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/2022.9	吕萍/2022.9	

大数据安全拓展要求（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
基础设施位置	[关键]a)应保证承载大数据存储、处理和分析的设备机房位于中国境内。	对机房选址时，应确保机房位于中国境内、确保系统计算服务器及运行关键业务和数据处理的物理设备等基础设施位位于中国境内。	1)访谈管理员并查阅最新的机房资产，并询问 2)核查计算服务器及运行关键业务和数据的物理设备等基础设施是否都在中国境内。	部署整个大数据平台、应用的计算环境的机房，服务器及运行关键业务和数据的物理设备等基础设施均位于中国境内。	符合情况：机房位于中国境内，数据存储、处理不出境 不符合情况：机房位于中国境外
网络架构	[关键]a)应保证大数据平台不承载高于其安全保护等级的大数据应用和大数据资源；	大数据平台单独作为定级对象定级,大数据应用和大数据资源也可与大数据平台等级保护对象作为定级对象定级,大数据平台的等级要不低于所承载的大数据应用和大数据资源。	1)查看大数据平台备案证及大数据应用或者大数据资源系统定级备案材料。 2)核实是否存在大数据资源和大数据应用系统等级高于平台等级的情况。	1)提供有大数据平台等级保护备案证及大数据应用或大数据资源的定级材料。 2)大数据应用或大数据资源系统安全保护等级不高于大数据平台/系统的安全保护等级。	符合情况：大数据平台具有备案证且所承载大数据应用或大数据资源系统等级等于或低于大数据平台安全保护等级 不符合情况：大数据应用或大数据资源系统等级高于大数据平台安全保护等级
	[一般]b)应保证大数据平台的管理流量与系统业务流量分离；	大数据平台的管理流量与业务流量进行分离。	1)核查或访谈管理员，大数据平台管理采用何种方式，管理流量数据与业务流量数据如何分离。	1)大数据平台的管理流量与系统业务流量进行分离，流量不互相干扰；	符合情况：大数据平台管理流量与系统业务流量划分为不同的vlan或者采用不同的网络物理隔离 。 不符合情况：大数据平台管理流量与系统业务流量未采取措施进行隔离。
	[一般]c)应提供开放接口或开放性安全服务，允许客户接入第三方安全产品或在大数据平台选择第三方安全服务。	API(Application Ppogramming Interface,应用程序编程接口)是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件的以访问一组例程的能力,而又无需访问源码，或理解为内部工作机制的细节,API本身是抽象，仅定义了一个接口，大数据平台目前面临的互操作性问题的重要原因就是缺乏标准化和被广泛认可接受的API标准，因而大数据平台应提供开放和公开的API,允许第三方安全产品或服务接入	1)访谈大数据应用客户是否使用了第三方安全产品或服务； 2)查阅大数据平台接口设计文档或开放性安全服务文档	1)大数据应用客户使用了第三方安全产品或服务； 2)提供允许第三方安全产品接入的开放接口说明； 3）大数据平台允许第三方安全产品或服务接入，支持大数据用户选择第三方安全产品；	符合情况：大数据平台允许第三方安全产品接入，支持用户选择第三方安全产品 不符合情况：大数据平台不允许第三方安全产品接入，不支持用户选择第三方安全产品。
	[重要]a)大数据平台应提供双向认证功能，能对不同客户的大数据应用、大数据资源进行双向身份鉴别；	认证是验证或确定用户提供的访问凭证是否有效的过程，是网络安全第一道防线。在远程管理大数据平台中的设备时，双向认证有助于保证双向安全，有效的防止重放攻击和拒绝服务攻击。双向认证保证了终端不会被伪装服务器攻击，大数据平台不会被非法入侵,大大的提高了大数据平台和大数据客户的大数据应用、大数据资源系统连接的安全性。	1)访谈管理员，大数据平台和大数据应用、大数据资源之间采用的身份验证机制是什么 2)核查采用的身份验证机制是否实现了双向身份验证	1)认证方式采用双向身份验证机制 2)认证接入到统一身份认证中心，对接入到网络内的所有用户进行统一身份认证	符合情况：认证方式采用双向身份验证机制 不符合情况：认证方式未采用双向身份验证机制

身份鉴别	[关键]b)应采用口令和密码技术组合的鉴别技术对使用数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的主体实施身份鉴别；	一般采用账户和口令身份鉴别，随着安全性要求的提高，需要满足口令和密码技术组合的方式进行身份鉴别，比如动态口令、ukey、证书等，这样在很大程度上增加了非授权用户对身份鉴别信息进行攻击的难度，更有效的防止非法入侵。	1)询问系统管理员，数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件等是否采用动态口念，数字证书和生物技术等两种或两种以上组合的鉴别技术对管理用户身份进行登别 2)询问系统管理员，其中一种鉴别技术是否使用密码技术来实现 3)使用管理用户登录系统，验证其登录方式是否与询问结果一致	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：同时采用两种或两种以上的身份鉴别方式，且其中一种鉴别方式采用了密码技术。 部分符合情况：采用了两种及两种以上的身份鉴别方式，但未包含密码技术。 不符合情况：未采用两种或两种以上的身份鉴别方式。
	[重要]c)应对向大数据系统提供数据的外部实体实施身份鉴别；	身份鉴别是防止非法入侵最基本的一种保护措施，增加身份认证保护系统的安全性。	1)询问系统管理员，是否对向大数据系统提供数据的实体设备、系统进行身份鉴别。 2)查看系统或实体设备，是否具有身份鉴别模块或功能。	1)系统提供了身份鉴别措施 2)在未登录的状态下，外部实体或系统不可向大数据系统提供数据，身份鉴别措施不能被绕。	符合情况：实体设备、系统向大数据系统提供数据时必须需要进行身份鉴别。 不符合情况：未采取身份鉴别方式。
