安全计算环境（S3A3G3）作业指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换	应检查MySQL数据库的口令策略配置，查看其身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口令复杂(如规定字符应混有大,小写字母数字和特殊字符)，口令定期更新，新旧口令的替换要求	1)尝试登录数据库，执行mysql -u root -p查看是否提示输入口令鉴别用户身份 2)使用如下命令查询账号 select user, host FROM mysql.user 结果输出用户列表，查者是否存在相同用户名 3)执行如下语句查询是否在空口令用: select * from mysql.user where length(password)= 0 or password is null 输出结果是否为空 4)执行如下语句查看用户口令复杂度相关配置: show variables like 'validate%'; 或 show VARIABLES like "%password"	1)用户登录数据库时，采用用户名、口令的方式进行身份鉴别 2)查询user表，不存在相同的用户名 3)不存在空口令用户; 4)配置信息: validate_password_length 8 validat_ password_mixed_case_count 1 validate_password_number_count 1 validate_password policy MEDIUM validate_password_special_char_count 1	符合情况：仅可通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，并已设置口令复杂度要求，且当前口令符合口令复杂度要求，并定期更换口令 部分符合情况：通过账户名加口令的方式进行登录，不存在空口令和弱口令账户，但未设置口令复杂度要求，当前口令不符合口令复杂度要求，或口令未定期更换 不符合情况：存在空口令或弱口令账户、可绕过身份鉴别措施进行登录
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施	应检查数据库系统，查看是否已配置了鉴别失败处理功能，并设置了非法登录次数的限制值，对超过限制值的登录终止其鉴别会话或临时封闭帐号。查看是否设置网络登录连接超时，并自动退出	1)询问管理员是否采取其他手段配置数据库登录失败处理功能。 2) 执行 show variables like %max_connect_errors%";或核查my.cnf文件，应设置如下参数: max_connect_errors=100 3) show variables like "%timeout%",查看返回值	1)MySQL数据库采用第三方管理软件，且第三方管理软件设置登录失败锁定次数 2)3)数据库管理系统本地配置了参数max_connect_errors=100, Wait_timeout = 28800，如果mysql服务器连续接收到了来自于同一个主机的请求，且这些连续的请求全部都没有成功的建立连接就被断开了，当这些连续的请求的累计值大于max_connect_errors的设定值时，mysql 服务器就会阻止这台主机后续的所有请求。Wait_ timeout: 一个连接connection空闲超过8个小时(默认值28800秒)，MySQL就会自动断开这个连接	符合情况：已配置登录失败处理功能相关参数，且设置登录超时锁定参数 部分符合情况：已配置登录失败处理功能相关参数，但未设置登录超时锁定参数，或未配置登录失败处理功能相关参数，但已设置登录超时锁定参数 不符合情况：未配置登录失败处理功能参数，未设置登录超时锁定参数
	c)当进行远程管理时，应采取必要措施、防止鉴别信息在网络传输过程中被窃听	为了防止包括鉴别信息在内的敏感信息在网络传输过程中被窃听，应限制从远程管理数据，如果使用了远程访问，要确保只有定义的主机才可以访问服务器，一般通过 TCP wrappers 、iptables或任何其它的防火墙软件或硬件实现	1)是否采用加密等安全方式对系统进行远程管理 2)执行 mysql>show variables like %have_ssl%" 查看是否支持ssl的连接特性,若为disabled说明此功能没有激活,或执行\s查看是否启用SSL;	1)远程管理采用的方式:远程管理数据库，启用了SSL连接特性。 2)用户远程管理数据库时，客户端和服务器的连接不通过或跨越不可信任的网络，采取SSH隧道加密连接选程管理通信 3)本地管理，本条N/A	符合情况：采用的远程管理方式启用了SSL连接特性，采取SSH隧道加密连接远程管理通信 部分符合情况：无 不符合情况：采用未进行加密处理的远程管理方式
