是不是不是不是不是不是不是不是不是不是不是不是不是不是不是不是不是不是不是	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</daemonname>	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	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

	•	I		T	
恶意代码防范		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变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,并在和应用程序等进行可信验证,并在加度用程序的关键执行环节进行动态可信验证,在检测到其构验证结果形成环行进行报警,并验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攻行为能被发现,并报警便于后续的处置动作		1) 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	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
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、重要配置数据、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	完整性	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	个人信息。 部分符合:系统采取措施对传输中的数据进行 宗整性校验:仅包括业务数据
XXXXIII II		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、重要业务数据、重要更重要的发展。 1	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		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	部分符合:系统通过https协议对传输过程中的
数据保密性		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	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		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;

剥余信息保护	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	(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信	应用系統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,以及对存用户鉴别信息的临时文件进行删除或内容清除等	部分符合:无部分符合
初示旧心体扩	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	间间系统管理页,应用系统定台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	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。 好清除B/S系统中的Session和Cookie信息,以及对 存用户鉴别信息的临时文件进行删除或内容清除 等	后得到完全清除; 部分符合 无部分符合
	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	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	身份证号、电话等个人信息	NG: 不知以来来用户姓石, 电记, 用了 XXXXXXX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	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	0.1 控权工法分词和使用用点的人工信息	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	寻 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
	2) 你对孩是你用户准怎点你在江和"你	Linux系或統的用户鉴别过程与其他UNIX系統相同:系统管理员为用户建立一个账户并为其指定一个口令,用户使用指定的口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、组标识等的点数位,这样用户就具备一个私有口令。在《中记录用户的属性信息、包括用户名、密码、用户标识、组标识者标为正的口令文件,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,又有超级用户才有权读取。Linux中的经记(20)或由信息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文件是为作,也就是说/etc/pam.d/system-auth型的设置为准,也就是说/etc/pam.d/system-auth或的显优先级高于/etc/login.defs,但可能是该是有调用PAM的应用程度认证用户。登示服务、屏保等功能,其一一个重要的文件使是etc/pam.d/system-auth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	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 #登录密码量短修改时间,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	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,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
身份鉴别		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,瞬锁时间等。 看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	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	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,但未设置登录组时锁定参数。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
	的三进行近往管理时,应未取必委捐 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Telnett登录,也可以使用SSH登录。但是,Telnet不安全。因为其在教据传输过程中,账户与密码设明文传输,这是非常危险的。黑客通过一些网络对嗅探工是能够轻别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)以root身份登录进入Linux查看是否运行了sshd服务, service - status-all grep sshd 查看相关的端月是否打开,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 servicestatus-all grep running, 查看是否存在Telnet服务	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
		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		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	以有怕应权限的身份包求进入LINUX,使用 IS-1 X 件名 可 本手手更文件和日子权阻讼罢且不合理 加. # 1。 1	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 :数字表示为744 - rw - rw - r- :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合理部分符合情况: 重要文件和目录权限设置不合理理设置,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
	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 Ip 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		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	1)应核查是否不存在多余或过期账户,如查看games、news、ftp、10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	2)各类管理员均使用自己分配的特定权限账户登	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	是否实现管理用户的权限分离	o) 禁用 只 把 四 /0 /1 和	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
访问控制	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 不用户或某个进程,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"Is -1文件名"命令,查看重要文件和目录权限设置是否合理、如:#Is -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	部分符合情况: 由管理用户进行用户访问权限分配
	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(读一写、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		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。	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待语况: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	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	否正常 # ps =efgrep 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以以root身份登录进入Linux查看安全事件配置: #aerep'	[root@localhost april]# service auditd status auditd (pid 1656) is running	符合情况:已开启安全审计功能,且审计覆盖到每
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	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	100ddy , X 1 , 63 <u>H</u> X H 1 110g, X H 2 ddi 20	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 总部分符合情况: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。		3) 部署有第三方审计工具, 可实时记录审计日志,	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: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	在安装Linux操件系统时,应试循最小化安装原则,即不需要的包不进行安装。安装的包越多,面临的风险起大,系统瘦身有利于提高系统的安全性。在操作系统使用过程中,为了避象由于多余组件和应用程序带来的安全风险,通常遵循最小安装原则,仅安装需要的组件和应用程序	1)访谈安装系统时是否遵循最小化安装原则,查看安装操作手册 2)使用命令'yum list installed" 查看操作系统中已安装的程序包,询问是否有目前不需要的组件和应用程序	1)系统安装遵循最小化安装原则 2)不存在业务所不需要的组件和应用程序	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獻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	务	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、上关闭多余端口,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P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,/etc/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)是否采用了从防火塘设置了对接入终端的限制	限制IP及其访问方式,如(举例): ssbd; 192. 168. 1.10/255.255 255.0	限制等 部分符合情况:通过网路地址范围对终端接入方式
入侵防范	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	时补修	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
	的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。如果假设自常存不会受到攻击,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一般宽义上,入侵威胁分为外部渗透、内部渗透和不法行为三种,入侵不多,不够无所不以侵成协会了三种造成入侵威胁的入侵行为分为物理入侵、系统所面对的入侵成协可能包含了三种造成入侵威难的人侵行为主要是系统所面入侵人员两种东流动。通常,如果将用及时发展实现不近级账号权限下进行的破坏活动。通常,如果将用及时发现更新取变的新量,以是不知识,是不知识,是不知识,是不知识,是不知识,是不知识,是不知识,是不知识,	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</daemonname>	2)开启主机防火墙相关置 3)安装有基于主机的IDS设备	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,并进行报警部分有合情况: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

	•	I		T	
恶意代码防范		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变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,并在和应用程序等进行可信验证,并在加度用程序的关键执行环节进行动态可信验证,在检测到其构验证结果形成环行进行报警,并验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攻行为能被发现,并报警便于后续的处置动作		1) 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	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
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、重要配置数据、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	完整性	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	个人信息。 部分符合:系统采取措施对传输中的数据进行 宗整性校验:仅包括业务数据
XXXXIII II		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、重要业务数据、重要更重要的发展。 1	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		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	部分符合:系统通过https协议对传输过程中的
数据保密性		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	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		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;

剩个信自促铂	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	(如硬盘或内存)防止其他用户非授权获取该用户的鉴别信	应用系統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,以及对存用户鉴别信息的临时文件进行删除或内容清除等	部分符合:无部分符合
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	间间系统管理页,应用系统定台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	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。 好清除B/S系统中的Session和Cookie信息,以及对 存用户鉴别信息的临时文件进行删除或内容清除 等	后得到完全清除; 部分符合 无部分符合
	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	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	身份证号、电话等个人信息	NG: 不知以来来用户姓石, 电记, 用了 XXXXXXX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	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	0.1 控权工法分词和使用用点的人工信息	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一,因此对操作系统的密码是操作系统最常遇到的攻击方法之一,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。	3)打开"控制面板"-》"管理工具"-》"计算机管理"—"本地用户机组"检查有哪些用户,并尝试空口令登录	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	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,并定期更换口令的分合情况: 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 受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,从而增加猜测它码和难度的目的。 Window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》"密码锁定策程第2)右键点击桌面。>"个性化"->"屏幕保护复时。在恢复,不在恢复的形的长短以及"在恢复时的长短以及"在恢复时的长短,及"在恢复时的长短,及"在恢复了的长期,一个一个时间,一个一个时间,一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	a)账户锁定时间:不为不适用 b)账户锁定阈值:不为不适用	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		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理,但未关闭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	

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资原的,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可和如何访问这些文件和目录。对于操作系统中心些重的文件,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	が、	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	口 令 。 Windows 的 系 统 管 理 员 账 户 名 称 就 是	和组"窗口,查看"本地用户和组->用户"中的	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
	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	在命令行輸入"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 旁具有哪些权限,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	户权限分配"中的相关项目。右侧的详细信	角色分配权限,实现管理用户的权限分离,仅授予管理	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,且采用权限分配易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	目录)具有哪些权限,能进行哪些操作、通过在操作系统	10 m/c 2)查看重点目录的权限配置,是否依据安全	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	、%systemdrive% \system32 等重要的文件 夹,以及%systemdrive%\Windows \system32	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,依据访问控制策的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
	(b))应重命名或删除默认账户,修改默认账户的默认口令 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 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 d)应由授权主体配置访问控制策略规定主体对客体的访问规则 e)访问控制策略规定主体对客体的访问规则	控制的主要任务是保证操作系统资源不该非法使用和访师的,使用访问控制的自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自灵产的设计,是一个工作。	控制的主要任务是保证操作系统资源不该非法使用和访问、使用的证价。使用证价率的证价,使用证价率的简单。	按的的主要任务是保证操作系被资源,在基件生就中的每一个文件或 的问用采供严禁资源。在基件生就中的每一个文件或 的问用采供严禁资源。在基件生就中的每一个文件或 是一个文件或 的文学、则需要严格验据计论问规则是工作能的。 文学、则需要严格的数据的问题,从而加强系统的 为文学、则需要严格的数据的问题,从而加强系统的 为企业、周此、为了特殊系统的变之。需要对显示的 作的加速的,并合理是重庆行政。 大力和发展力,并合理是重庆行政。 大力和发展力,并合理是重庆行政。 对于操作系统的歌认唯户。由于它们的某些权限与实际 系的的变产的有关,是自身不在影子全间,在规模的所 对于操作系统的歌认唯户。由于它们的某些权限与实际 系的的变产的有关系,是有可以省解等期用户实际 系的的变力的形式。但是是是一个主义系称,是有可以省解等期用户实际 系的的变力,能力可能是一个主义系称,是有可以省解等期用户会 企业实现在一个主义系称,是有可以省解等期用户关 企业实现在一个主义系称,是可以省解等期用户关 对的版户,通免共享账户的存在 权限 建作系统的。为权限进行细数处的一个有利于会 所的版户,通免共享账户的存在 权限 操作系统的访问控制策略应由及权工体(如实定管理用 则是是是是一个的规模的。有关系统是一个主义系统,是一个的一个主义系统,是一个的主义。 或者是是原产的规模的。 "操作系统的访问控制策略应由及权工体(如实定管理用 的定接子管理用户的保险分离。" 操作系统的访问控制策略应由及权工体和自己实验,所以是一个有企多条账户,通过证明服户。不存在多部门、多人 对的条张产的用途、确认账户是需要于多全的 对的系统产的规模的。 "操作系统的访问控制策略应由及权工体和的主义系统。"并且是是一个特别,是是一个的规模的。 "操作系统的访问控制策略应由及权工体和的重要的。"访问的 "被解证用户的权限分离",实现可能是一个有企多条账户,通过证明服户。 本令个行像"不是如此的。"并且,在例的背话后,是全是是一个专业系统则, 对应由授权主体和更加强。是可以是一个对处,是是一个的规模的。 "是是一个的问题的解析是是一个数据的是是一个数据的现实管理 是一个的问题的解析是是一个数据的证明的主义。 是一个方面,是一个的规模系统定是是一个的权限分离。但是一个所有的最小权限,是是一个的规模的是一个可能是一个的规模的。 "是一个的问题的解析是是一个数据的主义。"并是一个可能是一个的规模的。 是一个的问题的的程度也还当中, 是一个的问题的则,并统一管理 是一个的问题的则, 也由是现在体配度之体, 是一个的问题的则,并统一管理 是一个的问题的则则,并统一管理 是一个的问题的则,并统一管理 是一个的问题的的程度上在, 是一个的问题的和是是一个数据的问题的是一个。 是一个的问题的和是是一个数据的问题,并统一管理 是一个的问题的知识,并统一管理 是一个的问题的则,并统一管理

	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	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。	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	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	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
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	定、损失评估、系统恢复提供关键性信息,所以审计覆	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)甲核近性成际,加划, 天败 e)以审核目录服务访问:失败 f)审核与权使用:失败	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"eventwir.msc",弹出"事件查看器"窗口,"事件查看器"在地)->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	和申订日志,而及现入侵的取同早取且接的力法就走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。 eventrwr. 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: 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	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、影 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Windowe 使盘默认共享。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	端口,如TCP 2745、3127、6129端口。 3)查看默认共享。	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防火墙是否启闲 。查看Windowsd防火墙。查看上便侧的"高级设置",打开侧列表中的"高级设置",打开闸列表。由击左侧列表中的"高级设置",打开"动开""远尾中中的"入站规则",双击右侧入站规则",对于"近年"的一种"窗口,选择"作用力模式(TCP-In)属性"窗口,选择"作用为模式(TCP-In)属性"窗口,选择作用场"查看P筛选器对登录终端的接入地址限制在命令行输入"gpedit.msc"打开本地组筑计查看P筛选器对登录终端的接入地址限制路等界面,算机配置"为中的"本地分第一次中,算机配置"为中的"本地分第一次中,第一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	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
	洞,并在经过充分测试评估后,	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必护自己不会受到攻击,或认为防护措施已全全,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,入侵威胁分为外部浸侵、系统不管人为三种,入侵行为三种,入侵行为三种,入侵侵所分为的政争人侵、系统入侵。所不能入人侵成战功的人侵成战的人侵人人侵,不能力,并不是有人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人	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	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,可以检测到对重要方点进行入侵的行为,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体内的病毒库子。只有当所毒有主机都及时更新了病毒库才能够做到防止病毒的入侵。因此应有统一的病毒管理策略,统一更新病毒库,定时查杀,及时发现入侵行为有效阻断等	1)查看系统中安装的防病毒软件。询问管理员病毒库更新策略。查看病毒库的最新版本更新日期是否超过一个星期 2)查看系统中采取何种可信验证机制,访谈管理员实现原理等 3)询间系统管理员网络防病毒软件和主机防病毒软件分别采用什么病毒库 4)询凡系统管理员是否果有统一的病毒更新策陷五套统策略 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,并在应态可信验证,在检测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,查看对那些系引导程序、系统 程序或重要配置参数进充行可信验证 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	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	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、重要配置数据、重要视频数据和重要个人信息等	的吸收,这对数据的无笔住进行检测,目检测到数据的 完整体集到现代时点或取标复类的对数据进行标复。 大	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20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	个人信息。 部分符合:系统采取措施对传输中的数据进行