	[重要]d)大数据系统提供的各类外部调用接口应依据调用主体的操作权限实施相应强度的身份鉴别。	针对数据调用接口的主体划分权限，根据权限级别施行身份鉴别，身份鉴别强度根据权限相应提升。	1)询问系统管理员，大数据系统是否提供外部调用接口，并是否进行权限划分和施行身份鉴别。 2)查看系统或登录验证，是否具有身份鉴别模块或功能。	1)大数据系统提供外部调用接口，且对调用主体的操作权限进行不同强度的身份鉴别 2)在未登录的状态下，调用主体不能进行操作。	符合情况：大数据提供外部调用接口，根据调用主体的权限实行不同强度的身份鉴别机制。 不符合情况：未对调用主体进行身份鉴别。
	[重要]a)对外提供服务的大数据平台，平台或第三方应在服务客户授权下才可以对其数据资源进行访问、使用和管理；	为避免客户数据的非法访问，对数据的管理权限进行控制，仅允许客户的管理员访问，若需要大数据平台或第三方对数据进行访问、使用和管理，必须客户管理员提供授权，方能进行数据管理	1)核查客户的授权机制，如授权流程、授权方式及授权内容 2)检查大数据平台是否有客户数据的管理权限，是否有相关的授权	大数据客户根据账号创建子账号，提供大数据平台或第三方使用，客户可对子账号进行授权和收回	符合情况：只有在客户授权下，大数据平台或第三方才具有客户数据管理权限； 部分符合情况：存在部分数据管理权限无需客户授权，大数据平台或第三方即可进行管理。 不符合情况：大数据平台或第三方未经客户授权即具有对客户数据管理权限。
	[重要]b)大数据系统应提供数据分类分级标识功能；	根据数据在系统中的重要性、功能性对数据进行分类、分级，便于数据的流转和管理等。	1)核查大数据系统建设文档，是否具有数据分类分级机制。 2)访谈管理员或者登录系统核查，是否具有相应功能。	大数据系统具有数据分类分级的相关要求，并按照要求建设。	符合情况：大数据系统具有分类分级标识功能； 不符合情况：大数据系统不具有分类分级标识功能；

访问控制	[关键]c)应在数据采集、传输、存储、处理、交换及销毁等各个环节，根据数据分类分级标识对数据进行不同处置，最高等级数据的相关保护措施不低于第三级安全要求,安全保护策略在各环节保持一致；	数据在一个完整的生命周期内，根据数据分类分级标识采取不同的处置措施。根据数据的级别，对最高等级的数据安全保护采取对应级别的防护措施，在数据各个环节，安全保护措施一致。	1)核查大数据系统建设文档，是否具有数据分类分级机制，是否根据数据级别制定相应的安全保护策略； 2)访谈管理员或者登录系统核查，是否具有相应功能。	大数据系统具有数据分类分级的相关要求，并按照数据的级别制定相应的安全保护措施。	符合情况：大数据系统具有分类分级标识功能，并根据数据的级别采取不同的安全保护策略； 部分符合情况：大数据系统具有分类分级标识功能，未根据数据的级别采取不同的安全保护策略； 不符合情况：大数据系统不具有分类分级标识功能，未对数据进行安全防护；
	[重要]d)大数据系统应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；	大数据系统应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；	1)核查大数据系统建设文档，是否具有数据分类分级机制，是否根据数据级别制定相应的安全保护策略； 2)访谈管理员或者登录系统核查，是否具有相应功能。	大数据系统具有数据分类分级的相关要求，并按照数据的级别制定相应的安全保护措施。	符合情况：大数据系统具有分类分级标识功能，并根据数据的级别采取不同的安全保护策略； 部分符合情况：大数据系统具有分类分级标识功能，未根据数据的级别采取不同的安全保护策略； 不符合情况：大数据系统不具有分类分级标识功能，未对数据进行安全防护；
	[重要]e)应最小化各类接口操作权限；	最小化各类接口操作权限；	1)核查大数据系统建设文档，是否对各类接口的操作权限进行限制； 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，最小化各类接口操作权限； 2)登录系统核查，具有相应功能。	符合情况：大数据系统最小化各类接口的操作权限； 不符合情况：大数据系统未最小化各类接口的操作权限；
	[重要]f)应最小化数据使用、分析，导出、共享、交换的数据集；	最小化数据使用、分析，导出、共享、交换的数据集；	1)核查大数据系统建设文档，是否最小化数据使用、分析，导出、共享、交换的数据集； 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，最小化数据使用、分析，导出、共享、交换的数据集； 2)访谈管理员或者登录系统核查，是否具有相应功能。	符合情况：大数据系统最小化数据使用、分析，导出、共享、交换的数据集； 不符合情况：大数据系统未最小化数据使用、分析，导出、共享、交换的数据集；
	[重要]g)大数据系统应提供隔离不同客户应用数据资源的能力；	客户应用数据资源为该客户的私有数据，数据资源之间需要进行隔离防护。	1)核查大数据系统建设文档，是否具有隔离不同客户应用数据资源的能力； 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，具有隔离不同客户应用数据资源的能力； 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据系统提供隔离不同客户应用数据资源的能力； 不符合情况：大数据系统不能提供隔离不同客户应用数据资源的能力；