	d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现	MySQL不能集成其他身份鉴别措施，应通过对操作系统层面实现双因素，强化数据库安全	1)MySQL不能集成其他身份鉴别措施,应通过对操作系统层面实现双因素 2）访谈系统管理员，是否采用其他技术手段实现双因素身份认证，是否采用了两种或两种以上组合的鉴别技术，如口令、数字证书Ukey. 令牌、指纹等，是否有一种鉴别方法使用密码	1)采用的登录方式有:用户名口令，MySQL数据库无法集成其他身份鉴别方式，在操作系统实现双因素，通常将服务器纳入到堡垒机管理，同时通过限制仅允许通过堡垒机坛维服务器。在堡垒机实现双因素身份认证。常见的双因素认证方式有口令、数字证书Ukey. 令牌、指纹等 2)采用的密码技术是: 在硬件UKey中使用了加密算法	符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，且在硬件Ukey中使用了加密算法 部分符合情况：已部署堡垒机，通过堡垒机管理服务器来实现双因素身份验证，但采用加密算法 不符合情况：未部署堡垒机，未通过堡垒机管理服务器来实现双因素身份验证
	a)应对登录的用户分配账户和权限	访谈管理员数据库用户账户及权限分配情况，并测试网络管理员、安全管理员、系统管理员或核查用户账户和权限设置的情况，有些mysql数据库的匿名用户的口令为空，因而，任何人都可以连接到这些数据库。如果匿名帐户grants存在，那么任何人都可以访问数据库，至少可以使用默认的数据库"test",因此，应核查是否已禁用匿名、默认账户的	1)执行语句select user,host FROM mysql.user 输出结果是否为网络管理员，安全管理员，系统管理员创建了不同账户: 2)执行show grants for' XXXX'@' localhost': 查看网络管理员，安全管理员、系统管理员用户账号的权限，权限间是否分离并相互制约	1)审计员的角色，创建了不同的账户，并为其分配了相应的权限 2)已禁用匿名、默认账户或限制匿名、默认用户的权限	符合情况：已创建不同账户，并且根据用户所需为其分配相应的权限 部分符合情况：已创建不同的用户，但未进行权限的划分 不符合情况：未对登录的用户分配账户和权限
	b)应重命名或删除默认账户，修改默认账户的默认口令	在linux中，root 用户拥有对所有数据库的完全访问权。因而，在linux的安装过程中，一定要设置root口令，要改变默认的空口令	1)执行select user,host FROM mysql.user 输出结果查看root用户是否被重命名或被删除 2)若root账户未被删除，是否更改其默认口令，避免空口令或弱口令.	1)数据库管理系统默认账户已被删除 2)数据本管理系统账认账户root未被删除，但增强其口令复杂度，不要空口令、弱口令的现象	符合情况：不存在默认的、无用的可登录账户，已删除或禁用默认账户 部分符合情况：存在默认账户，但已修改默认账户默认口令
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在	在默认安装mysql中，匿名户可访问test数据库.我们可以移除任何无用的数据库，以避免在不可预料的情况下访问了数据库，同时删除数据库中多余的、过期的账户，如测试账号等	1）在sqlplus中执行命令：select username,account_status from dba_users 2)执行下列语句: select * from mysql.user where user="" select user, host FROM mysql.user 依次核查列出的账户，是否存在无关的账户。 3)访谈网络管理员，安全管理员、系统管理员不同用户是否采用不同账户登录系统	1)不存在示例帐户 2)数据库管理系统用户表中不存在无关账户 3)不存在多人共享帐户的情况	符合情况：不存在默认的、无用的可登录账户， 部分符合情况：存在默认账户，但已修改默认账户口令 不符合情况：存在默认账户，且默认账户口令也未修改
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离	有些应用程序是通过一个特定数据库表的用户名和口令连接到MySQL的,安全人员不应当给予这个用户完全的访问权。如果攻击者获得了这个拥有完全访问权的用户，他也就拥有了所有的数据库。因此应核查用户是否行角色划分,核查访问控制策略，查看管理用户的权限是否已进行分离,并核查管理用户权限是否为其工作任务所需的最小权限	1)是否对用户进行角色划分且只授予账号必须的权限 如除root外,任何用户不应该有mysql库user表的存取权限，禁止将fil、.process、 super权限授予管理员以外的账户 2)查看权限表，并验证用户是否具有自身角色外的其他用户的权限	1）2)记录管理用户的权限分配情况：分配了网络管理员、安全员、审计员账号，root账户使用需向数据库管理员申请	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理