	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、重要审计数据、重要业务数据、重要配置数据、重要配置数据、重要观频数据和重要个人信息等	、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	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	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	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	在传输过程中的保密性	 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 通过嗅探等方式抓取传输过程中的数据,未发现鉴别 	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;
334 PK III 1			在存储过程中的保密性	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 自等性间容存储	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—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	保存7天,数据每天凌晨1:00全量备份;
	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	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	证对存储介质(如硬盘或内存)防止其他用户		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	益以内付)/用陈归才能力能与共使用户, 例如.有的应用标	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	部分符合: 无部分符合
	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	业号、电话等个人 全身	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 本条款要求应用系统应采取措施,禁止未授权访问和非 (1)询问系统管理员,哪些系统账户可以访问 (1)询问系统管理员,哪些系统账户可以访问 (1)承统采取了措施控制可访 (1)系统采取了措施控制 (1)询问系统管理员,哪些系统账户可以访问 (1)系统采取了措施控制 (1)均问系统管理员,哪些系统账户可以访问 (1)系统采取了措施控制 (1)系统采取了任务。 (1)系统采取了任务证明 (1)系统采取了任务证明 (1)系统采取了任务证明 (1)系统采取了任务证明 (1)系统证明 (1)系统采取了任务证明 (1)系统采取了指施控制 (1)系统证明 (1)系统采取对 (1)系统证明 (1)系统采取了指施控制 (1)系统证明 (1)系统证明 (1)系统证明 (1)系统证明 (1)系统证明 (1)系统证明 (1)系统证明 (1)系统采取 (1)系统证明 (1)系统证证明 (1)系统证明 (1)系统证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明证证证证证证证证证证证证证证证证证证证证证证证证证证证证证证证证证证	・
--	---

	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一,因此对操作系统的密码是操作系统最常遇到的攻击方法之一,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。	3)打开"控制面板"-》"管理工具"-》"计算机管理"—"本地用户机组"检查有哪些用户,并尝试空口令登录	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	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,并定期更换口令的分合情况: 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 受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,从而增加猜测它码和难度的目的。 Window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》"密码锁定策程第2)右键点击桌面。>"个性化"->"屏幕保护复时。在恢复,不在恢复的形的长短以及"在恢复时的长短以及"在恢复时的长短,及"在恢复时的长短,及"在恢复了的长期,一个一个时间,一个一个时间,一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	a)账户锁定时间:不为不适用 b)账户锁定阈值:不为不适用	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		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理,但未关闭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	

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资原的,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可和如何访问这些文件和目录。对于操作系统中心些重的文件,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	が、	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	口 令 。 Windows 的 系 统 管 理 员 账 户 名 称 就 是	和组"窗口,查看"本地用户和组->用户"中的	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
	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	在命令行輸入"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 旁具有哪些权限,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	户权限分配"中的相关项目。右侧的详细信	角色分配权限,实现管理用户的权限分离,仅授予管理	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,且采用权限分配易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	目录)具有哪些权限,能进行哪些操作、通过在操作系统	10 m/c 2)查看重点目录的权限配置,是否依据安全	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	、%systemdrive% \system32 等重要的文件 夹,以及%systemdrive%\Windows \system32	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,依据访问控制策的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
	(b))应重命名或删除默认账户,修改默认账户的默认口令 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 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 d)应由授权主体配置访问控制策略规定主体对客体的访问规则 e)访问控制策略规定主体对客体的访问规则	控制的主要任务是保证操作系统资源不该非法使用和访师的,使用访问控制的自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自灵产的设计,是一个工作。	控制的主要任务是保证操作系统资源不该非法使用和访问、使用的证价。使用证价率的证价,使用证价率的简单。	按的的主要任务是保证操作系被资源,在基件生就中的每一个文件或 的问用采供严禁资源。在基件生就中的每一个文件或 的问用采供严禁资源。在基件生就中的每一个文件或 是一个文件或 的文学、则需要严格验据计论问规则是工作能的。 文学、则需要严格的数据的问题,从而加强系统的 为文学、则需要严格的数据的问题,从而加强系统的 为企业、周此、为了特殊系统的变之。需要对显示的 作的加速的,并合理是重庆行政。 大力和发展力,并合理是重庆行政。 大力和发展力,并合理是重庆行政。 对于操作系统的歌认唯户。由于它们的某些权限与实际 系的的变产的有关,是自身不在影子全间,在规模的所 对于操作系统的歌认唯户。由于它们的某些权限与实际 系的的变产的有关系,是有可以省解等期用户实际 系的的变力的形式。但是是是一个主义系称,是有可以省解等期用户实际 系的的变力,能力可能是一个主义系称,是有可以省解等期用户会 企业实现在一个主义系称,是有可以省解等期用户关 企业实现在一个主义系称,是可以省解等期用户关 对的版户,通免共享账户的存在 权限 建作系统的。为权限进行细数处的一个有利于会 所的版户,通免共享账户的存在 权限 操作系统的访问控制策略应由及权工体(如实定管理用 则是是是是一个的规模的。有关系统是一个主义系统,是一个的一个主义系统,是一个的主义。 或者是是原产的规模的。 "操作系统的访问控制策略应由及权工体(如实定管理用 的定接子管理用户的保险分离。" 操作系统的访问控制策略应由及权工体和自己实验,所以是一个有企多条账户,通过证明服户。不存在多部门、多人 对的条张产的用途、确认账户是需要于多全的 对的系统产的规模的。 "操作系统的访问控制策略应由及权工体和的主义系统。"并且是是一个特别,是是一个的规模的。 "操作系统的访问控制策略应由及权工体和的重要的。"访问的 "被解证用户的权限分离",实现可能是一个有企多条账户,通过证明服户。 本令个行像"不是如此的。"并且,在例的背话后,是全是是一个专业系统则, 对应由授权主体和更加强。是可以是一个对处,是是一个的规模的。 "是是一个的问题的解析是是一个数据的是是一个数据的现实管理 是一个的问题的解析是是一个数据的证明的主义。 是一个方面,是一个的规模系统定是是一个的权限分离。但是一个所有的最小权限,是是一个的规模的是一个可能是一个的规模的。 "是一个的问题的解析是是一个数据的主义。"并是一个可能是一个的规模的。 是一个的问题的的程度也还当中, 是一个的问题的则,并统一管理 是一个的问题的则, 也由是现在体配度之体, 是一个的问题的则,并统一管理 是一个的问题的则则,并统一管理 是一个的问题的则,并统一管理 是一个的问题的的程度上在, 是一个的问题的和是是一个数据的问题的是一个。 是一个的问题的和是是一个数据的问题,并统一管理 是一个的问题的知识,并统一管理 是一个的问题的则,并统一管理

	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	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。	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	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	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
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	定、损失评估、系统恢复提供关键性信息,所以审计覆	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)甲核近性成际,加划, 天败 e)以审核目录服务访问:失败 f)审核与权使用:失败	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"eventwir.msc",弹出"事件查看器"窗口,"事件查看器"在地)->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	和申订日志,而及现入侵的取同早取且接的力法就走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。 eventrwr. 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: 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	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、影 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Windowe 使盘默认共享。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	端口,如TCP 2745、3127、6129端口。 3)查看默认共享。	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防火墙是否启闲 。查看Windowsd防火墙。查看上便侧的"高级设置",打开侧列表中的"高级设置",打开闸列表。由击左侧列表中的"高级设置",打开"动开""远尾中中的"入站规则",双击右侧入站规则",对于"近年"的一种"窗口,选择"作用力模式(TCP-In)属性"窗口,选择"作用为模式(TCP-In)属性"窗口,选择作用场"查看P筛选器对登录终端的接入地址限制在命令行输入"gpedit.msc"打开本地组筑计查看P筛选器对登录终端的接入地址限制路等界面,算机配置"为中的"本地分第一次中,算机配置"为中的"本地分第一次中,第一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	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
	洞,并在经过充分测试评估后,	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必护自己不会受到攻击,或认为防护措施已全全,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,入侵威胁分为外部浸侵、系统不管人为三种,入侵行为三种,入侵行为三种,入侵侵所分为的政争人侵、系统入侵。所不能入人侵成战功的人侵成战的人侵人人侵,不能力,并不是有人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人	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	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,可以检测到对重要方点进行入侵的行为,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体内的病毒库子。只有当所毒有主机都及时更新了病毒库才能够做到防止病毒的入侵。因此应有统一的病毒管理策略,统一更新病毒库,定时查杀,及时发现入侵行为有效阻断等	1)查看系统中安装的防病毒软件。询问管理员病毒库更新策略。查看病毒库的最新版本更新日期是否超过一个星期 2)查看系统中采取何种可信验证机制,访谈管理员实现原理等 3)询间系统管理员网络防病毒软件和主机防病毒软件分别采用什么病毒库 4)询阳系统管理员是否果有统一的病毒更新策陷五套统策略 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,并在应态可信验证,在检测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,查看对那些系引导程序、系统 程序或重要配置参数进充行可信验证 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	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	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、重要配置数据、重要视频数据和重要个人信息等	的吸收,这对数据的无笔住进行检测,目检测到数据的 完整体集到现代时点或取标复类的对数据进行标复。 大	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20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	个人信息。 部分符合:系统采取措施对传输中的数据进行

	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、重要审计数据、重要业务数据、重要配置数据、重要配置数据、重要观频数据和重要个人信息等	、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	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	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	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	在传输过程中的保密性	 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 通过嗅探等方式抓取传输过程中的数据,未发现鉴别 	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;
334 PK III 1			在存储过程中的保密性	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 自等性间容存储	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—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	保存7天,数据每天凌晨1:00全量备份;
	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	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	证对存储介质(如硬盘或内存)防止其他用户		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;
**! 赤 后 总 体 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	益以内付)/用陈归才能力能与共使用户, 例如.有的应用标	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	部分符合: 无部分符合
	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	业号、电话等个人 全身	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 本条款要求应用系统应采取措施,禁止未授权访问和非 (1)询问系统管理员,哪些系统账户可以访问 (1)询问系统管理员,哪些系统账户可以访问 (1)承统采取了措施控制可访 (1)系统采取了措施控制 (1)询问系统管理员,哪些系统账户可以访问 (1)系统采取了措施控制 (1)均问系统管理员,哪些系统账户可以访问 (1)系统采取了措施控制 (1)系统采取了任务。 (1)系统采取了任务证明 (1)系统采取了任务证明 (1)系统采取了任务证明 (1)系统采取了任务证明 (1)系统证明 (1)系统采取了任务证明 (1)系统采取了指施控制 (1)系统证明 (1)系统采取对 (1)系统证明 (1)系统采取了指施控制 (1)系统证明 (1)系统证明 (1)系统证明 (1)系统证明 (1)系统证明 (1)系统证明 (1)系统证明 (1)系统采取 (1)系统证明 (1)系统证证明 (1)系统证明 (1)系统证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明 (1)系统证证证明 (1)系统证证明 (1)系统证证明 (1)系统证证明证证证证证证证证证证证证证证证证证证证证证证证证证证证证证证证证证证	・
--	---

	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		
	a)应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定期更换	应检查MySQL数据库的口令策略配置,查看其身份鉴别信息是否具有不易被冒用的特点,例如,口令足够长,口今复杂(如规定字符应混有大,小写字数字和特殊字符),口令定期更新,新旧口令的替换要求	1)尝试登录数据库,执行mysql -u root -p查看是否提示输入口令鉴别用户身份2)使用如下命令查询账号select user, host FROM mysql.user 结果输出用户列表。查者是否存在相同用户名3)执行如下语句查询是否在空口令用: select * from mysql.user where length(password)= 0 or password is null 输出结果是否为空4)执行如下语句查看用户口今复杂度相关配置: show variables like 'validate%; 或 show VARIABLES like '%password'	1)用户登录数据库时,采用用户名、口令的方式进行身份鉴别 2)查询user表,不存在相同的用户名 3)不存在空口令用户; 4)配置信息: validate_password_length 8 validate_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,但未设置口令未定期更换了个符合口令复杂度要求,或口令未定期更换不符合旧令,存在空口令或弱口令账户、可绕过身份鉴别措施进行登录		
身份鉴别	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	2/3) 数据库官理系统本地能置 J 参数max_connect_errors= 100, Wait_timeout = 28800, 如果mysql服务器连续接收到 フェ白工同一个土机的诗歌。日这此连续的诗歌会或和恐	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 该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		
		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	2)执行 mysgl>show variables like %have ssl%"	1)远程管理采用的方式:远程管理数据库,启用了SSL连接特性。 2)用户远程管理数据库时,客户端和服务器的连接不通过或跨越不可信任的网络,采取SSH隧道加密连接选程管理通信 3)本地管理,本条N/A			
	d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行与份鉴别,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	其他身份鉴别方式,在操作系统实现双因素,通常将服务器统入到堡垒机管理,同时通过限制仅允许通过堡垒机坛维服务器。在堡垒机实现因素身份认证。常见的双因素 31还产生在几个数字还是规模。	部分符合情况: 已部署堡垒机, 通过堡垒机管理服务器来		
	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	輸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	17年17月17日,10年17月17年77,开入共为617日2	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		

	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	select * from mysgl.user where user=""	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
访问控制	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	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	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	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
	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)	权限列 mysql>selcec * from mysql.tables_priv\G 一检查 用户表权限列	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	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) 2) 九丰22 从京人只在丰村22 12 12 12 12 12 12 12 12 12 12 12 12 1	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
		计会引起服务器的高昂成本。 因此建议采用第三方	mysal/show variables like 'log M' 查看輸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。 文审计记录覆盖内容 2)核查是否采取第三方工具增强MySQL目志功 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	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	部分符合情况: 已开启安全审计功能, 但审计未覆盖到所