	[一般]h)应对重要数据的数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警，并能够对突发的严重异常操作及时定位和阻断。	需要对重要数据的数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警，并能够对突发的严重异常操作及时定位和阻断。	1)核查大数据系统建设文档，是否对重要数据的数据流转、泄露和滥用情况进行监控，发生异常时能否定位和阻断； 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，能够对重要数据的数据流转、泄露和滥用情况进行监控，发生异常时能定位和阻断； 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据系统对重要数据的数据流转、泄露和滥用情况进行监控，发现异常时能够定位和阻断； 部分符合情况：大数据系统对重要数据的数据流转、泄露和滥用情况进行监控，发现异常时不能够定位和阻断； 不符合情况：大数据系统无法对重要数据的数据流转、泄露和滥用情况进行监控；

安全审计	[一般]a)大数据系统应保证不同客户的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力；	对不同客户的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力；	1)核查大数据系统建设文档，是否对不同客户的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力； 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，对不同客户的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力； 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据系统对不同客户的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力； 不符合情况：大数据系统未对不同客户的审计数据隔离存放，并未提供不同客户审计数据收集汇总和集中分析的能力；
	[重要]b)大数据系统应对其提供的各类接口的调用情况以及各类账号的操作情况进行审计；	数据系统需要对其提供的各类接口的调用情况以及各类账号的操作情况进行审计；	1)核查大数据系统建设文档，是否对其提供的各类接口的调用情况以及各类账号的操作情况进行审计； 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，对其提供的各类接口的调用情况以及各类账号的操作情况进行审计； 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据系统对其提供的各类接口的调用情况以及各类账号的操作情况进行审计； 不符合情况：大数据系统未对其提供的各类接口的调用情况以及各类账号的操作情况进行审计；
	[重要]d)应保证大数据系统服务商对服务客户数据的操作可被服务客户审计。	大数据服务商应在客户授权后才能够对云客户系统和数据的访问,为避免大数据服务商的恶意访问,云客户应采取审计机制，对大数据服务商的操作行为进行审计，以避和及时发现违规的操作	1)访谈大数据服务商是否允许访问客户系统和数据 2)是否采取了相关的审计机制，能够记录大数据服务商对客户系统和数据的操作，并核查审计记录的有效性	1）大数据服务商对客户系统的操作需提交工单，使用大数据服务客户的账户，相关操作行为通过客户的管理平平台进行审计	符合情况：大数据系统服务商对服务客户数据的操作可被服务客户审计。 不符合情况：大数据系统服务商对服务客户数据的操作不可被服务客户审计。
入侵防范	[重要]a)应对所有进入系统的数据进行检测，避免出现恶意数据输入。	对所有进入系统的数据进行检测，避免出现恶意数据输入。	1)核查大数据系统建设文档，是否对所有进入系统的数据进行检测，避免出现恶意数据输入。 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，对所有进入系统的数据进行检测，避免出现恶意数据输入。 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据系统对所有进入系统的数据进行检测，避免出现恶意数据输入。 不符合情况：大数据系统未对所有进入系统的数据进行检测。
数据完整性	[重要]a)应采用技术手段对数据交换过程进行数据完整性检测；	为确保数据交换过程中的完整性，防止数据遭受篡改，应采用加密技术或手段对数据交换过程进行防护。	1)核查数据交换过程是否采用校验码或密码技术 2)测试采用的校验码技术或密码技术是否能够保证数据在交换过程中的完整性	保证数据交换过程通过密码机进行加密传输，实现了源机与目标机的数据同步，保证数据交换的完整性	符合情况：采用加密技术手段等对数据交换过程进行数据完整性检测； 不符合情况：未采用技术手段等对数据交换过程进行数据完整性检测；
	[重要]b)数据在存储过程中的完整性保护应满足数据提供方系统的安全保护要求。	为确保数据存储过程中的完整性，防止数据遭受篡改，应采用加密技术或手段对数据存储过程进行防护。	1)核查数据存储过程是否采用校验码或密码技术 2)测试采用的校验码技术或密码技术是否能够保证数据在存储过程中的完整性	保证数据交换过程通过密码机进行加密传输，实现了源机与目标机的数据同步，保证数据存储的完整性	符合情况：采用加密技术手段等对数据存储过程进行数据完整性保护； 不符合情况：未采用技术手段等对数据存储过程进行数据完整性保护；
	[重要]a)大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；	大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；	1)核查大数据系统建设文档，是否提供静态脱敏和去标识化的工具或服务组件技术。 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，提供静态脱敏和去标识化的工具或服务组件技术。 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台提供静态脱敏和去标识化的工具或服务组件技术； 不符合情况：大数据平台未提供静态脱敏和去标识化的工具或服务组件技术；