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	应检查数据库系统的安全策略，查看是否明确主体(如用户)以用户和/或用户组的身份规定对客体(如文件或系统设备，目录表和存取控制表等)的访问控制，覆盖范围是否包括与信息安全直接相关的主体(如用户)和客体(如文件，数据库表等)及它们之间的操作[如读、写或执行)	1.访谈管理员是否制定了访问控制策略 2.执行语句: mysql>selcec * from mysql.user\G -检查用户权限列 mysql>selcec * from mysql.db\G --检查数据库权限列 mysql>selcec * from mysql.tables_priv\G 一检查用户表权限列 mysql>selcec * from mysql.columns_privi\G -检查列权限列管理员 输出的权限列是是否与管理员制定的访问控制策略及规则一致 3)登录不同的用户，验证是否存在越权访问的情形	1制定数据库访问控制策略，由专门的安全员负责对访问控制权限的授权工作: 2)各账户权限配置，均是基于安全员的安全策略配置进行的访问控制 3)无越权访问	符合情况：已对各不同权限的用户创建不同的账户，如安全管理员、审计管理员、系统管理员，且采用权限分配最小化原则对管理用户进行权限分配 部分符合情况：已对各不同权限的用户创建不同的账户，但各用户权限限分配不合理 不符合情况：未对不同权限的用户进行权限分离，仅采用超级管理员账户进行管理
	e)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	明确提出访问控制的粒度要求，重点目录的访问控制的主体可能为某个用户或某个进程，应能够控制用户或进程对文件、数据库表等客体的访问	1）执行下列语句: mysql>selcec * from mysql.user\G -检查用户权限列 mysql>selcec * from mysql.db\G --检查数据库权限列 2)访谈管理员并核查访问控制粒度主体是否为用户级，客体是否为数据库表级	1) 2)由专门的安全员负责对访问控制权限的授权工作，授权主体为用户，客体为数据库表	符合情况：已指定授权主体（一般为安全管理员）对数据库访问控制权限进行配置，且授权主体为用户，客体未数据库表 部分符合情况：已指定专门的安全员负责对访问控制权限的授权工作，但安全策略配置不合理 不符合情况：未指定授权主体对操作系统访问控制权限进行配置
	f)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	MySQL不提供该项功能	访谈管理员，是否采用其他技术手段	MySQL不提供该项功能，主要依据操作系统层面实现该项功能	符合情况：在数据库所在操作系统上，已对重要主体或客体设置安全标记，且已控制主体对有安全标记信息资源的访问 部分符合情况：在数据库所在操作系统上，已配置安全标记，但安全标记配置不合理等 不符合情况：未在数据库所在操作系统上对重要主体或客
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	如果数据库服务器并不执行任何查询，建议启用审计。在/etc/my.cnf文件的[Mysql]部分添加:1og,=/var/1og/ my1ogfile 对于生产环境中任务繁重的MySOL数据库，启用审计会引起服务器的高昂成本，因此建议采用第三方数据库审计产品收集审计记录。应检查数据库系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户登录系统、自主访问控制的所有操作记录、重要用户行为(如增加/删除用户，删除	1)执行下列语句: mysql>show variables like' log_%' 查看输出的日志内容是否覆盖到所有用户，记录审计记录覆盖内容 2)核查是否采取第三方工具增强MySQL日志功能。若有，记录第三方审计工具的审计内容，查看是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	1)数据库本地启用了日志功能，审计内容覆盖到每个用户，能够记录用户行为和重要安全事件 2)启用审计功能策略为:配置了审计日志存储位置，或部署第三方数据库审计产品，审计内容覆盖到所有用户	符合情况：已开启安全审计功能，且审计覆盖到每个用户 部分符合情况：已开启安全审计功能，但审计未覆盖到所有用户 不符合情况：未开启安全审计功能
	b)审计记录应包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息	应检查数据库系统，查看审计策略是否覆盖系统内重要的安全相关事件，例如，用户登录系统、自主访问控制的所有操作记录、重要用户行为(如增加/删除用户，删除库表)等	1)执行下列语句: mysql>show variables like 'log_%' 查看输出的日志内容是否覆盖到所有用户，记录审计记录覆盖内容 2)核查是否采取第三方工具增强MySQL日志功能。若有，记录第三方审计工具的审计内容，查看是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	1）数据库本地启用了日志功能，审计内容覆盖到每个用户，能够记录重要用户行为和重要安全事件 2)采用第三方数据库审计产品，审计内容覆盖到每个用户，能够记录重要用户行为和重要安全事件	符合情况：审计记录包括事件的日期和时间，用户、事件类型，事件是否成功及其他与审计相关的信息 部分符合情况：审计记录不全、记录信息不够详细 不符合情况：未开启审计功能，无审计记录