	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	重要的安全相关事件,例如,用户登录系统、自主	录审计记录覆盖内容	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	类型,事件是否成功及其他与审计相关的信息
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	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MySql可以访问hostnam'err日志文件,由于该文件存放表名,存储过程名、代码等敏感信息,易被用于信息收集,并且有弃限仓,被导致多器的为强格的人员,不可以为数据存储,是有关的人员,是有关的人员,是有关的人员,是有关的人员,是有关的人员不能对自己的人员,非授权人员不能对自己进行了权限设置,非授权人员不能对自志进行是决估。另外,应防止审计日志空间不够而与数无法仍,根据《网络安全法》要求,日志应至少保存6个月以上	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	17未取了备价、软件等于权利审订比求进行保护,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	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: 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
		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	> GRANT ALL ON *.* TO 'root'@'%'	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 间的若干主机;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	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jp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
		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	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	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		留切束畸为.对数据件里安数据母人指里留切, 母同王里留 丛.	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	进行恢复。平宗孙安尔凡金加数师、 里安里穷数 按 重要由计粉据 重更配署粉据 重更加频粉据和	务数据、重要审计数据, 重要配置数据、重要	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	不符合情况: 未采用校验技术或密码技术保障重要数据在
	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、重要计数据、重要补照数据和重要十数据、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	传输过程中的保密性	1)数据库管理员采用密码技术对鉴别数据、重要业务数据 和重要小人信息进行了保密性处理 2)通过映探等方式加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
	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 分传合情况: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
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	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: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	个人信息	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	的,不存在非必要用户个人信息
	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亲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		
	a)应对登录的用户进行身份 标识和鉴别,身份标识具有 唯一性,身份鉴别信息具有 复杂度要求并定期更换	应检查Oracle数据库的口令策略配置,查看其身份鉴别信息是否具有不易被冒用的特点,例如,口令足够长,口今复杂(如规定字符应混有大,小写字母数字和特殊字符),口令定期更新,新旧口令的替换要求	1)访谈数据库管理员系统用户是否已设置密码,并查看登录过程中系统账户是否使用了密码进行验证登录2)查看是否启用口令复杂度函数: select limit from dba profiles where profile= 'DEFAULT' and resource_name='PASSWORD_VERIFY_FUNCTION' 3)检查 utlpwdmg.sql 中" Check for the minimum length of the password"部分中"length(password)<"后的值4) PASSWORD_LIFE_TIME(口令过期时限)	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)<"	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信况:存在空口令或弱口令账户、可绕过身份鉴别措施进行登录		
身份鉴别	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'	2)dba_pofiles 策略中 PASSWORD_LOCK_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, 但未设置登录组时锁定参数, 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_OS_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		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		
	(1)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	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		
		1)在oracle系统安装时存在部分默认口今,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的口今是否为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		

i					
	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——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
访问控制	d)应授予管理用户所需的最小权限,实现管理用户的权限,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	但各用户权限限分配不占理 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、家统管理员,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,但各种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) 向可重要数据存储表格名称 6) 向高策略与模式 表的对应关系: select * from dba_sa_tables policies, 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 访问 高大学 一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个
	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 结果处个为pone 2)可在Oracle数据库中查看不同的用户登录数据库 多绘进进行不同的操作中主记录	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
安全审计	期和时间, 用户、事件类	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集作记录、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	OCCUPATION AT ATAMA	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P地址	查 看 在 sqinet. 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
		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/Opatch opatch Isinventory	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		数据库系统至少达到以下的备份要求:提供本地实时备份的功能,当数发生错误时,能及时恢复数据	1)询间系统管理员数据库的备份和恢复策略是什么, 查看是否达到上述要求 2)检查相关文档和配置,查看是否与系统管理员回答的一致	核查备份结果与备份策略—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
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	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	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	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 自第五条统计程由依定整件展到进程区型和7144	不符合情况: 未采用校验技术或密码技术保障重要数据在
	b) 应采用校验技术或或存储过 技术保证重整性,重要业务数据在存储的完整性,重要业务数据 程中的数据、数据、数据等重要业务数据 数据、负据重要业务数据 数据、负据重要和重要和负数据	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 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、重要观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、重要被规数据和重要个人信息等被修改的行为,并具备恢复措施	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
数据保密性	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	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	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 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

	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	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
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	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: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
	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 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	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	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
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		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	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:无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		
	有九府亜北升空期再協	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	和常见密码试图登录数据库系统,查看是否成功。		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		
身份鉴别	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,起其中一种鉴别 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		
	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		
		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	令;	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		
访问控制	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) 左 五五百左前 / 久五日 1, 起 1 马 1 豆木/// 1	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		

	制策略、访问控制策略规定	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)	切以官理贝数循件使用的切凹在制模型定省通过切凹 控制等數控制主体社会体验管理制制	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		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
	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
	期和时间 用户 事件类	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
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	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		测试等;	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
数据条价标		数据库系统至少达到以下的备份要求:提供本地实时备份 的功能,当数发生错误时,能及时恢复数据	1)询间系统管理员数据库的备份和恢复策略是什么,查看是否达到上述要求 2)检查相关文档和配置,查看是否与系统管理员回答的一致)核查备份结果与备份策略一致 2)核查近期恢复测试记录能够进行正常的数据恢复	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

双加田 川内			T	I	M A 1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
复		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	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	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	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 自等左传验过程中的宣数性图列被坏压至取了技术	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
	b) 应采用校验技术或密码技术保证重要数据在存储过技术保证重要数据在存储过程中的完整性、重要业务数据生生等。 医非动数据 电话分别数据 电电子 医乳数据 大 电电子 电力量 大 电电子电子 电电子电子电子电子电子电子电子电子电子电子电子电子电子电子电子	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	据、重要审计数据、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、重要观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、重要加频数据、重要配置数据、重要配置数据、重算机频数据和重要个人信息等被修改的行为,并具备恢复措施	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 存除过程内的完整性
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	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	陈杏注 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	体创任 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
	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:无
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	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		
	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 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	了用户身份证号、电话等个人信息	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
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	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	访问, 如权限控制等	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:无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

-	安全事業	安全计算环境-网络	等设备-cisco(S3A3G3)作业指导 制作方法	* *********	符合情况
ST A		- 新来位 日白春寺株山麓の大才を活を日前知らか		お用用常用工会を 機	行台情化
	s)应对登录的用户进行身份标识和查 别、身份能识具有地一性、身份鉴别信 是具有坚治度安齐定期更势	口COMPON 過程事に終了本業を登出地、列門報報の (ALMA) 選ば加州を同じておりを発生する。 選切時間(VTT)通ばてDVP内地位下された。 選切時間(VTT)通ばてDVP内地位下された。 15 でも連絡中面情報が立て、都需要の日からなどである。 15 でも連絡中面情報が立て、都需要の日からなどである。 15 でも関係を表現している。 15 でものでは、15 でありまた。 15 では、15 で	 Coco 職人show run®や、存在如下表現月戸到象配置 usermane addring relivings 15 personal 0 socoocox を記述される場合機能である。 を記述される場合をは、するのは、 ないまする。 を記述される場合をは、するのは、 ないまする。 を記述される。 とのできまする。 とのできまする。<	11 采取用户名口令进行身份垄断; 21 身份标识具有第一性; 31 房口中心部以上由数字字母将号组	符合情况:采用了一种及以上的身份 鉴别方式、身体标识具各唯一性、用 户口令的及以上,口令组成由大小写 字母、数字和字形组成,口令相约5天 运行一次更换。
		方規免身物を新信息被買用、可以進江米州今牌、仏 证服务器等措施、加强身份を到信息的保护。如果仅 の世エニム外会社のの	新聞館と使用して登場の場合を表示を示す。 第二年の場合を表示を表示を表示を表示を表示を表示を表示。 2. 治決管理度口や至島東原、宇宙等程の登場のである。 ロ今組立由数学、字母、特殊字符組成 ロ今組立由数学、字母、特殊字符組成 ロ今を変更大学、 ロ今を変更大学、 ロ今を変更対象のである。 ロ今を変更対象のである。 ロークを変更がある。 ロークを変更がな ロークを変更がな ロークを変更がな ロークを変更がな ロークを変更がな ロークを変更がな ロークを変更がな ロークを のを のを のを のを のを のを のを のを のを の	3) 用户口令地位以上曲數字字母符号组成: 成: 4) 定期 (90天以內) 更换用户口令。	部分符合体及、预期效果12.3.4美足一部分为部分符合。 不符合体及、采取及给砂瓷到方式。 用户口令也以下、且口令组成来采用 大小马字母、数字和特殊字符。未定 期进行口令更换。
		以後)はその対対を対し、2013年に十年を示定や足所 変更的要求。 使用"sowice password-encryption"命令对持续在配置 文件中的所有口令和長级最高进行加密。避免通过状 取配置文件而級取口令的明文			
902N		可以通过配膜性寒冷症、限制管理员的最大量等失确 次数、网络迅速解的自由进程等各种组织实现金分支 及效、网络迅速解的自由进程等各种组织实现金分支 级力可能解。 第二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十	接続登記文支援等子達施、不会管定、检查管条文施 能定性点、分析時候及 分析時候及 からないでは、 からができ、 からがでは、 からがでは、 からがでは、 からがでは、 からがでもでき、 からができ、 もができ、 もができ、 もがでを もができ、 もがでを もができ、 もがでを もがでを もがでを もがでを もがでを もがでを もがでを もがでを	 息用了管果失復处理功能: 主品量单处封一定次数支持限户输定: 主品量单处封一定次数支持限户输定: 最初到限个人子の分替。 	符合情况。应用了登录失晓处理功能。且至这登录这种一定次载机运行 限制。 起至这登录这种一定次载机运行 限制。 配置了进程给机运出地。 部分符合协定、张规则是是从决理之一 部分为他分符合。 是是是头皮处理功能。未能置于还登录到相随。未能 置量并且进行如副对流出功能。
	()当进行远视管理时,应采取必要措施、防止鉴别信息在网络传输过程中被容析	当对网络设备进行远视管理时,为避免口令持输过程 中别权取,不应当使用明文传送的robot服务。而应 当采用SSH、ITPS等加密协议等方式进行交互式管理	核童运程管理采用价格协议。 能入show numbe中、童器如下类均配置 line vity 0.4 ence-timeout 5.0 prolikige level 15 possword 7 00000FLCZ243 transport input sigh	 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值HTIPS的加密方 实施行这程管理。 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 进行证程管理。
	如应采用口令、客码技术、生物技术等 育和或再构以上组合的鉴别技术对用户 在行身协会创 且其中一种鉴别技术至 少应使用客码技术来实现	深用双回子垄别是防止欺骗的有效方法。双因子牵到 不仅要支访问者知道—也查别信息,还需要访问者拥 有垄别特征。例如采用令牌、智能少等	 访谈身份鉴别过程采用哪几种鉴别技术、并含着管理 员型参过程能证; 尤 他查查提供如中显否采用了密码技术、如调用了密码 技术采取5M1·5M4等算法 	 同封采用两种或两种以上结合的鉴别方式对用户身份进行鉴别。 其中一种方式采用密码技术。 	國打巡核管理。 明台懷尽。同財采用兩种成兩种以上 的身份臺刻方式。且其中一种臺刻方 宜采用了密码技术。 能分符合懷之。采用了两种及两种以 上的身份臺刻方式。但未包含密码技术。 不符合懷父:朱同时采用两种成两种 以上的身份臺刻方式。
	a)应对登录的用户分配账户和权限	为了确保文殊机的安全,需要对验证的用户分配股 户,并合理配置账户权限。例如、相关管理人员具相 均职位相对应的帐户和时限	 被金用户部户和权限设置情况、輸入力ow numbed 含着取下配置: username XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	1) 各帐户权限设置与实际业务需求一载。	符合情况:对登录的用户分配了不同 的帐户,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:朱对登录的用户分配不 同的帐户,且朱分配相关的权限。
	b)应重命名成删除新认账户,掺改新认 账户的新认口令	对下路由器的联认账户,由于他们的其位权限与实际 要求可能存在差异,从而组也安全隐患。因此这些联 认账户 应 被 蒙用, 并且 应 不 存 在 联 认 账 户 admin.husweit及联认口令	1、輸入がpow numleや、食養如下配置: username 20000000 pulledge xx password 2000000000 を容量を存在数以限プ、即spamener からなっ、CBcの容板 た。 2、砂波管理量名像改数以口や、食料登录过程验证。	 董命名默认居户、禁用或删除款认账 户; 惨次了默认报户的职认口令。 	特合情况: 已當会在機能験以版 户, 且已替改教以版戶的联认口令。 部分符合情况: 预期效果1.2 カー部分 符合为部分符合。 不符合情况: 太重会名或删除釈以版 户, 且使用軟以口令建设。 報合情况: はないないのできません。
結同控制	(1)应及对膨胀或停用多余的、过期的原 户、避免共享客户的存在	商由等中如果存在多余的、过期的限户、可能会被攻 由者利用其进行支出操作的风险、回应应及时清理路 由器中的限户、删除或等用多余的限户	1. 能入show number,查看如下配置: username XXXXXXXX givelege or provined XXXXXXXX 或收入于最后企业 2. 走台存在不同省環狀使用同一聚户。	 不存在多余或过期限户; 不存在共用能力。 	明合情况、通过show sunning来发现多 余、过期联户符在、且管理员用户与 条户之间——对应、五世单股户存在 。 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、且存在共享聚户。
	如应授予管理用户所需的最小权限。实 设管理用户的权限分离	格器管理用户的角色,对我都还有细致的分,有对于 各类的加致场面工作。同时仅是不看或用户所需的都 小权限。是他比较级被的施斯拉姆一些海底用户中等 让大约权限,例如,但万段全型分为两份管理员 ,安全管理员,系统管理员二个角色,并没置对应的 恢废	1. 访读管理员,连行角色部分,分为网络管理员,安全管理员,或全量组员不含有。 不设置的经验的管理 (1) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	 合理角色划分、管理用户的权限显否已 运行分度(设置程度、审计员、操作 员); 各用户权限为其工作任务所需的最小权 程。 	符合情况:创建有系统管理员、审计管理员、安全管理局等的选过12F41。 经济等级均分,安全管理局等等户进过12F41。 名张户仅加压最小的功效。 部分符合情况: 张照结束12为一部分符合情况: 张则结束12为一部分符合情况: 张则结束结管理员、审计管理员、审计管理员、安全管监内等限户单位。 各张户之俱基础内管理员风能。
	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	访问控制策略由接权主体进行配置,它规定了主体可以对各体进行的接作。访问控制能度要求主体为用户 级或进程程,客体为文件、数据库表程	此項不适合,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	×	×
	n)访问控制的粒度应达到主体为用户标或 进程组、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。访问控制就度要求主体为用户吸或进程组。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	×	×
	助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	報應報之是無數的同控制的模型,主當体都有它存在 的形式无所谓,可能是整形的数字,也可能是手程。 总之它表示主体的实金级制,她随标记由头空标 员进行设置,通过对重要信息资源设置输胀标记,决 主体议何种权限可客体进行操作,实现强制访问控制。	此項不適合	×	×
	s)应息用安全审计功能,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	为了利用税设备的运行状况、网络金雕、管理记录等 运行检查和记录。需要总图系统由立功能、系统自志 中的特个信息部分配了一个产量级别、并停塞一些 设施公务员等成功。在自己等的发现之一。 发展的另条经过度自愿推销。还各种管理及 则据证明的基础是一个企业。 的自己主动能处于自用以市	查看日步开启请求: show logging查看如下配置: Console logging (控制自日息): level debugging, O medages logging, und deatherfairen gleisteit Monitor logging (医对自身): level debugging, 0 medige logging (医对自身): level debugging, 0 medige deather specified (國內國際): enabled, xml deather (國內國際) (國內國日息): enabled, xml deather (國內國際) (國內國日息): enabled, xml deather (國內國際)	1) 开台了自志审计功能; 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00目志功能。 审计团整理重例每个用户: 并对每 个重要安全事件正审计。 部分符合情况: 强照规律12.3为一部 分符合情况: 设备未开启目志功能。 未被审计别每个用户行为以及重要安 全事件。
安全审计	約率计记录应包括事件的目期和时间。 用户、事件类型、事件是否成功及其他 均率计值关的信息	对于交换机应备。日志审计会容需要记录时间、类型 计开文换机应备。日志审计会容需要记录时间、类型 、用户、审件类型、零件是否成功等相关信息	ii產者具体日志: show loggin buffer, 查看如下配 量 (Cut 30 0815.06.582 2015 HZ75.035: S OFTMCD/MANDUE IN Grigolatine et al. (2) The transcriver is 1000 8ASE SC 559: 金倉で北長石台フ事件的日期制制则、用户、事 件景型、事件层近成功等位息。 可以重要的表现。 可以重要的表现。 可以正常的一位的一位,	 审计记录包括事件的目期和时间、用户、零件类型、零件是否成功及其他与审计程关的信息。 基础则正确。 	符合情况。审计记录账差盖到具体的 目期等均同、用户、等符度点、事符 显示成。或审计检点意、张明同 正确。 部分符合情况:预期结果12为一部分 符合为部分符合。 不符合情况:朱开启审计场底。审计 记录长名台目前时间,用户、事件 类型、零件是否成功及其他审计信息
		申计论是概要解助管理人员及对发现系统出行状况和 用稳改出行法。而是需要实验计上收支链基上和他 但上的保护,而正本技术等点,超越和超环		11 深取技术措施对审计记录进行保护; 21 蒋自立安医到坦志服务基底综合安全审 计移程保存; 31 定期条件设备审计记录。	符合情况: 您要有第三方目志审计系统、设备日志上传发第三方审计平台。 运行保护,目志与特别代达尼内等计平台。 运行保护,目志与特别代达尼人。 划引合合能及: 张熙继续上2.3为一部 分引合合能及: 张熙继续三方目志审计 系统、朱师继续三方目志审计 系统、朱师等计记者运行保护。 目志 保存时间不满足个片。
		保护好會计量程。当安全事件发生对能够及对记录事件发生的能够及对记录事件校生的详细内容。非审计员的其他聚户不能争断审计 进程	 粮食拿拿计员的其他股户是否能中新审计道程; 粮食是否盖过整金机运行管理,远程管理地址是否限制为整金机。 	1) 字审计员的其他账户不能中断审计进程: 程: 2) 通过继急机对设备进行管理,且远程管理地址规制为整垒机。	羽台情况: 丰寧計畫程贝的其他級戶 不能中新审计进程。 部分羽台情况: 无部分羽台情况。 不羽台情况: 丰审计管理员的其他账 户能中斯审计进程。
	a)应直摄最小安装的原则仅安装需要的 组件和应用程序	遵循最小交领原则,仅安装需要的些件和应用程序。 影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	×	×