	[关键]b)应依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理；	依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理；	1)核查大数据系统建设文档，是否依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理； 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理； 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理； 不符合情况：大数据平台未依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理；

数据保密性	[重要]c)数据在存储过程中的保密性保护应满足数据提供方系统的安全保护要求;	为确保数据存储过程中的保密性，防止数据遭受泄露，应采用加密技术或手段对数据存储过程进行防护。	1)核查数据存储过程是否采用校验码或密码技术 2)测试采用的校验码技术或密码技术是否能够保证数据在存储过程中的保密性	保证数据存储过程通过密码机进行加密存储，实现了源机与目标机的数据同步，保证数据存储的保密性	符合情况：采用加密技术手段等对数据存储过程进行数据保密性保护; 不符合情况：未采用技术手段等对数据存储过程进行数据保密性保护;
	[重要]d)应采取技术措施保证汇聚大量数据时不暴露敏感信息;	采取技术措施保证汇聚大量数据时不暴露敏感信息，对敏感数据进行静态脱敏和去标识化处理	1)核查大数据系统建设文档，是否采取技术措施保证汇聚大量数据时不暴露敏感信息; 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，采取技术措施保证汇聚大量数据时不暴露敏感信息; 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：采取技术措施保证汇聚大量数据时不暴露敏感信息，对敏感数据进行静态脱敏和去标识化处理 不符合情况：未采取技术措施保证汇聚大量数据时不暴露敏感信息
	[一般]e)可采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。	采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。	1)核查大数据系统建设文档，是否采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。 不符合情况：未采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。
数据备份恢复	[重要]a)备份数据应采取与原数据一致的安全保护措施;	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。本条款要求备份数据应采取与原数据一致的安全保护措施	1)访谈管理员备份数据和原数据采取何种安全保护措施。	备份数据与原数据采用一致的安全保护措施;	符合情况：备份数据与原数据采用一致的安全保护措施。 不符合情况：备份数据与原数据未采用一致的安全保护措施;
	[关键]b)大数据平台应保证用户数据存在若干个可用的副本，各副本之间的内容应保持一致;	本条款要求大数据平台提供用户数据可存在多个可用的副本，各副本之间的内容应保持一致;	1)核查大数据系统建设文档，是否保证用户数据存在若干个可用的副本，各副本之间的内容应保持一致; 2)访谈管理员或者登录系统核查，是否具有相应功能。	大数据平台提供用户数据可存在多个可用的副本，各副本之间的内容应保持一致;	符合情况：大数据平台保证用户数据存在若干个可用的副本，各副本之间的内容保持一致; 不符合情况：大数据平台无法保证用户数据存在若干个可用的副本;
	[重要]c)应提供对关键溯源数据的异地备份。	应提供灾备中心，对重要的数据（溯源数据）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	询问管理员，是否提供异地实时备份功能，并通过网络将重要数据实时备份至备份场地	供异地实时备份功能，并通过网络将重要数据实时备份至备份场地	符合情况：大数据平台对关键溯源数据异地备份; 不符合情况：大数据平台未对关键溯源数据异地备份;
剩余信息保护	[一般]a)大数据平台应提供主动迁移功能，数据整体迁移的过程中应杜绝数据残留;	大数据平台提供主动迁移功能，数据整体迁移的过程中应杜绝数据残留;	1)核查大数据系统建设文档，是否提供主动迁移功能，采取何种措施防止数据残留; 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，提供主动迁移功能，采取措施防止数据残留; 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台提供主动迁移功能，数据整体迁移的过程中防止数据残留; 不符合情况：大数据平台提供主动迁移功能，数据整体迁移的过程中未防止数据残留;
	[重要]b)应基于数据分类分级保护策略，明确数据销毁要求和方式;	基于数据分类分级保护策略，明确数据销毁要求和方式;	1)核查大数据系统建设文档，是否基于数据分类分级保护策略，明确数据销毁要求和方式; 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，基于数据分类分级保护策略，明确数据销毁要求和方式; 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台基于数据分类分级保护策略，明确数据销毁要求和方式; 不符合情况：大数据平台未基于数据分类分级保护策略，明确数据销毁要求和方式;