	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	应保证只有root和mysql可以访问这些日志文件，其中，错误日志务必须确保只有root和MySq1可以访问hostnam'err日志文件，由于该文件存放在mysql数据历史中，文件包含如口令、地址，表名，存储过程名、代码等敏感信息，易被用于信息收集，并且有可能向攻击者提供利用数据库漏洞的信息,攻击者获取安装数据库的服务器的内部数据.MySQL日志，应确保只有root和mysq1可以访问logfileXY日志文件，此文件存放在mysq1的历史目录中。因此，应检查MySQL数据库系统是否对日志进行了权限设置，非授权人员不能对日志进行操作。另外，应防止审计日志空间不够而导致无法记录日志的情况发生，并对审计日志进行定期备份，根据《网络安全法》要求，日志应至少保存6个月	1)访谈管理员对审计话录如何保护，对审计记录是否定期备份，备份策略 2)是否严格限制用户访问审计记录的权限	1)采取了备份、转存等手段对审计记录进行保护，避免未预期的删除、修改或覆盖，数据库本地日志保存时间超过6个月 2)采用第三方数据库审计产品，审计记录保存时间超过6个月	符合情况：已对审计记录进行保护，无法进行删除、修改或覆盖，且定期备份，定期将本地存储日志转发至日志服务器，且保存时间大于半年 部分符合情况：无 不符合情况：未对审计记录进行保护、保存时间未达到半年
	d)应对审计进程进行保护，防止未经授权的中断	应测试通过非审计员的其他账户来中断审计进程，验证审计进程是否受到保护;对于MySQL数据库系统默认符合，但是如果采取了第三方工具，则应检查数据库系统，查看未授权用户是否能中断审计进程	1)询问是否严格限制管理员、审计员权限 2)用户重启实例关闭审计功能，查看是否成功	1)非审计员账户无法中断审计进程，审计进程受到保护 2)测试其他人员是否可以对审计进程进行开启，关闭操作，并记录	符合情况：已通过第三方系统对审计进行进行监控和保护，审计进程无法进行未授权的中断，管理员不可对日志进行删除 部分符合情况：无 不符合情况：未对审计进行进行保护，非授权人员可中断审计进程，可随意对审计日志进行更改、删除等操作

入侵防范	a)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制	直接通过本地网络之外的计算机连接生产环境中的数据库是异常危险的。有时，管理员会打开主机对数据库的访问: > GRANT ALL ON *.* TO 'root'@'%' 其实是完全放开了对root的访问，因此把重要的操作限制给特定主机异常重要: >GRANT ALL ON *.* TO 'root'@'localhost' >GRANT ALL ON *.* TO 'root'@'myip.athome' >FLUSH PRIVILEGES此时，即限制仅允许指定的IP(不管其是否静态)可以访问	查看用户登录的IP地址;是否给所有用户加上IP限制，拒绝所有未知主机进行连接 注:当user表中的Host值不为本地主机时,应指定特定IP地址，不应为%；或将user表中的Host值为空，而在host表中指定用户帐户允许登陆访问的若干主机；在非信任的客户端以数据库账户登录应被提示拒绝，用户从其他子网登录，应被拒绝	配置安全策略为:在防火墙上限制特定的终端(IP) 连接(访问)数据库:限定的IP地址为:XXXX	符合情况：已通过防火墙或其他安全设备对接入终端进行限制，如指定特定ip或对网络地址范围进行限制等 部分符合情况：通过网路地址范围对终端接入方式进行限制，但地址范围过大 不符合情况：未对终端接入方式进行限制
	b) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞	攻击者可能利用操作系统存在的安全漏洞对系统进行攻击，应对系统进行漏洞扫描，及时发现系统中存在的已知漏洞，并在经过充分测试评估后更新系统补丁，.避免遭受由系统漏洞带的风险	访谈MySQL补丁升级机制，查看补丁安装情况: 1)执行如下命令查看当前补丁版本: show variables where variable name like "version" 2)访谈数据库是否为企业版，是否定期进行漏洞扫描，针对高风险漏洞是否评估补丁并经测试后再进行安装	1)数据库当前不有在高风险漏洞，补丁更新及时，记录补丁信息为: MySQL数据库补丁定期更新版本 2) 数据库为企业版，定期进行漏洞扫描，在发现数据库漏洞时，必须经测试估后进行漏洞修补	符合情况：有定期进行漏洞扫描，及时发现安全风险，并根据扫描结果及时对安全问题进行修补 部分符合情况：定期进行漏洞扫描，但未及时修补漏洞 不符合情况：未定期进行漏洞扫描
数据备份恢复	a)应提供重要数据处理系统的热冗余，保证系统的高可用性	任何系统都有可能发生灾难，服务器、MySQL也会崩溃，也有可能遭受入侵,数据有可能被删除。只有为最糟糕的情况做好了充分的准备，才能够在事后快速地从灾难中恢复。用户应把备份过程作为一项日常工作。数据库系统至少提供本地实时备份的功能，当数据发生错误时，能够及时恢复数据	询问系统管理员数据库的备份和恢复策略是什么	备份策略为:对数据库重要数据每天增量备份，每周全量备份: 近期恢复测试时间:每月（季度）定期进行恢复性测试演练	符合情况：已提供重要数据处理系统的热冗余，如热备、集群、负载均衡等高可用方式 部分符合情况：无 不符合情况：未提供重要数据处理系统的热冗余