短期所 安全要求 要求解读 別呼方法 主要证据

	6)应关闭不需要的系统服务、默认共享 和高色观口	吳地不需要的系位服务、新认共享和离危端口, 可以 有效跨位系统建设攻击的可能性	能入社的ow number。 但是实际网络早晚参考是否关闭不必 更多的的证据。 1995年100日 159-11991 1995年100日 159-11991 1995年100	1) 己美術幸必要的系统服务。	符合情况: 已关例不需要的系统服务 、默认共多和高金值口等。 部分符合情况: 无部分符合情况。 不符合情况: 存在多金系统服务和D. telvor等。存在身危服口和共享福口等。
入侵勢范	c)应通过设定终端接入方式或网络地址 范围时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访问网络必备的登录 地址运行原制,避免未经权的访问。可以利用。 scose-close 提供访问VTY的中途交配。同时, VTYS的报目年一定的提供,当房有的VTY。用来,就不 能再建立区面的同路建建了。这就有可能被利用进行 Dos (托德里多交击)	W.Attownse命や、重吾加下英宗配置 control 10 10 10 10 10 10 10 10 10 10 10 10 10	 仅允许管理终端或堡垒机运程量录设备。 	符合情况: 通过策略限制设备仪通过 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: 未采取描述对远程管理 设备的地址进行规制。
	の止提供数据有效性检验功能、保证通 过人机能口输入或通过通信接口输入的 内容符合系统设定要求	本条数要求应用系组应对数据的有效性进行验证,主 要验证那些独立人机进口加超许的开始输出会人或是 通信证目由的规则超低流性。建毛符合系统处定要 点。防止个侧所产幅人喷水板或毛布铁系统出地能如 系。防止个侧所产幅人喷水板或毛布铁系统出地能如 系统的安全。	此场不适合。该项要求一般在应用层面上标查	×	×
	e) 应能发现可能存在的已知漏剂,并在 经过充分调试评估后,及对修补漏剂	移查簿扫修补报告,管理员定原进行高调扫值,发现 编词在经过充分测试评估后及对修补漏调	1) 访该是否定原进行推测标题,查看展测标题检查; 2) 是否对亡支现的推测在经过克分测设评估后及时惨补。	 定期(至少每年一次、選評却的不算) 進行運用均額、并生成運用対路接受; 及对修补漏洞或按过海或评估后充分谈 喷漏刷不益行修补。 	符合情况:定期对改基进行漏洞打 据。且针对改现的漏洞经过测试评估 后及时运行维令。 部分符合情况:无部分符合情况。 不符合情况:朱定顺对设备进行漏洞 封班。且朱进均支把的漏洞进行测评 评估后及财运行维令。
	n应能够检测到对重要节点进行入侵的行力,并在发生严重入侵事件对提供报警	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US IPS等系统。或在的 火塘、UTM房间入侵检测功能,以检查息是否发生了 入侵和攻击	此项不适合,该项要求一般在人侵防护系统上实现	×	×
恶意代码防范	应采用免受恶意代码攻击的技术措施或 主动免疫可信验证别制及时识别入侵和 病毒行为, 并将其有效阻断	无论是Windows主机还是Limpx主机、都面临木马、辐 生等病毒的破坏。因此一般的主机为防范病毒、均企 安核反病毒软件、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	×	×
可做验证	可基于可信根对计算设备的系统引导程 序、系统程序、重要区景参数和反用程 中域任方式中分钟区 集全 四种类的		10点就是是基于可信用对政会的系统引导程序。 系统程 市、重聚汇票者长火城市应用的库托等估计包验证 运输等最后应用的分域操作等 专用之间分可能 可能量用应用的一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	初在杜鹃與其可信性受异唑基环在行政量。 并專聯証結果形成申計记录返至安全管理 中心 句安全管理中心可以接收设备的验証效果记 录 [2.23]	中的电影,并被交换的想象了可能力 可能和对于特别,所以使用的一种更更更重 相对与特别,系统程序,需要更更重 相对与特别,系统程序,需要更更重 电对与特别,不使程序,是更是重 是一种的一种。 是一种的一种。 是一种的一种。 是一种的一种。 是一种的一种的一种。 是一种的一种的一种。 是一种的一种的一种。 是一种的一种的一种的一种。 是一种的一种的一种的一种的一种的一种的一种的一种的一种的一种的一种的一种的一种的一
	3)应采用校验技术或密码技术保证重要 数据在价验证程中的场景性。包括他介 展了鉴别数据。重要全者规则 数据、重要企业数据、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中储和价值过程中免受未受 权的概点,应对该等的完整性进行检测,当性到到 短的资单性重例如时过应或未定重遇的模型指于恢 是一条条板要不是到限度,需要少数型,要于 计数据,需要是重数据重要的接触的需要个人信息 在特量过程中分配。	10向间系经管理员,该系统的鉴别数据,重要业务程度, 直要等计划型。重要设置数据。重要实施数据中重于人 信息等在"特础"的一名采用了较恰性水场空间技术是 定整性 次型性 元间,直要还重数据。重要领数数据、重要多条数据,重 等等行图表。查看是否被转进到外来到现在"传输过程中 的完整性受到他环并能够及时恢复	1) 系统提供对金别数据、重要业务数据、 重要审计数据、重要配置数据、供票数据 的重要个人的需要个价格证在中的实整性 保护推断 2) 系统检测引金别数据、重要业务数据、 重要审计数据、重要配置数据、供票数据 必需要个人创金各任物验证面积 足到推址后来是了技术推测进行处理,如 重传或是由无行	符合: 系统通过https协议对传输过程中的数据运行完整性故障: 包括 器中的数据运行完整性故障: 包括 图分符合: 系统实现指施对传输中 的数据运行完整性故障: 仅包括业 务数据。 不符合: 系统未买取指施对传输中 的数据运行完整性故障:
数据实整性	b) 应采用校验技术或密码技术保证重要 数据在存储证程中的运费性。包括包含 板子鉴别数据。重要全者数据、重要等 计数据、重要配置数据、重要视频数据 和重要个人位息等	本条柱要求对鉴别数据。重要业务数据、重要审计数据、重要审计数据、重要审计数据 重要规则数据,重要规则数据和重要个人也会在 特征过程中的原理性运行检测,并在检测到来整性受 到被可对深取恢复推炼	10向间系统管理员,显否误用检查技术或密码技术标准金 的报题。重更多各数型。重要临时数型。重要配置数型。 需更顺度数型需量于人位指导在特性证可的实理性 20世纪协会价格在股票中介金部股票。重要多效数。 需更审计数据、重要股票数据、重要被股款和重要个人 位息等。查看系统反应	1)系统采用检验技术或密码技术保证了鉴别 裁据、重要业务数据、重要审计数据、重 要处置数据、重要更换数级和电量个人位 20条项一位的对单位。 20条项一位的对中的决整性 20条项一位的对中域在超级中的多级数 、重要业务数据、重要审计数据、重要配 复数据、重要与计数据、重要配 复数据、重要处数据和重要中人、信息等 验验的工作。	符合: 系统通过MD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MD技术对存 储中的数据运行完整性校验: 仅对 鉴别数据, 未包括业务数据和个人 信息。 不符合: 系统术来则指述对存储中 的数据进行完整性校验:
	a)应采用會码技术保证重要数据在传输 过程中的保密性、包括但不同于鉴别数据、指重更业务数据、和重要个人信息等	本条款要求对金别数据、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	12询问系统管理员,是否采用密码技术保证鉴别数据。 要全多数股和需要个人信息等在传输过程中的保险性 21 通过保持等方式活取传输过程中的保险、查看服别数 56、需要全多数股和需要个人信息等在传输过程中及否进 行了加密处理	11.局域管理员采用密码技术对查别数据。 赛业多数据和重要个人信息进行了保密性 处理 21.通过或等等方式抓取特徵过程中的数 提供。未及设备的数据、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: 包括垄卸数据之行加密: 包括垄卸数据人位息。 部分符合: 系统通过https协议对传输过程中的数据进行加密; 包括垄卸数据、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;
数据保密性	(v)应采用密码技术条保证重要数据在存储过程中的保密性、包括他不限于备到数据。重要业务数据和重要人信息等	本多數要求对金別數据,重要业务数据和重要个人信息在分數过程中采取保密措施。如对立控数据进行加密等	10向间系统管理员,最否某所密码技术保证金函数据,重 更全参数器按重要个人信息等在中被证据中的保密性 力 故意就是中央的批评分。 詹若金徵据述,重更至外数 报和重要个人信息等是否加密件键	1) 系统采用了密码技术对存储在数规库中的 参测数据,需更业务和数据数据 完成规率中户的金融银度。 定数规率中均能分量的限度。 和重要个人信息等均加密存储	符合: 系统通过shz(26)对存储中的 数速进行加密: 40括差别数据、全 务数据即个人信息。 部分符合: 系统通过shz(26)37行间。 相关等分别第一个人信息。 不符合: 系统来取到他对存储中 的数据进行加密;
数据各份和按	s)应提供重要数据的本地数据各份与恢复功能	对数据进行各份。 是防止数据重到破坏后无法使用的 最好方法。 通过对数据紧索不同的各份方式和形式 等。 保压帐值要表现在发生结坏后能够恢复。 本条 被要求对应用系统的重要数据提供本地数据各份均恢 复功能	拉特问教理库管理员,我把非价各价处理复纯是什么 力球在各种策略企业是不合作。 配置显示列工确 功能全金的地震是行马台的推断。 动能全位的地震是行马台的推断。 动能全位的恢复测试记录。 查得是否能够进行正常的数据 恢复	1)提供数据的每天全量各份《(成每天增量 各价、定价全量各份 2)应则数据协致到成记录显示、影够使 用各价文件进行数据恢复	符合: 系统通过快振形式对应用程序进行备告。备价管理为每周2。 4、6进行备份。备价保存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、未摆供数据检查价能力、未摆供数据恢复功能。 不符合: 系统未对应用程序及数据进行备份。系统未对应用程序及数据进行备份。
	b)应提供异地实时各份功能,利用通信 网络将重要数据实时各份至各份场地	应提供灾各中心,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期(如火灾)不可恢复则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,是否提供异地实时各份功能。并通过 网络将重要配置数据,重要业务数据实时各份至各份场地	提供异地实时各份功能,并通过网络将重要配置数据、重要业务数据实时各份互各份起地	計行 所述等所为正用在77次数38 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 餘:
剩余信息保护	a)应保证鉴别信息所在的存储空间被罪 放成重新分配前得到完全调题	本条款要求应用系统持用户的鉴别结息所在的存储空间的现在。 同知理盘清接的才能分配绝类使用户),例如有的应 用系统特用的各量的信息或也内存中进行处理、处理 定域而分离分量消腾等。 这其他的用户通过一些非 正常于段就有可能获取该用户的鉴别信息	询问系统管理员,应用系统是否紧取措施保证对存储介质 (该够查成内存)防止其他用户字授权获取该用户的查别信息 息	应用系统采取措施保证对行储介质(如硬金成内存)中的用于全部信息进行及时清脆。 或内存)中的用于全部信息进行及时清脆。 如系统会对存储或调用过金彩信息的运货 实金是及时等收置空。及对清脆的S系统 中的Session和Coole信息,以及对存有用 户鉴别信息的临时文件进行删除成内容清 物态。	在 符合: 采取描绘保证鉴别信息存储 空间被释放后得到完全清除; 部分符合: 无部分符合 不符合: 未采取描绘保证鉴别信息 存储空间被释放后得到完全清除;
1 to 10 to 18 5	to)应保证存有敏感数据的存储空间被释 放成重新分配前得到完全调验	本各數要求应用系統应待敬感數理所在的存储空间(效 經查或內針消費給了被分別企業其他用戶,例如有的应 用系統在使用过程中可能分生之場相以所。 经有时间 的文件中间接受记录一些物质信息。 当我这些资源分 起始其他用户时,其他用户被有可能获取这些敏感信息	询问系统管理员, 应用系统是否紧取推施保证对存储介质 (你硬盘或内引)中的收益指定进行及时清除, 防止其他用 户字数权系取收函数据	戶臺新總惠的協助文件進行繼續使內容演 醫等 但用系統漢取「指統保証时待結合版」如 最成內內人中與他裁就提了資訊 如系統企即存據使调用过差別進動的系統 或支援及則可能應關定。及時期的系統 中的Session和Cooke信息,以及則有相用 是副值島的高助文件進行繼續或內高統 執行	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;
	s)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 集了用户身份证句、电话等个人 信息 70记录应用系统等个动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	行台: 泉球以米集用户姓名, 电 语: 用于XXX,XXX功能; 部分符合: 无部分符合 不符合: 系统采集信息专业务必 要;
个人信息保护	的应禁止未授权访问和幸运使用用户个 人信息	本多数要求应用系统应紧取措施。 蒙止未授权访问和 非运使用个人信息。从后保护个人信息	12询问系统管理员、哪些系统规户可以访问个人信息。 系统来取了什么国旗控制可访问个人信息的系统股户对个 人信息的访问 7就变有较其能是否有效的规制了相关账户对个人信息的 访问和使用		符合: 系统对个人信息显示界面进 行了图象处理。防止个人信息的字 该使用; 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。 且每次人员未签署保密协议。防止 个人信息进行