	[重要]c)大数据平台应能够根据服务客户提出的数据销毁要求和方式实施数据销毁。	根据服务客户提出的数据销毁要求和方式实施数据销毁。	1)核查大数据系统建设文档，是否能够根据服务客户提出的数据销毁要求和方式实施数据销毁。 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，能够根据服务客户提出的数据销毁要求和方式实施数据销毁。 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台能够根据服务客户提出的数据销毁要求和方式实施数据销毁。 不符合情况：大数据平台不能够根据服务客户提出的数据销毁要求和方式实施数据销毁。
个人信息保护	[关键]a)采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内,并保留操作审计记录;	本条款要求采集、处理、使用、转让、共享、披露个人信息在个人信息处理的授权同意范围内,并保留操作审计记录;	1)核查大数据系统建设文档，是否在个人信息处理的授权同意范围内,并保留操作审计记录; 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，采集、处理、使用、转让、共享、披露个人信息在个人信息处理的授权同意范围内,并保留操作审计记录; 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台采集、处理、使用、转让、共享、披露个人信息在个人信息处理的授权同意范围内,并保留操作审计记录; 不符合情况：大数据平台采集、处理、使用、转让、共享、披露个人信息未在个人信息处理的授权同意范围内,未保留操作审计记录;
	[重要]b)应采取措施防止在数据处理、使用、分析、导出、共享、交换等过程中识别出个人身份信息;	在数据处理、使用、分析、导出、共享、交换等过程中防止识别出个人身份信息;	1)核查大数据系统建设文档，是否采取措施防止在数据处理、使用、分析、导出、共享、交换等过程中识别出个人身份信息; 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，采取措施防止在数据处理、使用、分析、导出、共享、交换等过程中识别出个人身份信息; 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台采取措施在数据处理、使用、分析、导出、共享、交换等过程中防止识别出个人身份信息; 不符合情况：大数据平台未采取措施在数据处理、使用、分析、导出、共享、交换等过程中防止识别出个人身份信息;
	[重要]c)对个人信息的重要操作应设置内部审批流程，审批通过后才能对个人信息进行相应的操作;	本条款要求针对个人信息的重要操作设置内部审批流程，审批允许后方能操作	1)核查大数据系统建设文档，是否对个人信息的重要操作设置内部审批流程 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，对个人信息的重要操作设置内部审批流程 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台对个人信息的重要操作设置内部审批流程 ，批准后方可操作; 不符合情况：大数据平台未对个人信息的重要操作设置内部审批流程 ;
	[重要]d)保存个人信息的时间应满足最小化要求，并能够对超出保存期限的个人信息进行删除或匿名化处理。	大数据系统对个人信息的保存具有一定的期限要求。对超出保存期限的个人信息进行删除或匿名化处理。	1)核查大数据系统建设文档，是否对保存个人信息的时间进行限制，对超出期限的个人信息如何处理; 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，对保存个人信息的时间进行限制，对超出期限的个人信息进行删除; 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台对保存个人信息的时间进行限制，对超出期限的个人信息进行删除; 不符合情况：大数据平台未对保存个人信息的时间进行限制，未对超出期限的个人信息进行删除
数据溯源	[关键]a)应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程;	本条款要求跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程;	1)核查大数据系统建设文档，是否跟踪和记录数据采集、处理、分析和挖掘等过程; 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，大数据平台跟踪和记录数据采集、处理、分析和挖掘等过程; 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台跟踪和记录数据采集、处理、分析和挖掘等过程; 不符合情况：大数据平台未跟踪和记录数据采集、处理、分析和挖掘等过程
	[重要]b)溯源数据应满足数据业务要求和合规审计要求;	溯源数据满足数据业务要求和合规审计要求;	1)核查大数据系统建设文档，溯源数据是否满足数据业务要求和合规审计要求; 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，溯源数据满足数据业务要求和合规审计要求; 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台溯源数据满足数据业务要求和合规审计要求; 不符合情况：大数据平台溯源数据不满足数据业务要求和合规审计要求

	[一般]c)应采取技术手段保证数据源的真实可信。	本条款要求采用技术手段保护数据源的真实可信。	1)核查大数据系统建设文档，是否采取技术手段保证数据源的真实可信。 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，采取技术手段保证数据源的真实可信。 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台采取技术手段保证数据源的真实可信。 不符合情况：大数据平台未采取技术手段保证数据源的真实可信。
