安全计算环境-应用（S3A3G3）作业指导书

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

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