		安全计算环境	- 网络设备-H3C(S3A3G3)作业指导 测许方法		
控制点	安全要求	要求解读	瀬序方法 回転車用户在登录时是各条用了身份整别措施 口应核車用户対表、測试用户身份核识是否具有唯一性 以华先跨由最为例、輸入 (doplay current-configuration 即 [do cu] 命令: 检查是否存在如下配置:	授期结果或主要证据	符合情况
	小应对是各种户流行身份以次收益。 由他也就有效一步,并他当时应其有实 可能是是有效。	- BALL AP BRADENT FINE HARMS H	La Cardinal Service de Configuence à l'American de Cardinal de Car	1) 英语一种或证 由中華制度集 2) 新年级品种之一。 20 新年级品种之一。 20 第一次公司,董师介中中。	行合構図、其同了一報及以上的身份 整型方式、身份的公司基础。1寸,月 等金元方式、身份的公司基础。1寸,月 等金、竞争的时间成、口令等的次 日本一支票。 他の一支票。 他の一支票。 をの一支票。 一支票。 一支票。 一支票。 一支票。 一支票。 一支票。 一支票。
免债金别	的应具有登录失致处理功能。 应配置并 息用 的第全语。 源制华品登录次数 种当登录性 推翻的自动激出等相关推断	可设施订配置效率全还,随期管理员的最大竞争 失败次度。用格也建超的自动建二等各种抽题。 有量,是我必定功能。例如,可以用于 onco- tionous/ 命令 配配VI的信贷别,进步一个归约的 是一个归约的。从后是是是的过去也就能 是一个归约的。 从后是一个归约的。 一日接近日的一个归约的。 一日接近日的一个归约的。 一日接近日的一个归约的一个归约的一个归约的一个归约的一个归约的一个归约的一个归约的一个归约	1. 网络设备帐以应用登录支税处理功能。 2. 网络哈格尼斯拉曼克森处理功能 1. 化压燃机,他就可以second-control logi-attempt 3 exceed footime 300 — SEE	1) 企用并能實了資源失限处理功能 2) 等法量投码 "定次股后有股小稳定" 3) 配置了连接相时自动造出功能,相时制码不大 730万钟。	符合情况: 由用了登录失政处理功能, 且包含显示权应进行 能, 且包含显示权应进行 规则 配置了运动中退也功能。 他们可能的特合。 他们可能的特合。 不符合情况: 未配置整是2.5次建功能 成。 未配置整是2.5次建功能 成。 未配置整定效率或 置量分准接向动翻时提出功能。未配置整合性的 置量分准接向动翻时提出功能。
	(1)然後行延期管理時,企業等必要措施、訴 (2)然後有延期性報信理中被前所 (2) (3) (3) (4) (4) (4) (5) (5) (6) (6) (6) (6) (6) (6) (6) (6) (6) (6	当时网络设备还行运程管理时,为避免口令传输 过程中的协定,不是当使用耐文等运动Teles相 可以上,可以是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	 直接对必备进行运程管理的, 华力村区(输入 [display current-configuration] 命令, 查得显示在放下类似底置 isodi-uper text password opter-displaced to the configuration of the configuration of the state of the subherication type password the interface to the configuration of the Protocol induced on Subjective-Oper England 为研究情能设定所不符合要求。 网络设备通信保全机运行运程管理参照1、现行。 	1)深层SS4、HTIPS等加密或其他的安全方式进行 证据管理。	符合情况:采用SSA域HTTPS的加密方式连行运程管理。 然分符合情况:无部分符合情况。 不符合情况:采用tehnet、http的方式 进行运程管理。
	如应展用口令、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连行身 检查别,且其一一种鉴别技术至少应使用 由码技术来实现	採用取回子签码是抗止欺骗的有效方法。及回子 查到不仅要求访问者知道一些查别信息,还需要 访问者拥有鉴别特征,例如采用令牌、智能卡等	1、核查斯姓是否采用口令、密码技术、生物技术等两种或用种以上结合的鉴别技术对用户身份进行鉴别	 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 的身份是别方式,且其中一种鉴别方 该采用了密码技术。 您分约合情况:采用了两种及两种以 上的身份鉴别方式,但未包含管码技 未。 不符合情况:朱同时采用两种或两种 以上的身份鉴别方式。
	402对肇等到两户分配数户种权限	○ 7 株式交換性的なき、電管対象を成功への数 のである。 のでは、 のでは、 のでは、 のでは、 のでは、 のでは、 のでは、 のでは、	DEPARTMENT OF THE TAX AS THE TAX	1) 各版产的指总量与农职业务需求一批。	作品情報、対象最高用户分配了不同 計算が、且定能了不同時代報 他の目前情報、光郎が自合構品 がの目前機能、光郎が自合構品 不自合能。 まは意識用の一配不 明的部か、且まが配相気的収録。
访问控制	6)应重命名或删除款认服户,排改聚认服户 的聚伙口令	对于结由器的联认账户,由于他们的某些权限与 实际要求可能存在差异,从而造成安全撤走,因 反应查帐以原产应益被用,并且应不存在新认账 户odmin huswei及账认口令	使用較込服力を輸送しつ手工位登表拠由器 さ、学かれて交換机不存在較以原力のdrain biograph をかれて交換物能力 doubly book upon 報认存在的無力	 重命名款认账户、禁用或無赊款认账户; 参次了款认帐户的款以口令。 	符合情况: 巴重命名成態除數以账 户, 且已排收數以账户的數以口令。 部分符合情况: 强额结果1.2为一部分 符合为部分符合 所分,未重命名成態除數以账 户, 且使用數以口令登录。
	(1位及列蓋聯或等用多余的、过期的账户, 避免共享账户的存在	議会署中起東持在多金的。过期的账户,可要会 辖攻击者利用其运行李法兼行的风险。原此改及 时清理路由器中的账户,重除或传用多余的账户	1、华为州口、徽人 dagby current-configuration命令, 查看 每多加下类的命令形定数词产产品是奇啸大必要: local-user sooms privilege from tx 2、均整世风碑认服号的使用人具,分析是否存在共享限户, 过期多余数户。	 不存在多余或过期限户; 管理見用户均限户之间ーー对应。 	符合情况:通过dsplay current- configuration未完成多点。过期账户存 在、显错成员用户场股户之间——对 企、无非常形户存在。 部分符合情况: 短期结果12为一部分 符合力部分符合 不符合相说: 设备存在多余、过期账 户、且存在共享帐户。
	心立役于管理用户所需的最小电缆,实现管理用户的权限分离	27. 27. 27. 27. 27. 27. 27. 27. 27. 27.	1. (Calentina) 銀行機会的。 テクス機会管理が、安全管理 東、高級機能と、デクスを 1. を分れてご乗れ場 人の知知の current configuration像や をなった。 そのれてご乗れ場 人の知知の current configuration像や をなった。 そのない はいました。 1. (Calentina	 合理角色划分、管理用户的双项是否已进行分 角(场管理员、审计员、接标员); 各用户权限为其工作任务所需的最小权限。 	符合情况:创建有系统管理尽、审计 管理员、安全管理员等限户进红LUVEL 进行等级划力,推计于高角色型。 各族户位为起最小的权益。 场外的传输及:强制度是12为一部分符合为期分符合。 不符合情况:未创建本管理尽、审 计管理点、安全管理员等限户绝色。 各族户均具各相同的管理员权限。
	(),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各体的访问规则	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,访问控制程度要求主体为用户级或进程级,客体为文件、教授库收级	×	×	×
	e)访问控制的粒度应达到主体为用户级或道 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。访问控制程度要求主体为风户组成进程级,客体为文件、数据库表统	×	×	×
	们应对需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	18. 越級标记是遏制访问控制的体提、主客体都有它 存在的形式子所谓、可能是整形的数字、也可能 是字母、总之它表示主客的的安全级别、被抵标 让由实金管型显示行设置、通过可需更信息实验 设置载值标记、决定主体以何种权限对客体进行 操作、实现强制访问控制。	×	×	×
	si应应用安全审计功能,审计准直影特个用户,对重要的用户行为标准要安全事件进行审计	为了对网络设备的旅行状况、网络遗籍、管理记录等在比较等心思。 需要总用每级日本功能。 高等在于此类的心思,需要总用每级日本功能。 最级日本中的每个位置都设计是了一个产量级 交换时间来提出了企业是需要他是全种管理域口, 内部每件或者目志服务最左转音指交下,控制 行项口上的目志中提供于仓库状态	、金介ACC用的な必要が必要の出版を終一年世界が40の方式 金統AMP 7月前日は交換可能は多差。 直接を入る。1969年の1979年で、1	13 开启了日志审计功能 23 审计范围推断每个用户: 33 对重要的用户行力和重要安全审件进行了审计	符合情况。设备已开启log目忠功能 审计控范股匯重到输个用户,并对每 个重要安全率件进行审计。 您的分价信息、复数股票12.3为一部 分符合为部分符合。 不符合情况、设备未开启目示功能。 未能审计例每个用户行为以发重要安 全事件。

