安全计算环境（S3A3G3）作业指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换	应检查Sql server数据库的口令策略配置，查看其身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口令复杂(如规定字符应混有大,小写字母数字和特殊字符)，口令定期更新，新旧口令的替换要求	1）展开服务器组，编辑SQL Server注册属性，查看身份认证方式；或者直接登录SQL Server企业管理器，试图连接数据库，查看系统是否出现用户和密码的输入框。 3）1）询问是否在安装时立刻修改sa口令，用该用户和常见密码试图登录数据库系统，查看是否成功。 4）2）在SQL 查询分析器中执行命令: use master select * from syslogins where password is null 查看是否有空口令用户。 5）询问口令的管理要求，如口令的长度、口令复杂性	1）选中“使用SQL Server身份认证”，并且选中“总是提示输入用户名和密码”。 2）提示用户输入密码。 3）sa用户的口令不是常见口令。 4）无空口令用户。	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施	应检查数据库系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值，对超过限制值的登录终止其鉴别会话或临时封闭帐号。查看是否设置网络登录连接超时，并自动退出	访谈管理员是否启用登录失败处理功能：是否限制用户尝试登录次数、登录尝试失败次数超过一定次数后数据库对用户的处理策略。	1）如果没有采用第三方工具或对SQL Server2000安全功能进行增强，则该项要求为不符合。	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	c)当进行远程管理时，应采取必要措施、防止鉴别信息在网络传输过程中被窃听	为了防止包括鉴别信息在内的敏感信息在网络传输过程中被窃听，应限制从远程管理数据，如果业务模式需要从远程进行管理，则应提供包括SSH在内的方式对传输数据进行加密	1）询问是否能对数据库进行远程管理; 2）在服务器网络实用工具中查看是否启用“强制协议加密(C)”。	如果能够对数据库进行远程管理，则应选中“强制协议加密(C)”，并对其进行配置。	符合情况：采用的远程管理方式启用了SSL连接特性，采取SSH隧道加密连接远程管理通信 部分符合情况：无 不符合情况：采用未进行加密处理的远程管理方式
	d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现	Sql server不能集成其他身份鉴别措施，应通过对操作系统层面实现双因素，强化数据库安全	访谈系统管理员并核查系统除用户名+口令外有无其他身份鉴别方法，如有没有令牌、数字证书和生物技术等，且其中一种鉴别技术至少应使用密码技术来实现。	采用除用户口令外另一种密码技术，可调用密码机制或使用SM1-SM4密码技术	符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，且在硬件Ukey中使用了加密算法 部分符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，但采用加密算法 不符合情况：未部署堡垒机，未通过堡垒机管理服务器来实现双因素身份验证
访问控制	a)应对登录的用户分配账户和权限	应检查数据库系统的安全策略，查看业务数据的管理员是否具有系统管理功能，业务数据库的操作人员是否具有删除数据库表或存储过程的权限	1）在“企业管理器”-）“安全性”中，选中每个登录用户，在右键菜单中选择“属性”，查看是否为每个用户指定了角色和能够对每个数据库的访问权限。	为每个登录用户指定了角色，并限定了每个角色的访问权限。	符合情况：已创建不同账户，并且根据用户所需为其分配相应的权限 部分符合情况：已创建不同的用户，但未进行权限的划分 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	SQL Server中的默认账户是sa账户，是在安装数据库时，初始化设置时设置的密码，sa账户是可以重命名或者删除的，至于默认口令，sa是不存在的，一般就是修改一下sa的名称	1）询问并验证sa用户的密码是否是空口令或弱口令; 2）现场让用户登录一次进行测试，验证用户的密码是否与描述一致。	管理用户sa的密码不是空口令和弱口令。	符合情况：不存在默认的、无用的可登录账户，已删除或禁用默认账户 部分符合情况：存在默认账户，但已修改默认账户默认口令
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在	应删除数据库中多余的过期的账户，如测试帐号等	访谈并核查数据库表中用户是否存在多余的、过期的账户，并询问管理员账户是否与自然人做到一一对应，不存在多人共用一个账户的情况。	不存在多余过期和共享账户。	符合情况：不存在默认的、无用的可登录账户， 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离	数据库的权限划分跟业务多少有非常大的关系，一般是有多少业务就有多少数据库，有多少数据库就有多少用户管理，我们给数据库划分权限，也最好按照数据库来划分	1）在“企业管理器”-）“安全性”中，选中每个登录用户，在右键菜单中选择“属性”，查看每个登录用户的角色和权限，是否是该管理用户所需的最小权限。	为每个登录用户授予所需的最小权限。	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	d)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	应检查数据库系统的安全策略，查看是否明确主体(如用户)以用户和/或用户组的身份规定对客体(如文件或系统设备，目录表和存取控制表等)的访问控制，覆盖范围是否包括与信息安全直接相关的主体(如用户)和客体(如文件，数据库表等)及它们之间的操作[如读、写或执行)	访谈管理员数据库使用的访问控制模型是否通过访问控制策略控制主体对客体的访问控制规则。。	由特定账户进行配置访问控制策略，并根据用户角色限制账户权限	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	e)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	明确提出访问控制的粒度要求，重点目录的访问控制的主体可能为某个用户或某个进程，应能够控制用户或进程对文件、数据库表等客体的访问	询问数据库管理员，访问控制的粒度主体是否用户级或进程级，客体是否为文件、数据库表级	由管理用户进行用户访问权限分配进行设置，依据访问控制策略，对各类文件和数据库表级进行访问	符合情况：已指定授权主体（一般为安全管理员）对数据库访问控制权限进行配置，且授权主体为用户，客体未数据库表 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置