系统管理	[一般]a)大数据平台应为服务客户提供管理其计算和存储资源使用状况的能力；	本条款要求大数据平台为服务客户提供管理其计算和存储资源使用状况的能力；	1)核查大数据系统建设文档，是否为服务客户提供管理其计算和存储资源使用状况的能力； 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，为服务客户提供管理其计算和存储资源使用状况的能力； 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台为服务客户提供管理其计算和存储资源使用状况的能力； 不符合情况：大数据平台未为服务客户提供管理其计算和存储资源使用状况的能力；
	[重要]b)大数据平台应对其提供的辅助工具或服务组件实施有效管理；	本条款要求大数据平台对其提供的辅助工具或服务组件实施有效管理；	1)核查大数据系统建设文档，是否对其提供的辅助工具或服务组件实施有效管理； 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，对其提供的辅助工具或服务组件实施有效管理； 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台对其提供的辅助工具或服务组件实施有效管理； 不符合情况：大数据平台未对其提供的辅助工具或服务组件实施有效管理；；
	[重要]c)大数据平台应屏蔽计算、内存、存储资源故障,保障业务正常运行；	本条款要求大数据平台屏蔽计算、内存、存储资源故障；	1)核查大数据系统建设文档，是否屏蔽计算、内存、存储资源故障； 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，屏蔽计算、内存、存储资源故障； 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台屏蔽计算、内存、存储资源故障； 不符合情况：大数据平台未屏蔽计算、内存、存储资源故障；
	[一般]d)大数据平台在系统维护、在线扩容等情况下,应保证大数据应用和大数据资源的正常业务处理能力。	本条款要求大数据平台在系统维护、在线扩容等情况下,保证大数据应用和大数据资源的正常业务处理能力。	1)核查大数据系统建设文档，是否在系统维护、在线扩容等情况下,保证大数据应用和大数据资源的正常业务处理能力。 2)访谈管理员或者登录系统核查，是否具有相应功能。	1)核查大数据系统建设文档，在系统维护、在线扩容等情况下,保证大数据应用和大数据资源的正常业务处理能力。 2)访谈管理员或者登录系统核查，具有相应功能。	符合情况：大数据平台在系统维护、在线扩容等情况下，保证大数据应用和大数据资源的正常业务处理能力。 不符合情况：大数据平台不能保证大数据应用和大数据资源的正常业务处理能力。
集中管控	[重要]a)应对大数据系统提供的各类接口的使用情况进行集中审计和监测，并在发生问题时提供报警。	为便于大数据服商和大数据客户能够及时掌握系统运行情况，对提供的各类接口的使用情况进行集中审计和监测	1)检查大数据平台是否对提供的各类接口的使用情况进行集中审计和监测	大数据平台能够对提供的各类接口的使用情况进行集中审计和监测	符合情况：能够对提供的各类接口的使用情况进行集中审计和监测，并在发生问题时提供报警。 部分符合情况：能够对部分提供的各类接口的使用情况进行集中审计和监测 不符合情况：不能够对提供的各类接口的使用情况进行集中审计和监测
安全策略	[重要]a)应制定大数据安全工作的总体方针和安全策略,阐明本机构大数据安全工作的目标、范围、原则和安全框架等相关内容；	本条款要求制定大数据安全工作的总体方针和安全策略,阐明本机构大数据安全工作的目标、范围、原则和安全框架等相关内容；	1)访谈管理员是否制定大数据安全工作的总体方针和安全策略，是否阐明本机构大数据安全工作的目标、范围、原则和安全框架等相关内容 2）查阅机构安全管理制度，是否具有相关制度	1)制定大数据安全工作的总体方针和安全策略，是否阐明本机构大数据安全工作的目标、范围、原则和安全框架等相关内容 2）查阅机构安全管理制度，具有相关制度	符合情况：制定大数据安全工作的总体方针和安全策略,阐明机构大数据安全工作的目标、范围、原则和安全框架等相关内容； 部分符合情况：制定大数据安全工作的总体方针和安全策略,未阐明机构大数据安全工作的目标、范围、原则和安全框架等相关内容； 不符合情况：未制定大数据安全工作的总体方针和安全策略

安全策略	[关键]b)大数据安全策略应覆盖数据生命周期相关的数据安全，内容至少包括目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。	本条款要求大数据安全策略覆盖数据生命周期相关的数据安全	1)访谈管理员是否制定大数据安全策略，以及安全策略内容 2）查阅机构安全管理制度，是否具有相关制度	1)访谈管理员制定大数据安全策略，以及安全策略内容包括目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等 2）查阅机构安全管理制度，具有相关制度	符合情况：大数据安全策略覆盖数据生命周期相关的数据安全，内容包括目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等； 部分符合情况：大数据安全策略覆盖数据生命周期相关的数据安全，内容不全面 不符合情况：未制定大数据安全策略
授权和审批	[关键]a)数据的采集应获得数据源管理者的授权，确保符合数据收集最小化原则；	数据的采集获得数据源管理者的授权，确保符合数据收集最小化原则；	1）查阅机构安全管理制度，是否具有相关制度	具有相关制度，要求数据的采集应获得数据源管理者的授权	符合情况：数据的采集需获得数据源管理者的授权 不符合情况：未制定相关的安全制度，未对数据的采集进行要求规范。