	b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地	应提供灾备中心，对重要的数据提供异地数据级备份，保证当本地系统发生灾难性后果不可恢复的，利用异地保存的数据对系统数据能进行恢复	1）询问系统管理员是否提供异地数据备份功能,是否定时批量传送至备用场地 2)如果条件允许，则查看其实现技术措施的配置情况	部署数据备份机房：有异地备份机房，实时（定期）将数据备份到机房	符合情况：已提供异地数据备份功能，实时将数据备份至异地备份机房 部分符合情况：已提供异地数据备份功能，但未实时将数据备份至异地机房 不符合情况：未提供异地数据备份功能
数据完整性	a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	为了保证各种重要数据在存储和传输过程中免受未授权的破坏，应对数据的完整性进行检测，当检测到数据的完整性遭到破坏时应采取恢复措施对数据进行恢复。本条款要求对鉴别数据、重要业务数据、重要审计数据、重要配置数据.重要视频数据和重要个人信息在传输过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施，如重传或其它方式	1)询问系统管理员，该数据库的鉴别数据、重要业务数据、重要审计数据，重要配置数据,重要视频数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性 2)使用工具对通信报文中的鉴别数据、重要业务数据、重要审计数据，重要配置数据、重要视频数据和重要个人信息等进行篡改，查看是否能够检测到未知据在传输过程中的完整性受到破坏并能够及时恢复	1）数据库提供对鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性保护措施 2）数据库检测到鉴别数据、重要业务数据、重要审计数据、重要配置数据、视频数据和重要个人信息等在传输过程中的完整性受到被坏后采取了技术措施进行处理，如重传或其他方式	符合情况：已采用校验技术或密码技术保障重要数据在传输过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在传输过程中的完整性
	b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息在存储过程中的完整性进行检测，并在检测到完整性受到破坏时采取恢复措施	1)询问数据库管理员，是否采用校验技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性 2)尝试修改存储在数据库中的鉴别数据，重要业务效据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等，查看系统反应	1)数据库采用校验技术或密码技术保证了鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性 2)数据库可检测到存储在数据库中的鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等被修改的行为，并具备恢复措施	符合情况：已采用校验技术或密码技术保障重要数据在存储过程中的完整性 部分符合情况：无 不符合情况：未采用校验技术或密码技术保障重要数据在存储过程中的完整性
数据保密性	a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据、和重要个人信息等	对鉴别数据、重要业务数据、和重要个人信息在传输过程中采取保密措施，如对这些数据加密等	1)询问数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在传输过程中的保密性 2）通过嗅探等方式抓取传输过程中的数据，查看鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理	1)数据库管理员采用密码技术对鉴别数据、重要业务数据和重要个人信息进行了保密性处理 2）通过嗅探等方式抓取传输过程中的数据，未发现鉴别数据、重要业务数据和重要个人信息	符合情况：已采用密码技术保障重要数据在传输过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在传输过程中的保密性
	b)应采用密码技术来保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要人信息等	对鉴别数据、重要业务数据和重要个人信息在存储过程中采取保密措施，如对这些数据进行加密等	1)询问数据库管理员，是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性 2) 核查数据库中的相关字段，查看鉴别数据、重要业务数据和重要个人信息等是否加密存储	1)系统采用了密码技术对存储在数据库中的鉴别数据、重要业务数据和重要 2)数据库中存储的鉴别数据、重要业务数据和重要个人信息等均加密存储	符合情况：已采用密码技术保障重要数据在存储过程中的保密性 部分符合情况：无 不符合情况：未采用密码技术保障重要数据在存储过程中的保密性
	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

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：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