控制点 安全要求 要求解读 润钾力压 主要证据

	(s)审计记录应包括事件的目期和时间、用户 、事件类型、事件是否成功及其他均审计	对于交换机设备,目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结	1. 华为/IOC网络设备配置的自志演略、通过線入 'deplay logging' 南 deplay logkuffer '命令、 存在が下表が配置 9an 30 03822216 2019 Spine AUL/VPFURE,STATE,BNO: -MCD-1-Chassent-1-Ber 3333 risk 2 GgabatthermetU/2042 (belound: 'Packet-flee' 3333 risk 2 permit, comp source 192.1681.109 logging counting 7	 事计记录包括事件的目期和利润、用户、事件 类型、事件是否成功及其他与审计相关的信息; 系统利用工作。 	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12为一部分 符合为部分符合。
安全审计	相关的信息	息	GigabiEthemet1/1/042 (inbound): Packet-filter 3333 rule 2 permit cmp source 192.168.1.10 0 logging counting 7 packet(s).	2) 系统时间正确。	行官为即对付官。 不符合情况: 未开启审计功能。审计 记录未包含目期和时间、用户、事件 类型、事件是否成功及其他审计信息。
	cl应对审计记录进行保护、定期基础、避免 受到水发期的删除、协改或覆盖等	审计记录概律影響理人员及对及现系统运行状况和现象或由行为。 但如现象也许多。而是需要对对计记录实施故 从上向管理上的保护。历工未投权协议、撤除和 统环	 本方内C同格设备配置的目志実施、通过能力「display university on figures (中心 有位) 下表域配置 info-center enable info-center enable info-center enable info-cente subject on ourse (see-institute) info-cente support on 122-2012.1 positive local 1 info-cente source default channel 2 log level warning ramp-agent page enable standard subheroscotion samp-agent target host standard sutheroscotion samp-agent target host standard sutheroscotion samp-agent target host standard sutheroscotion 	 部署了综合安全审计系统; 采取技术措施的审计记录进行保护; 定期基恰设备审计记录. 	符合情况: 想要有第三方目志审计系 统。设备目志上传复第三方审计平台 這行保护。目志保存的间长达6个月。 部分符合规定: 恐厥处果12.3为一部 分符合协定: 恐厥处果12.3为一部 分符合协定: 未给要领三方目志审计 条件 条件 条件 条件 条件 等的间径有规定 等的现在分词 等的现在分词 等的现在分词 等的现在分词 等的则 等所 是一个 是一个 是一个 是一个 是一个 是一个 是一个 是一个
	如应对审计进程进行保护,防止未经授权的 中断		×	1) 拿审计员的其他账户不顺中账审计进程。	符合情况: 北审计管理员的其他联户 不能中新审计进程。 部分符合情况: 无部分符合情况。 不符合情况: 北审计管理员的其他联 户能中新审计进程。
	a)应遵循最小安装的原则仅安装需要的组件和应用程序	遺循最小安裝原則、 仗安裝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、避免遭受由于系统赢消带来的风险	×	×	×
	(s)应关地不需要的系统服务、默认共享和高 推議口		着人delay current-configuration命令。根据实际网络环境争 考已最近的不必要服务。例如: p http://down	1) 已关地字必要的系统服务。	符合情况: 已关闭不需要的系统服务 、账认共参和高危端口等。 部分符合情况: 无部分符合情况。 不符合情况: 存在多余系统服务和, relnet等。存在高危端口和共享端口等
	cl应通话说定转调整人方式或网络电丝范围 时通过网络蛋行管理的管理终端遮行期制	为了保证安全、需要对通过VTV访问网络设备的 登进地址在序题制、避免投现的访问。可以利 用Dacosot-coma 操动设计的中地处立图。同 时,由于VTVs级数目有一定的原制,组织有的 VTV网壳、整个两直过压缩的网络建筑了。这 就有可能被利用进行Dos (把绝级系改造)	会会記憶性会中中年美術加下配置性急 soft matther 200 rule 10 permit source 10.1.100.0.00.0.255 rule 10 permit source 10.1.100.0.00.0.255 and 2001 inbound and 2001 inbound source rule permit source rule scheme user privilege level 1	1) 仅允许管理主机证程量录设备。	符合情况:通过策略限制设备仅通过 基地址成场进行成相管理。 部分符合情况:无部分符合情况。 不符合情况:朱采取塘施对远程管理 设备的地址进行限制。
入侵訪范	如应提供数据有效性处验功能。保证通过人 机能口输入或通过通信接口输入的内容符 合系统设定要求	本多數要求应用系统应对数据的有效性进行验证、主要验证部股通过人则建口(知程序的界面) 被人或进行性能定计解。外面整体式或处理是否 对合系统定更求。 防止十分原户输入或形型器 而导致系统处验更求。 防止十分原户输入或形数器 而导致系统处验例识以(注入支资等)人而影响系 使的正常使用甚至危害系统的实金	×	×	×
	e) 应能及现可能存在的已知漏洞,并在经 过支分测试评估后,及时修补漏洞		×	 管理员定额连行漏洞扫描、发现漏洞、在经过 支分测试评估后及时修补漏洞。 	符合情况: 定期对设备或行期则打 据。且针对及现价期间经过测试评估 行及则运行特别。 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 扫插,且未运对改更的漏洞进行洞评 评任后及时运行
	向应能够检测到对重要 节点进行入侵的行力,并在发生严重入侵事件时提供报警	要维护系统安全,必须进行主动直视,一般是在 网络边界、核心等重要节点处部署DS IPS等系统、或在的处理、UTM等用入侵检测功能、以检 窒息是否发生了人侵和攻击	×	×	×
恶意代码防范	应采用免受恶意代码攻击的技术抽造或主 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Unix主机,都面临水马、螺鱼等病毒的破坏。因此一般的主机为防范病毒。均全安装反病毒软件,或者采用可供验证机制可原设程序、应用程序等进行可信执行验证	×	×	×
可信验证	写基于可能解析并最近表的基础过程可以 。 医短视序,重要定置重要和原序程序等 进行可能处。 并在应用程序分类键形式 可可能处。 并在应用程序分类键形式 可定式作品可能能力。 在他类别类 性类类似化形式生活器, 非确显过机类形 现象计论是是某些查错符心	级备应作为通信设备或边界设备对特	1110年度是古塔丁刊度明省各省新兴到电视,新级观察 · 董安斯普特的文献的现在今年前了中的社 120年度,在120年度,12	疣量 引在检测到其可信性受到破坏后进行报警,并将验	行合模件。并是多点型等离子了包含。 特性操作。其一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是一种,是
	s)应高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,包括他不用于备 别数据。重要生务数据、重要申时数据、 重要配置数据、重要视频数据和重要个人 信息等	为了保证各种需要数据在存储和传输过程中免支 条接权的破坏。应对数据的完整性运行证例。 给我到数据形式更整性重新破坏应率效整理能 对数据运行效定,本务检查不可参加数据。需要 多条据。需要中计程则。需要死且数据 医安斯氏 振致和需要个人信息代物过程中的完整性进 行数据,被使用的重要性是列链环则采取恢复 推览,如案情或其它方式	1)询问系统管信息、该系统的鉴别数据、重要业务数据、重要等人的 要等计较远、重要起复数型、重要问题数据应量不少人信息 有一种编红即与显示同于效验计或自然技术经验等 7.0次工具对结组或文字的鉴别报题、重等业为报题、重要 运行程度、直接与影性地震到未知现在价格过程中的变型 性行程度、有差元影性地震到未知现在价格过程中的变型 性受到能坏并影響及对恢复	MALITACIA. MINISTERNATION	符合:系统通过https/bk以对传输过程中的数据进行完整性校验。但括显别数据。全条数据和个人信息。 部分符合:系统采取组施对传输中的数据进行完整性校验,仅包括全条数据。 不数据。 不数据。
数据实验性	b) 应采用校验技术成宏码技术保证重要数据在存储过程中的完整性,包括他不限于 整制效率,重要企业数据,需要申计数据 、重要配置数据、重要视频数率和重要个 人信息等	本各位原求对金分数据、重要业务数据、重要审计数据、重要国数据、重要股票数据、重要积极数据等个 人也是在价格证明中的实验性证明的。 开在他 周到完整性受到他环则采取快度抽搐	1)內同系被管理员,显否高用效的技术或容易技术保证金额 包括。重要业务数据,重要审计包想,重要配置收据,重要 报题股股收据于个人信息等在中的批评的的实验性 可能对效方价格也配定中与指导的性。要更多分别,更更多分别, 要申计书题,重要促展数据,重要现据数据和重要个人信息 等。查看所处反应	3)系统采用校验技术或密码技术保证了条的数据。 重要业务规划、重要审计规划、重要配置数据、重 要视频振型和重要个人信息等在 价值记录 性 7)系码可处进的价值在数据中的鉴别数据、重要 业务数据、重要申计数据、重要配置数据、重要研 数据标准。	符合: 系统通过MDS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MDS技术对存 储中的数据进行完整性校验。仅对 信息。 不符合:系统大学数据处计存储中 的数据进行完整性校验。 可可能是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个
	s)应采用密码技术保证重要数据在传输过程 中的保密性、包括他不规于鉴别数据、重 要业务数据、和重要个人信息等	本多故要求对益别数据、重要业务数据、和重要 个人信息在传输过程中采取保密抽题、如时这些 数据加密等	1)询问系统管理员。是否采用密码技术保证金别数据。重要 业务报股和需要个人信息等在传输过程中的保密性 21 通过领路等方式或集传输过程中投资起、套着鉴别数据、 需要业务报股标案学人信息等在传输过程中是否进行了加密处理。	1)系统管理具采用密码技术对查别数据、重要业务 数据收据要个人也包括行了保密包处理 2) 直过模据等方式指取传输近因中的数据、未发 现金别数据、重要业务数据和重要个人信息	符合、系统通过https协议对情能过 程中的数据过于规密。但活案制数 据、业务数据和个人信息。 到分符合、系统通过https协议对传 编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、系统未采取描述对传输中 的数据进行加密。
数据保密性	心症是用密码技术来保证重要数据在存储过程中的保密性,包括他不限于鉴别数据、 属于业务数据和重要人信息等	本各航票水利金函数据、重要业务数据和重要个 人但是在持续区群中采取保密措施、如时应控数 接进行加密等	1)內尼斯技管理员,是否是用密码技术保证查别表现,重要 业务影影或服务个人信息等在中被过程中的保健性 ,效据整型条件的联系等。 含著金劍散泥,重要业务数据 标量类个人信息等最否加密中槽	1)系统采用了密码技术对舟梯在数据库中的鉴别数 意。重要业务部部定要 记载提标中特殊品数据。重要业务数据有重要 个人信息等中均标准的指示。	符合、系统通过sha 256对存储中的 数据进行加密:包括鉴别数据、业 参数据和个人信息。 即分符合:系统通过sha 256对存储 中的数据进行加密:包括鉴别数 据、未对全参数据和个人信息。 不符合:系统被示 的数据进行加密
数据各价和恢复	a)应提供重要数据的本地数据各份与恢复功能			1)提供数据的每天企業条件《(成每天增量条件, 比期企集条件) (以加限组集中的效复测试记录显示, 能够使用备册 文件进行数据快整	符合: 系统通过快期形式对应用程 序进行备份。备份策略为构同2、 4. 6进行备份。备份策略为构同2、 4. 6进行备份。备份保存7天、数 据每天观尼1: 00全量备份 部分符合: 提供数据备份能力、未 提供数据备份能力、未 存行备份。 进行备份。
	b)应提供异地实时各份功能,利用通信网络 高重要数据实时各价至各价场地	应提供灾争中心,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适 行恢复	询问数据库管理员,是否提供异地实时各份功能,并通过网络将重要配置数据,重要业务数据实时备份至各份场地	提供异地实时各份功能,并通过网络将重要配置数据、重要业务数据实时各份至各份场地	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:
	s)应保证鉴别信息所在的存储空间被释放或 重新分配前得到安全满题	本多数要求应用系统専用户的垄销信息所在的存储空间(10等金项指令用户)。 明	询问系统管理员,应用系统是否深取推胜保证对存储介质(如 使盘或内存)防止其他用户非投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) 中的用户鉴别组象运行及财清额。如系统会对存储 或调用证鉴别组象的系数或变量及对可等或定义 及财清额的系统中的Sesson和Cooke位息、以及 对有用户鉴别信息的条数文件进行翻除或内容清 备等	符合: 采取植態保证鉴别信息存储 空间被释放后得到完全清除; 部分符合: 无部分符合 不符合: 未采取植脂保证鉴别信息 存储空间被释放后得到完全清除;
剩余信息保护	b)应保证存有敏感数型的存储空间被释放或 重新分配前得到完全调整	本条款要求应用系统应持敏感数据所在的存储空间的规律或内内:消除记不能分配的线性用户。 例如维查或内内:消除记不能分配的线性用户。 例如其的应用线在使用过程中可能会企场 临时文件,这些临时文件中可能会记录一些敏感 信息、等点还会资源分配处线世周户时,其他用 户被有可能获取这些被感息	询问系统管理员,应用系统是否深取措施保证对奇绪介质(如 便盘或分的产的被搭数测进行及时清除。 防止其他用户字径 仅原取取曲数据	在用系统采取了措施保证对并储介值(如便查提内 持入中的敏感教授在厅及时清脆,如系统会对存储 经调用证金别性息的无数改变是及对写物程度 及时清脆的系统中的Sesson和Coolse信息,以及 对存有用户鉴别信息的条款文件进行删除成内容清 等等	符合: 采取描绘保证敏感信息存储 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;

	0)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)我问系统管理员,该系统采集了用户的哪些个人信息 2)我问系统管理员,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。如系统采集了两 符合 聚姓文采集用户对 户身份证号、电话等个人 信息 7)记录应用系统等个功能领域使用等些用户个人编 有符合: 无部分符合 7)记录应用系统等个功能领域使用等些用户个人编 有符合: 系统采集信息想 度。
个人信息保护	b)应禁止未接权访问和非法使用用户个人信息	本条数要求应用系统应采取措施。 禁止免疫权识 问和李法使用个人信息,从而保护个人信息	1)询问系统管理员,哪些系统股户可以访问个人信息,且系 被某事了什么细胞控制可访问个人信息的系统股户对个人信息的访问 自然访问 可称重稳共调能是否有效的限制了相关联户对个人信息的访问和使用	将合:果她对个人信息自 行了股級处理。加止一个人信息 行了股级处理。加止一个 等级理。 1) 承级规定影等 7/2张授权走运访问和使用用户的个人信息 理,可直接在果板界理 用权关人员未受整律保密状 个人信息整整