	[关键]b)应建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程，赋予数据活动主体的最小操作权限、最小数据集和权限有效时长，依据流程实施相关控制并记录过程，及时回收过期的数据访问权限；	本条款要求建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程，赋予数据活动主体的最小操作权限、最小数据集和权限有效时长，依据流程实施相关控制并记录过程，及时回收过期的数据访问权限；	1）查阅机构安全管理制度，是否具有相关制度；	具有相关制度，赋予数据活动主体的最小操作权限、最小数据集和权限有效时长，依据流程实施相关控制并记录过程，及时回收过期的数据访问权限；	符合情况：建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程 不符合情况：未建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程
	[重要]c)应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。	本条款要求的是是否对跨境数据的评估、监督、审批管理等	1）查阅机构安全管理制度，是否具有相关制度以及相应的评估、审批和监督记录。	建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程	符合情况：建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程，保留有相关记录 不符合情况：未建立跨境数据的评估、审批及监管控制流程
审核和检查	[一般]a)应定期对个人信息安全保护措施的有效性进行常规安全检查。	由于个人信息的重要性，对个人信息保护的关注日益提升，大数据平台提供个人信息保护机制。	1）访谈管理员是否制定有个人信息保护安全措施，检查安全保护措施是否有效。	1）制定有个人信息保护安全措施，安全保护措施有效，具有检查记录。	符合情况：制定有个人信息保护安全措施，定期检查安全保护措施有效，具有检查记录 部分符合情况：　制定有个人信息保护安全措施，未定期进行检查（安全保护措施无效） 不符合情况：未制定有个人信息保护安全措施

服务供应商选择	[重要]a)应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用和大数据资源提供相应等级的安全保护能力；	为确保大数据服务商提供的服务符合安全性需求，大数据客户应当选取安全合规的大数据服务商，且大数据服务商提供的安全保护能力等级应具有相应的或高于业务应用系统需求的安全防护能力	1)访谈系统建设负责人确认选择的大数据服务提供商提供的大数据平台的安全服务等级，并核查大数据平台的安全防护等级 2)访谈管理员，大数据应用和大数据资源的安全防护等级 3)核查大数据服务商提供商提供的大数据平台的安全防护能力能够满足需求	大数据服务商提供大数据平台安全保护等级说明，大数据平台安全保护等级具有相应或高于大数据应用和大数据资源所需求的安全防护能力	符合情况：提供大数据平台安全保护等级说明，大数据平台安全保护等级具有相应或高于大数据应用和大数据资源系统所需求的安全防护能力 不符合情况：不提供大数据平台安全保护等级说明，大数据平台安全保护等级具有相应或低于业务应用系统所需求的安全防护能力
	[重要]b)应以书面方式约定大数据平台提供者和大数据平台使用者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。	大数据平台服务商与大数据客户签订协议 ,协议的内容可能会因不同的大数据服务 客户、业务类型、服务形式等发生很大变化。协议内容应尽可能全面的包括信息安全管理需求，明确大数据服务商所提供的服务内容以及大数据服务商需提供的技术指标	1)核查是否与大数据服务商签订服务水平协议或服务合同 2)检查服务水平协议或服务合同的内容是否对大数据服务商所提供的服务内容和需提供的技术指标进行规定	1)大数据服务商与大数据客户签订文本 2)文本内容包括了大数据服务商所提供的服务内容和需提供的技术指标	符合情况：大数据平台提供者和大数据平台使用者签订有合同，明确双方权限与责任、各项服务内容和具体技术指标等； 不符合情况：大数据平台提供者和大数据平台使用者签订有合同，未规定权限与责任、各项服务内容和具体技术指标等
供应链管理	a）应确保供应商的选择符合国家有关规定	在安全产品采购和使用、安全服务提供商选择以及云服务商的选择时，应确保符合国家有关规定要求。如《公安部关于加强信息网络安全检测产品销售和使用通知》，《含有密码技术的信息产品政府采购规定》等，此外部分特殊行业，如金融、电力、能源等。也对安全产品的采购和使用有规定。 大数据平台服务商在选择安全服务提供商时，应充分考虑国家法律法规、行业规范等要求，以保持大数据平台安全服务的持续性和合规性，如(商用密码管理条例》规定，商用密码产品发生故障， 必须由国家密码管理机构制定的单位维修	1)访谈确认选择的大数据服务商 2)核查大数据服务商提供的产品或服务清单，检查供应商的选取是否满足国家有关规定，如查阅安全产品的销售许可证、提供加密服务的资质	服务商提供的产品或服务清单符合规定，供应商的选取满足国家有关规定，如查阅安全产品的销售许可证、提供加密服务的资质	符合情况：提供的产品或服务清单符合规定，供应商的选取满足国家有关规定，如查阅安全产品的销售许可证、提供加密服务的资质 部分符合情况：提供的产品或服务清单部分符合规定，供应商的选取部分满足国家有关规定，如查阅安全产品的销售许可证、提供加密服务的资质　　不符合情况：提供的产品或服务清单不符合规定，供应商的选取不满足国家有关规定，如查阅安全产品的销售许可证、提供加密服务的资质
	[一般]b)应以书面方式约定数据交换、共享的接收方对数据的保护责任，并明确数据安全保护要求；	本条款要求的是数据交换、共享的接收方对数据的保护责任，并明确数据安全保护要求；	1)访谈确认选择的大数据服务商 2)核查书面文件，是否明确接收方对数据的保护责任	核查书面文件，明确接收方对数据的保护责任	符合情况：以书面方式约定数据交换、共享的接收方对数据的保护责任； 不符合情况：未以书面方式约定数据交换、共享的接收方对数据的保护责任，