	f)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	SQL Server本身并不具备这项功能，要想达到这一要求，就必须借助第三方软件了，这就需要根据被测评方所使用的的软件具体分析	1） 查看操作系统功能手册或相关文档，确认操作系统是否具备能对信息资源设置安全标记功能； 2） 询问管理员是否对重要信息资源设置安全标记。 3） 询问或查看目前的安全标记策略的相关设置，如：如何划分敏感标记分类，如何设定访问权限等。	1）主要数据库管理系统对重要信息资源设置敏感标记；2）强制访问控制的覆盖范围包括与重要信息资源直接相关的所有主体、客体及它们之间的操作。	符合情况：在数据库所在操作系统上，已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：在数据库所在操作系统上，已配置安全标记，但安全标记配置不合理等 不符合情况：未在数据库所在操作系统上对重要主体或客
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	应检查数据库系统是否开启安全审计功能，查看当前审计范围是否覆盖到每个用户	1）在“企业管理器”-〉右键单击注册名称-〉点击“属性”-〉“安全性”，查看审核级别。 2）访谈数据库管理员，了解是否采取第三方工具增强SQL Server的日志功能。	审核级别为“全部”。	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
	b)审计记录应包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息	应检查数据库系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户登录系统、自主访问控制的所有操作记录、重要用户行为(如增加/删除用户，删除库表)等	1）访谈数据库数据库管理员，了解是否采取第三方工具增强SQL Server的日志功能。 2）如果有第三方工具，则查看审计记录内容是否包括日期和时间、类型、主体标识、客体标识、事件的结果等。	有第三方工具且审计记录内容包括日期和时间、类型、主体标识、客体标识、事件的结果等。	符合情况：审计记录包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	应检查Sqlserver数据库系统，查看是否对日志进行了权限设置，非授权人员不能对日志进行操作,另外，应防止审计日志空间不够而导致无法记录日志的情况发生	1）访谈操作系统管理员，了解对SQL Server2000的日志记录采取的保护措施。	操作系统提供相关保护措施，不能被非授权破坏；通过备份审计记录文档避免未预期的覆盖。	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半
	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	Sqlserver数据库限制远程连接IP地址	在防火墙上做配置，只允许特定的IP地址建立1433通讯	已做限制符合	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	b) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击，应对系统进行漏洞扫描，及时发现系统中存在的已知漏洞，并在经过充分测试评估后更新系统补丁，.避免遭受由系统漏洞带的风险	1） 应核查是否不存在高风险漏洞,如漏洞扫描、渗透测试等; 2） 应核查是否在经过充分测试评估后及时修补漏洞。	1、有运维团队定期进行漏洞扫描，发现安全风险、及时修补 2、更新补丁时间为最近，对补丁进行控制和管理	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
数据备份恢复	a)应提供重要数据处理系统的热冗余，保证系统的高可用性	数据库系统至少达到以下的备份要求:提供本地实时备份的功能，当数发生错误时，能及时恢复数据	1)询问系统管理员数据库的备份和恢复策略是什么，查看是否达到上述要求 2)检查相关文档和配置，查看是否与系统管理员回答的一致	)核查备份结果与备份策略一致 2)核查近期恢复测试记录能够进行正常的数据恢复	符合情况：已提供重要数据处理系统的热冗余，如热备、集群、负载均衡等高可用方式 部分符合情况：无 不符合情况：未提供重要数据处理系统的热冗余
	b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地	应提供灾备中心，对重要的数据提供异地数据级备份，保证当本地系统发生灾难性后果不可恢复的，利用异地保存的数据对系统数据能进行恢复	1） 询问系统管理员是否提供异地数据备份功能,是否定时批量传送至备用场地 2)如果条件允许，则查看其实现技术措施的配置情况	1)已部署异地备份机房，并符合备份策略通过网络定期进行异地备份 2)查看实现的配置结果与备份策略一致	符合情况：已提供异地数据备份功能，实时将数据备份至异地备份机房 部分符合情况：已提供异地数据备份功能，但未实时将数据备份至异地机房 不符合情况：未提供异地数据备份功能
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、重要业务数据、重要审计数据、重要配置数据.重要视频数据和重要个人信息在传输过程中的完整性进行检测， 并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该数据库的鉴别数据、重要业务数据、重要审计数据，重要配置数据，重要视频数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、重要业务数据、重要审计数据，重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1） 数据库提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2） 数据库检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合情况：已采用校验技术或密码技术保障重要数据在传输过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在传输过程中的完整性
	b） 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问数据库管理员，是否采用校验技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等，查看系统反应	1)数据库采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性 2)数据库可检测到存储在数据库中的鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等被修改的行为，并具备	符合情况：已采用校验技术或密码技术保障重要数据在存储过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在存储过程中的完整性
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2） 通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中	1)数据库管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2） 通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合情况：已采用密码技术保障重要数据在传输过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在传输过程中的保密性

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