***	****	安全计算	环境-网络设备-华为(S3A3G3)作业指导	** ***********************************	符合情况
世刊点		表字語 - 製まび、用户登录銘由器的方式句法 利用的制み即つ	要所方法	- 現用項系式主要を借	符合情况
	的应对登录的用户进行身带标识 标差别,身份标识有唯一性。 身份检验性能具有至少度要求并 定帐逻辑	Controlの記憶の記録を記録を表現を表現を表現を表現を表現を表現を表現を表現を表現を表現を表現を表現を表現を	「現人のなかった」という。 「現人のなかった」という。 「現人のなかった」という。 「現人のなかった」という。 「現人のなかった」という。 「現人のなかった」という。 「現人のなかった」という。 「日本のなかった。 「日本のな	17 月本・特別以上共和金別開進: 17 月本・特別以上共和金別開進: 18 月中の全別以上の数字の目の 18 月中の全別以上の数字の目の形成。 18 日の天以内)変数用户口令。	符合语义 英国了一种及以上的身份 每到对工。由你和以及事他一样,另 户口令的是及以上,中华就是从内身 方法,就学验学到组组,几个都约之 是一个"天涯》。 能力评合语义,强烈使用。2.24《典之一 动力部分传动》,在一个"大涯"。 不符合信义,未发现金专业为"太", 用心口中也以"水",且一个他或水源, 就在行口中变换,但一种"由水",东至 就在行口中变换,
身份查别	的应具有登录失败处理功能,应 配置并自用的宣会话、限制幸运 登录次载和当登录连接超时自动 退出等租关推施	可以進江配資地東全活。原制管理周別會大計畫失敗次数 ,將然進進到的自动國忠等多种推廣或認證至失敗之間 。解於進進到的自动國忠等多种推廣或認證本大敗之間 建立。「一個的技術」在「同門」「从市場的政治院 企業的」「一個的技術」在「同門」「从市場的政治院 企業的、一旦該管理房的證券失敗次徵超过设计数 是天安次表。一旦該管理房的證券失敗次徵超过设计数 版 來來再到其在門房證付款。从而即止率压用戶進江鄉 別經顧的方式登录等開出書	1) 新以登起次失義新开達後,不会想定。 检查登录失效电池模 尽 他人"daskly cursert-configuration"。 检查查尔在斯尼尼 1008—180—180 more more promoved only interval 5 may may 3 block 27) 資產 空海 海 超 时 号 设置 情况: 他人"daskly cursert- less vg 0.4 dis-consocial 20	11 点用并配置了登录失败处理功能; 22 主法登录这样一定次数后将股户锁定; 33 配置了连接超时由动造出功能,超时时 间不大于30分钟。	符合情况、应用了量率失败处理功能。且些非量是这第一定大家后进行 報制、配置了直接自动退出功能。 想外有合物定:因解故算12.3满足一 部分为部分符合。 不符合情况:未配置任务决处理动 也、未定置生生免溃弱相继。未配 重生要进接自动超时退出功能。
	(5)当进行运程管理时,应采取必要等推集、防止等别信息在网络传输过程中被包听	当对网络农多油行过程管理时,为理免口令特殊过程中的 68. 不适宜是新版大性品的1660年的。 由应当某用的时 17中等加密的保等力支出行及主义者前	改造管理及管理方式(本等管理/CR管理)、協会正程管理采用符 特色化、最大/ dashy carrier code_pustor 管理架 下配業 first storer enable show the control of the control of the control Code-west transposered coher APRALT foot-west control of the cont	1) 溪形SSH, HTTPS等加密或其他的安全方式进行运程管理。 2) 本地管理。	符合情况:采用SSH值HTTPS的邮密方式进行证据管理。 部分符合情况:采册SPH有合情况, 不符合情况:采用tenet、httn的方式进行证据管理。
	如应采用口令、密码技术、生物 技术等两种政而种以上组合的查 技术等两种政而并以上组合的查 到技术和用户进行身份查别,且 其中种等到技术至少应使用密 明技术来实现	為用反因子差別品別之欺骗的有效方法。 反因子差别不仅 要求公司者知道一些差别性息。还需要切问者拥有查别特 证。例如其所令佛、智能予等	1. 访选专价备创过程采用每几种盈别技术,并查看管理员登录过 细胞证 2. 检查鉴别线制中是否采用了些构技术,如调用了密构机成率取 5441-5544等算法	 同时采用两种或两种以上组合的鉴别方式对用户给告进行鉴别。且其中一种方式采用密码技术。 	符合情况:同时采用高种或用种以上的身份鉴别方式,且其中一种鉴别方式,且其中一种鉴别方式,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。 不针合情况:朱同时采用两种或两种以上的身份鉴别方式。
	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。需要对盐是的用户分配服户,并 台程能复数户权限,领加,他关管理人员具有与职位相对 品的股户标权限	1. 核変用产級欠級交換後更減2、能入 de local-usor 金書加下	 各帐户权限设置与实际业务需求一致。 	符合情况: 对登录的两户分配了不同 的账户,且分配了不同的权限。 都分符合情况: 无部分符合情况。 不符合情况: 未对登录的用户分配不 同的帐户,且未分配相关的规则。
	切应集命名或删除新认账户,修改新认账户的联致口令	村子提品器的報从医戶。由于他们的某些收得力享等更多 可容存在差异,从而直接交往撤集,因此还是收换产品 被服用,并且还不存在载战度产品dmintemm更最从口令	数据用所限户逻辑域 機入 del total-wore 業務対形製 機定命令的用户 User-name	13. 重命名款认账户、然用或删除款认账户, 户, 27. 惨次了款认帐户的款认口令。	符合情况: 已重命名资惠赊款认服 戶, 且已修改款认服户的款认口令。 部分符合他公: 据顺达第12为一部分 符合为部分符合。 不符合情况: 未重命名成服除款认服 户, 且使闲款认口令量录。
访问控制	c)应及时删除或停用多余的、过 期的限户,避免共享帐户的存在	路由層中如果存在多余的、过期的限户、可能会被攻击者 利用某进行支生操作的风险。因此应及时清理商品等中的 股户、膨胀或得用多余的限户	1. 命令囚上: 2. 就查得絕營理员、安全管理员和系统管理员不同用户采用不同用户采用不同用户重要条件		打合情况:通过dsplay current- configuration表更基金、过期账户存 在,且管理员用户与账户之间——对 定、无共享账户存在。 部分符合情况:预顺地果12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。
	也应提予管理用户所需的最小权 提、实现管理用户的权限分离	與基礎資訊介的負別問題者可能認的於分,有好不称 也也就與漢江的,因於從於"智也用戶來報用是《代說 · 推出。但於原則與其使用一直與其戶即但江大於位。 · 推出。但於原則與其使用一直與其戶即但江大於位。 · 被理 · 使 · 使 · 使 · 使 · 使 · 使 · 使 · 使	Louis Maria 。 日本会社の、今本科学技術、学生性点、 を特性化・今点、全球型が対象。 1、1000年7月7日、新化プーサイドは高くので、他会主意 を表するとなっています。 を表するとなっています。 中のでは、1000年7月7日、日本会社の 中のでは、1000年7月7日、日本会社の 1000年7月7日、 1000年7月7日 1000年7	1) - 市場自然分,等個用户的权限是否下 用方式 (四数据表 率针为 电影)- 20 高。 20 高。 20 高。	符合協定: 包建有高纯管理员、审计 管理员、安全管理局等所产品LLLV以 直示备级分子,用于工商电价级 各部厂可含稳定。各种规则。2.5一部分 符立方部分符合。 全侧面系统管理员、审 计管理员、安全管理员等用户确色。 各级产品具备相同的管理员的施。
		访问控制策略由授权主体进行配置、它规定了主体可以对 各体进行的操作。访问控制粒度要求主体为用户级或进程 级、客体为文件、数据库录级	×	×	×
	引访同控制的程度应达到主体为 用户级或进程级、客体为文件、 数据库表级	級、畜幣为文件、整理库券级 市间控制策略由授权主体进行配置、它规定了主体可以对 各体进行的操作。访问控制检查要求主体为用户级级进程 级、畜体为文件、整理库券级。 被继续与尽量的计同价的检查量、土金化的自立企业公司。	×	×	×
	n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	6. 命沙刀又下、数四本型地 被垂标记是强制访问控制的传播。主客体都有它存在的形式无所谓,可能是整形的数字。他可能是字母。总之它表示主客体的全使相对。被感标记由安全管理员注诉设置。 还主客体的全使相对。 通过对重要自身通设置被断形式。决定主体以何种现现对各体还持续作。实现强制访问控制。	×	×	×
安全审计		カブ州用品発金的近方状況、同地点重、管理化工等を正 地面的でき、需要出来を他当立功能、器質は立つ内容介 位金部域が北下一个产業収別、評価を一起市で利用機の 交換利力を指する協立直接で製造工業合併管理は1、 交換利力を設定機能と至ら計算では1、内部機 域化了上間がある。 域化了上間がある。 域化了上間がある。	BBITES (BBIS) - Groups inputs the logging batter configuration and contents - enabled Ablaved max buffer size - 1004 Annual buffer size - 1004 Annual buffer size - 1004 Canada Surfar size - 1004 Canada Su	13 开启了自志审计协能。 23 审计范围覆盖领电个局户; 23 审计范围覆盖领电个局户; 27 审计。	符合情况、设备已开启的目志功能。 审计范围度温影响作用户、京邦电 个重要文字标准行审计。 部分符合信贷、图题结果12.3为一部 均符合为部分符合。 不符合情况、经备先开启目志功能。 生能审计前每个用户行为议及重要安 全等符。
	的事计记录应包括事件的目期和 时间,房户、事件类型、事件是 否成功支其他与审计相关的信息	如子交換租份為,你立即計內容需要已過例似,是型,用 中,事件表別,事件是否成功等稅米值意	1.8 ELECTRO BLOCKE B. Abdison brighter logging before configuration and contents enabled followed that before the 1004 Consect studies 1-0, followed travel logistic Consection messages 10 Consection messages 10 Conse	1) 审计记录包括审样的目期和时间、用户 等有类型、零件是立成功及其他与审计程 设的记录。	符合情况: 审计记录度覆盖到具体的 的期间时间,用户、事件类型、事件 最否也为及时计极效值念 系统时间 定规 12为一部分对合。 部分对合为部分符合。 不开户审计功能、审计 记录表包含品期存时间、用户、等件 类型、事件是否成功及其他审计检查
	c)应对审计记录进行保护、定期 各价、避免受到未预期的删除、 排改或覆盖等	等计记录影告帮助管理人员及对议职系经运行状态和网络 或齿行为,因此需要对等计记录系数技术上标管理上的保 护,历工来现代传统、删整和破坏	The Computational Controller (1) 中国 1. 查看自念是否定准至第三九保存,输入* deploy current configuration 第基部并在加下配置 1. 企作文学 (1) 中国 1. 企作文	13 您署了综合安全审计系统; 27 深电技术推搡的审计记录进行保护; 30 定期条件设备审计记录。	符合情况: 部署有第三方目志审计系 统。设备目志上传至第三方审计平台 进行编书。目志保书时间长达个月。 部分符合规定 范围被乘 12.3为一部 分符合为部分符合。 不符合情况: 朱郎崇延三方目志审计 条线、朱邓明计区设置行保护,目志 保存时间不满足个月。