	[一般]c)应将供应链安全事件信息或安全威胁信息及时传达到数据交换、共享的接收方。	大数据服务商应及时向大数据接收方及相关供应商通报安全事件，保障其知情权的同时作为风险评估的输入(如影响服务正常提供或涉及敏感信息泄露等重大问题),应及时向相关方提供信息，便于采取相应的应对措施	1)核查大数据服务商是否定期向数据接收方客户通报安全事件 2)检查是否有相关的供应链安全事件报告或威胁报告 3)核查供应链安全事件报告或威胁报告，查看事件报告是否及时，报告内容是否能够明确相关事件信息或威胁信息	大数据服务商推送最新的安全事件信息，以保证第一时间传达给数据接收方	符合情况：大数据平台推送最新的安全事件信息，以保证第一时间传达给数据接收方 不符合情况：大数据平台不推送最新的安全事件信息，不保证第一时间传达给数据接收方
数据源管理	[一般]a)应通过合法正当的渠道获取各类数据。	本条款要求的是保证数据来源的合法性。	1)访谈管理员，各类数据来源渠道是否合法合规	数据通过合法正当的途径获取。	符合情况：通过合法正当的渠道获取各类数据。 不符合情况：未通过合法正当的渠道获取各类数据
资产管理	[一般]a)应建立数据资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程；	本条款要求建立数据资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定	1)访谈管理员，是否对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定； 2）核查机构相关管理制度，是否具有相关规定。	1)访谈管理员，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定； 2）核查机构相关管理制度，具有相关规定。	符合情况：建立数据资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定 不符合情况：未建立数据资产安全管理策略，未对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定
	[关键]b)应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定相应强度的安全保护要求；	制定并执行数据分类分级保护策略，针对不同类别级别的数据制定相应强度的安全保护要求；	1)访谈管理员，是否制定并执行数据分类分级保护策略 2）核查机构相关管理制度，是否具有相关规定。	1)访谈管理员，制定并执行数据分类分级保护策略，并针对不同类别级别的数据制定相应强度的安全保护要求； 2）核查机构相关管理制度，具有相关规定。	符合情况：制定并执行数据分类分级保护策略，并针对不同类别级别的数据制定相应强度的安全保护要求 不符合情况：未制定并执行数据分类分级保护策略，并针对不同类别级别的数据制定相应强度的安全保护要求
	[重要]c)应定期评审数据的类别和级别，如需要变更数据所属类别或级别，应依据变更审批流程执行变更；	定期评审数据的类别和级别，如需要变更数据所属类别或级别，应依据变更审批流程执行变更；	1)访谈管理员，是否定期评审数据的类别和级别 2）核查机构相关管理制度，是否具有相关规定。	1)访谈管理员，定期评审数据的类别和级别 2）核查机构相关管理制度，具有相关规定。	符合情况：定期评审数据的类别和级别 不符合情况：未定期评审数据的类别和级别
	[一般]d)应对数据资产和对外数据接口进行登记管理，建立相应的资产清单。	对数据资产和对外数据接口进行登记管理，建立相应的资产清单	1)访谈管理员，是否对数据资产和对外数据接口进行登记管理，建立相应的资产清单 2）核查机构相关管理制度，是否具有相关规定。	1)访谈管理员，对数据资产和对外数据接口进行登记管理，建立相应的资产清单 2）核查机构相关管理制度，具有相关规定。	符合情况：对数据资产和对外数据接口进行登记管理，建立相应的资产清单 不符合情况：未对数据资产和对外数据接口进行登记管理，建立相应的资产清单

介质管理	[重要]a)应在中国境内对数据进行清除或销毁；	网络安全法》第三十七条规定，基础设施运营者在中国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因此清除或销毁也应在中国境内。	1）访谈管理员或者检查数据清除和销毁措施。 2）数据是否发送境外	1)机房的部署、数据存储位置均位于中国境内 2)制定有数据清除和销毁制度，要求数据的清除和销毁必须在中国境内	符合情况：机房的部署、数据存储位置均位于中国境内；数据清除和销毁在本地完成。 不符合情况：未在中国境内对数据进行清除或销毁；
	[一般]b)对存储重要数据的存储介质或物理设备应采取难恢复的技术手段，如物理粉碎、消磁、多次擦写等。	本条款要求对存储有重要数据的存储介质或者物理设备采取难以恢复的物理手段进行处理，如物理粉碎、擦写写零、消磁等	1）访谈管理员或者检查是否制定有介质管理制度，是否具有针对介质中重要数据处理的描述。 2）是否具有介质粉碎、消磁的记录等。	1)制定有介质管理制度，并对具有重要数据的介质或设备进行要求。	符合情况：制定有介质管理制度，对存储重要数据的存储介质或物理设备采取难恢复的技术手段，如物理粉碎、消磁、多次擦写等。 不符合情况：制定有介质管理制度。
网络和系统安全管理	[关键]a)应建立对外数据接口安全管理机制，所有的接口调用均应获得授权和批准。	大数据平台制定有对外数据接口安全管理制度和机制，规定接口的调用需要获得授权和批准。	1）访谈管理员或者检查是否制定有相关的安全管理制度，是否具有接口调用的授权审批记录等。	1)建立有对外数据接口安全管理机制，要求接口的调用需要授权和审批。	符合情况：建立有对外数据接口安全管理机制，要求接口的调用需要授权和审批 ，具有授权和批准记录。 不符合情况：未建立对外数据接口安全管理机制。