短期结果或 控制点 安全要求 要求解读 洞评方法 主要证据

					符合情况: 非审计管理员的其他联户 不能中新审计进程。
		保护好审计进程,当安全事件发生创能够及时记录事件发生的详细内容。2 审计员的其他账户不能中新审计进程	 秋章章申计员的其他股户是否能中新申计进程; 秋章是否通过银金机进行管理,远程管理地址是否限制为银金机,远程管理地址是否限制为银金机。 	 本审计员的其他账户不能中新审计选程: 通过保金机对设备进行管理。且远程管理地址限制为保金机。 	个能中都申订注程。 部分符合情况: 无部分符合情况。 不符合情况: 忠审计管理员的其他账 户能中新审计进程。
	s)应遵循最小安装的原则仅安装 需要的组件和应用程序	重循集小安装原则,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	×	×	×
	切应关绝不需要的系统服务、聚 认共享和高危端口	及人。」,可以他们的企业的企业, 关地不需要的系统服务,就认典李和高危端口,可以有效 降低系统建设改造的可能性	輸入的play current-configuration命令。超過支际网络环境参考已经 天統予心更繼多.例如: top shudown	1) 己美術学必要的系统服务。	符合情况: 已关闭不需要的系统服务 、默认共享和高色调口等。 部分符合情况: 无部分符合情况。 不符合情况: 存在多余系统服务作p. rotnet等, 存在集负调口和共享调口等
入侵防范	()应通过设定终端接入方式或同 格地址范围对通过网络进行管理 的管理终端进行规制	为了保证安全,需果对通过VYV的同网络设备的需要地址进行损耗,避免未提定的访问。可以利用pa accept class 限制 达到VYV的电话范围。同时,由于VYV的报告有一些的服务 当所有的VYVP用度。据代号用证此程的网络选择了, 这就有可能被制用进行Oos (在把重多次态)	能入每个寸分。对:社会是简信也中并在类似实下配置信息。 2d for the control of	 仅允许管理主机运程量录设备。 	符合情况:通过策略限制设备依通过 某地址成地址设可运行运程情况。 部分符合情况:无部分符合情况: 不符合情况:未深取避施对远程管理 设备的地址进行限制。
	の应提供教理有效性检验功能。 保证通过人机建口输入或通过通 链接口输入的内容符合系统设定 要求	本多數要求应用系统应对数据的有效性连行验证,主要验证标应能让人则被口抑制分的形物。 证标应能让人则被口抑制分的形的输入膨胀过速或进口输 人的数据整点或使最后符号系统处定要求,加上外的数据或与特殊系统已能如双以,注入攻击等)人而 则相处的正常使用器生血物系统的处分。	×	×	×
		核查漏扫零补报告,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惨补漏洞	×	 管理员定期进行揭洞扣携、发现漏洞。 在经过支分测试评估后及时修补漏洞。 	符合情况,定期对设备进行期间扣 市场政场的满洲经过测试评估 后及财运行路外 部分符合情况,无部分符合情况。 不符合情况,未定期对设备进行期间 种组,且未进对设现的漏洞进行测评 评估后及财运行路外。
	约应影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,必须进行主动直视,一般是在网络边界 、核心等重要市点处部署US IPS等系统,成在防火塘、 UTMI6用人级检测功能,以检查息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 制识别人侵和病毒行为, 并将其 有效阴断	光论是Windows主机还是Linux主机、都查临木马、蠕虫等 病毒的破坏。因此一般的主机为防范病毒。均会安极反病 毒软件、或者采用可信验证机制时系统程序、应用程序等 该行可信执行验证	×	×	×
可信舱证	可基于可值据对计算设备的系统 可与程序、系统程序、否实处理。 是实现了。 是实现了一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	以各应作为通信或各项应用设备对待	11位转变是还是于不仅值时以至的系统引导程序,系统程序,重要 在重单的大线面的程序或是打印电路。 2010年就是在四程序的文献和订单专起开始它可能是 2010年就是在四程序的文献和订单专起开始它可能是 2010年就是是在2010年代之前的文述主发生者指令心 (27)	第五社與到其可信性受到破坏后進行报費, 并非軸征起無形成率计论录返至安全管理中 心句安全管理中心可以接收设备的验证结果纪 景 (2.3)	中世纪、计算公众中断,可在了 可能明和一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个
	a)应采用校验技术或密码技术保整 实现现实现实现的现在分词 证证 包数据记不 随至的现在分词 证证 包数据记不 随至的数据、重 要必有数据、重 要配置数据、重 要不见数据系。 要不见数据系。	为了保证各种需要教资在存储的性量证据中电受太视识别 地球, 应对极限的安整性连行任间,当他测销度规则实整 性重新线积分组深效电量指数形式配行行效。本参数更 水场量到报税。需要多数股级,需要计划股、重聚型 数据重异规模形器和重聚个人信息在中能过程中的水差性 在标题,并不能用现实是由于现场,以来取收置指距。 如果中成其它方式。	1) 附近系特性性例,技术的设备对抗较。 医聚金光板层 医聚合叶 数据 医异位重视器 医外部病院的对抗原介人但是每点价格让现 中是光屏片,仅如此此本规则的技术是一个人但是每点价格让现 小的原产工具对插出核文中的运动形成。 医聚金素配置 医聚合甘酸 这 医聚定量的医 "是明光极度"的是,原来也未是因"是原本计数" 是可以此处,是一个人也是每点行业的 为时间,但是一个人也是一个人也是一个人也是一个人的一个人也是一个人的一个人们。 为时间,	1) 系统提供对金的股票。需要必多数据。 需要审计数据、需要形面数据、观频数型的 需要个人信息等在作输过程中的完整性保护 组施 (2) 系统检测列差别数据、需要业务数据、需要申计数据、需要保置数据、现据整理数据、需要不显数据、现据整理数据 需要个人信息等任务编述程中的完整性受损 循环标案取了技术细胞运行处理、知案传成 报告方式。	符合 - 系统通过https/sb以对传输过程中的数据进行实整性校验。包括程中的数据进行实整性校验。包括显示数据分符合: 系统来取福施对传输中部数据进行实整性校验: 仅包括空 多数据。 不能未来取福施对传输中的数据进行实整性校验:
数据完整性	b) 企采用收验技术观密码技术保 证值,但是不可能的技术观密码技术保 证值,但还是一个是一个是一个是一个是一个是一个是一个是一个是一个是一个是一个是一个是一个是	本於要求对無别教證、當更多条教證、當更审计教授、 當業足當就的、當英思縣教說和當著个人也由在中就社理 中的主整性显行检測、并在检測到實數性受到被以到深歇 性度閱题	1)询问系经管理员,是否采用较恰技术或密码技术保证金的数据。 重要业务效应,重要中计信息,重要处面数据,重要领面数块有量 7)均均均分价格在数据中的金函数据,重要必多效据,重要实计 7)均均均分价格在数据中的金函数据,重要多分级形,重要非 级型。 重要企业数据,重要规据数据和重要个人信息等,查看系统 反应	、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缘 改的行为、并具备恢复措施	符合: 寡绩適过MDS技术对存储中 的数据进行完整性校验: 包括鉴别 被据: 全身数据和个人信息。 部分符合: 系统查进MDS技术对存 结中的数据进行完整性校验: 仅对 备用的数据进行完整性校验: 仅对 信息: 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	3)应采用密码技术保证重要数据 在传输过程中的保密性,包括经 不限于垄到数据、重要业务数据 、和重要个人信息等		1)向网系格管提用,是否采用他的技术会征差别数据,重要全条数 影响框象个人组命等在特础过程中的保管性 2) 通过程序等方式部架特础过程中的程度,要等金别规矩,重要 发表视频率重聚个人组态等在传输过程中是否进行了加险处理	个人信息	符合: 系统通过https/bit/07/特鲁过程中的数据进行加密; 包括鉴别数据上行加密; 包括鉴别数据、全务数据和个人信息。 部分符合: 系统通过https/bit/07/6/6 部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: 系统未采取描述对伸轴中的数据进行加密;
	沙立采用密码技术来保证重要数据在持续过程中的保密性,包括 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位息等	本多數要求对簽別教證、廣東业务教證和廣要个人信息在 存據过程中采集保密措施。如时这些教授进行加密等	1)向风格整理度,是否采用密码技术点征差别数据,重要全条数 器收藏等个人也是等在中枢过程中的信息性 7)效象数据中分别民子说、查者会别取获、重要业务数据和重要 个人也思考点还如此存储	1)系统采用了密码技术对存储在数据库中的 强别数据,重要业务股股和重要 了数据库中的参数限据,重要业务数据 和重要个人信息等均加密存储	符合:原独通过sha256对存储中的 负表数据和个人信息。 等分符合:原始语言解数据、皇 部分符合:原统通过sha256对存储 中的数据运行部密、包括图别数 报。未对业务数据和个人信息。 不符合:原统证据的证明的 不符合:原统证的证明的的数据进行储中 的数据进行加密;
数据各份和依 至		对教座进行各份,显扬上教授遭到被坏后无法使用的最好 方法。通过对教授来取不同的各种方式也形式等,保证系 被重要假据在交生被坏后能够被整。未必然要求对应用系 统分重要数据准例本地数据各份与效型功能	1)與同數超单質提別,能應率的各种物度重視指在什么 2份或各种類构定量是否合理。配置是否例正确 3份或各种规则是否与各种规则。被 4份全定的恢复例以它使,查看是否使与进行正常的影響恢复	1)提供数据的每天企業各份《(成每天增量各份 份、定期企業各份) 力工能解故障系统度测试记录显示、影够使 用各份文件进行数据恢复	个行台: 系统术对应用程序及数据 读行备册:
	的应提供异地实时各份功能,利 用通信网络布里要数据实时各份 至各份场地	应提供灾备中心,对重要的数据提供异地数据级备价。保 证当本地系统发生灾难性后期(加火灾)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,是否提供开始实时各价功能,并通过网络将重要配置数据,重要业务数据实时各价业场协	提供异地实时各份功能、并通过网络将重要 配置数据、重要业务数据实时各份至各份场 地	
剩余信息保护		本各數要求应用系統特用户的鉴别信息所在的存储空间、如 經盘清潔化才能分配地其他用户),例如有的应用系统海 用户的金融值息放在内存中进行效理。处理效应是没有及 对编修等。及其集励的用户通过一型单正常子段被有可能 模取谈用户的鉴别信息	與同系統管理员。 应用系统最否减取措施保证对种维介员[如键盘或 内存]助止其他用户年授权贷取该用户的查别信息		行補空间被释取后得到完全清除 ;
	的)立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 滴除	本各數要次应用系统应非验酬数据所在的存储空间(如應盘或內的油廠已有 能分配检查用戶,預如有的正原系统在 或內的油廠貼不能分配检查用戶,預如有的正原系统在 使用过程中可能会产生。垫品對文件,这些能對文件中可能 会记录一些数据信息,当局这些资源分配检其他用戶對 其他用戶就有可能與單位空物感信息	與同系接管理例,应用系统是否是取措施保证可持續介限;如便查院 內中中的報應數据進行及时清除。防止其他用户字接领與取號應數 据	CONTRACTOR IN THE PROPERTY OF	符合: 采取植態保证敏感信息存储 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	各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 達系埃英集了用户的每步个人信息 7)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 引记录应用系统哪个功能模块使用哪些用户 小上位由 以当所编码个上位自动必要性	符合: 京姚仅采集用户姓名, 电 选, 用于XXXXXX功能; 部分符合: 无部分符合 不符合: 京姚采集信息非业务必
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	本多数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、哪些系统股户可以访问个人信息,且系统采取 了什么措施也等可访问个人信息的系统股户对个人信息的访问 72体来相关措施是否有效的限制了相关规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原户对个人信息的咨询。如识规控制等 2)未授权无法咨问和使用用户的个人信息	等合: 系统对个人信息显示界面连 行了影象处理。防止个人信息的非 途便期; 部分符合: 不配分符合 不符合: 系统未对个人信息进行处 建, 可直接在系统界面中最看到。 且相关人员未觉着保密协议。防止 个人信息测度。

	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	
	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 有值一性; 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。	
身份鉴别	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。	
	鉴别技术对用户进行身份鉴	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。	
	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——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。	
访问控制	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 2)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。
	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。
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) 应对甲订记求进行保护,定期 备份,避免受到未预期的删除	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	进过非单位管理员的共心燃厂能合中的单	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錯(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	下,客户自身定期进行漏扫或者安全评估

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、重要出分数据、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、重要设 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。	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	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,包括但不限工鉴别故 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	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
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	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、	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	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。		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。
	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。
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	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	数以发星及时与令以直至,及时消除系统 由的利众信息 以及对方方用页临别信息

数据完整性	、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	中光文水及代的吸外,应分数统的元莹性 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。 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 ************************************	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) 系統提供对鉴别数据、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	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:仅包括业条数据
	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、重要业务数置数据、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	本宗,孙安尔州金州致佑、重安业分致佑、 重要审计数据、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	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	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	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	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	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	本宗孙安水对金州致佑、里安业分致佑和 重要个人信息在存储过程中采取保密措施。 加对这此数据进行加密等	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	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		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) 即全量备份) 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	00全量备份;
	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;
	间被释放或重新分配前得到完	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,这样其他的用户的 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	被释放后得到完全清除; 部分符合: 无部分符合

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	广金加信总的响的文件近11 删除现内各消除等	空间做释放后侍到元至清际;
	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	ナXXX,XXX功能;
	b)应禁止未授权访问和非法使用 用户个人信息	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;

松 知 上	n.a.m.+		全计算环境-中间件(S3A3G3)作业		
控制点	安全要求 a)应对登录的用户进行身份标识	要求解读 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	测评方法	预期结果或主要证据 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	符合情况 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
	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	自 右 唯一州·	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)	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)	工, 主义三种子行关至组队, 并且定期支换, 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。
身份鉴别	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 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。
	鉴别技术对用户进行身份鉴	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。
	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——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。
访问控制	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、客体安全标记按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	全标记。
	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。
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,	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錯(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	
		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、重要配置数据重要心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。	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	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 据、重要业务数据、重要训 数据、重要配置数据、重 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	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
数据保密性	在传输过程中的保密性,包括	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、	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Cookle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	。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
	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Cookle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	。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

					,
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	条款要求对鉴别数据、重要业务数据、	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	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:仅包括业条数据
	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,包括但不限于鉴别散 据、重要业务数据、重要更散 数据、重要配置数据、重要视 频数据和重要个人信息等	数据和里安门入信息住行陷边住中的元金	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、 到数据、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	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	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	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	、重要业务数据和重要	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		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;
		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,这样其他的用户的 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	被释放后得到完全清除; 部分符合: 无部分符合

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		
	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	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	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	ナXXX,XXX功能;
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	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; 脱敏处理,防止个人信息的非法使用; 部分符合:无部分符合: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;

松 知 上	n.a.m.+		全计算环境-中间件(S3A3G3)作业		
控制点	安全要求 a)应对登录的用户进行身份标识	要求解读 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	测评方法	预期结果或主要证据 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	符合情况 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
	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	自 右 唯一州·	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)	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)	工, 主义三种子行关至组队, 并且定期支换, 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。
身份鉴别	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 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。
	鉴别技术对用户进行身份鉴	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。
	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——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。
访问控制	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		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。
	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。
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。
), 但形式	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錯(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。
入侵防范	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)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、重要配置数据重要心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。	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	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,包括但不限于鉴别散 据、重要业务数据、重要业务 数据、重要配置数据、重 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保单的。 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	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
数据保密性	在传输过程中的保密性,包括	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、	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Cookle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	。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
	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Cookle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	。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

					,
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	条款要求对鉴别数据、重要业务数据、	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	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:仅包括业条数据
	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,包括但不限于鉴别散 据、重要业务数据、重要更散 数据、重要配置数据、重要视 频数据和重要个人信息等	数据和里安门入信息住行陷边住中的元金	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、 到数据、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	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	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;
数据保密性数据备份和恢复	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	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	、重要业务数据和重要	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;
	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		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;
		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,这样其他的用户的 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	被释放后得到完全清除; 部分符合: 无部分符合

	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		
		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	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	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	ナXXX,XXX功能;
	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-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、重要电计数据、重要业务数据、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 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、重要业务视频数重要业务数据、重要配置数据重要免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	里安市订数始,里安配直数始,里安优观数据和里安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、独型规划数据和重要个人信息的"进行政",在第一次是是1974年	[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数据、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:新文学的 Ample of the part of	
	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	重安甲月数据、重安配直数据、重安代频 数据和重要个人信息在存储过程中的完整	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	部分行言: 系统通过MD5 技术对存储中的数据进行 完整性校验; 仅对鉴别和 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	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	本宗孙安水对金加数据、里安业务数据和 《香香》, (c) 在	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	sha256对存储中的数据进	

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	后工法旦1· ∩∩ □ □ □ □ □ □ □ □ □
	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		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		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	到完全清除; 部分符合: 无部分符合
剩余信息保护	 b)	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	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	部分符合: 无部分符合
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	授权访问和非法使用个人信息,从而保护	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内信息显示界面进行了脱处理,防止个人信息的非法使用;防止个合:无统可介个人合定。无统可介个人会。无统可可接合一个人在,对于有一个人。是没有一个人在系统界面中查看保密,以入员未会自己。