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	

云计算安全拓展要求（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	应保证云计算基础设施位于中国境内	云服务商对机房选址时，应确保机房位于中国境内、确保云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位位于中国境内	1)访谈并查阅最新的机房清单 2)核查云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	部署整个云计算环境的机房云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均位于中国境内	符合情况：机房位于中国境内 不符合情况：机房位于中国境外
网络架构	a)应保证云计算平台不承载高于其安全保护等级的业务应用系统	云服务方侧的云计算平台单独作为定级对象定级,云租户侧等级保护对象也应作为单独的定级对象定级,云平台的等级要不低于云上租户的业务应用系统最高级	1)查看云平台备案证及云客户系统定级备案材料 2)核实是否存在客户业务应用系统等级高于平台等级的情况	1)提供云平台备案证 2)云客户业务系统安全保护等级不高于云计算平台/系统的安全保护等级	符合情况：云平台具有备案证且云客户系统等级等于或低于云平台安全保护等级 不符合情况：云客户系统等级高于云平台安全保护等级
	b)应实现不同云服务客户虚拟网络之间的隔离	同一个物理主机上的虚拟机间可能通过硬件背板、不同物理机上的虚拟机可能通过网络进行通信，这些通信流量对传统的网络安全控制而言是不可见的，无法进行监控或封堵，为防止多租户间的相互影响及恶意攻击，确保租户安全及云平台安全，应对不同的云服务客户网络间进行有效的网络隔离，以保证云服务客户的访问与其他租户能够实现有效隔离	1)核查不同云客户间是否采取隔离手段或措施(如单独VPC、云防火墙、安全组)。	1)云服务客户系统/该系统部署在独立VPC中； 2）不同云服务客户通过云防火墙进行网络隔离； 3）不同云服务客户通过安全组进行网络隔离。	符合情况：云服务客户系统/该系统部署在独立VPC中；不同云服务客户通过云防火墙进行网络隔离 ;不同云服务客户通过安全组进行网络隔离. 。 不符合情况：云服务客户系统/该系统未部署在独立VPC中；不同云服务客户未通过云防火墙进行网络隔离 ;不同云服务客户未通过安全组进行网络隔离.
	c)应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范制等安全机制的能力	为应对源自各个层面的攻击，云服务商应该为云服务客户提供通信传输、边界防护、入侵防范等安全防护措施，云服务客户可根据业务安全防护需求选择适当的安全防护措施，提升业务系统的安全防护能力以应对外来的威胁攻击	1)核查云服务商提供的通信传输、边界防护、入侵防范等安全防护措施，并检查安全措施形成的安全防护能力 2)云服务商提供的通信传输、边界防护、入侵防范等安全防护能力是否能满足云服务客户业务需求	1)云服务商提供通信传输、边界防护、入侵防范等对应云安全产品或安全服务；	符合情况： 云服务商提供通信传输、边界防护、入侵防范等对应云安全产品或安全服务 部分符合情况：云服务商提供通信传输、边界防护、入侵防范等部分功能的云安全产品或安全服务 不符合情况：云服务商未提供通信传输、边界防护、入侵防范等对应云安全产品或安全服务
	d)应具有根据云服务客户业务需求自主设置安全策略的能力,包括定义访问路径、选择安全组件、配置安全策略	云服务客户可以根据自身的业务需求,在云服务商提供的安全组件上自定义安全策略，如定义安全访问路径、选择安全组件、配置安全策略	1)访谈云计算平台提供的安全组件有哪些，安全组件是否支持用户自定义 2)核查云服务客户是否能够自定义安全策略，包括定义访问路径、选择安全组件、配置安全策略	云安全产品的配置界面显示可以自主设置安全策略，如定义访问路径、选择安全组件、配置安全策略。	符合情况：云安全产品的配置界面显示可以自主设置安全策略，如定义访问路径、选择安全组件、配置安全策略。 部分符合情况： 云安全产品的配置界面显示可以自主设置部分安全策略 。 不符合情况：云安全产品的配置界面不可以自主设置安全策略。

	e)应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或云计算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，云计算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，因而云服务商应提供开放和公开的APIs,允许第三方安全产品或服务接入	1)访谈云客户是否使用了第三方安全产品或服务; 2)查阅云平台接口设计文档或开放性安全服务文档	1)云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）云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;	符合情况： 云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：云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。
访问控制	a)应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。	位于云平台边界外，云平台缺乏或缺失控制和管理的网络环境，被认为是不可信网络，与之对应的是可信网络，在可信与不可信网络间实施有效的安全控制，对，网络安全来说至关重要。通常使用虚拟防火墙进行可信与不可信网络间的连接控制，通过防火墙的访问控制策略配置，仅允许必要的流量通过，而其他流量均被禁止。虚拟网络边界主要包括云计算平台和云服务客户业务系统虚拟网络边界，不同云服务客户间的网络访问边界、云服务客户不同安全保护等级业务系统间的网络边界。可以防止攻击者通过未授权的IP地址访问可信网络，或以未授权的方式访问服务、协议或端口	1)访谈确认云计算平台的虚拟网络边界处采用的访问控制机制（如NAT网关、SLB、安全组、云防火墙等）; 2）核查具体访问控制规则，是否仅允许必要的流量通过，而其他流量均被禁止。。	1)虚拟网络边界处部署了访问控制措施（如NAT网关、SLB、安全组、云防火墙等）; 2)通过访问控制规则仅允许必要的流量通过，而其他流量均被禁止。	符合情况： 虚拟网络边界处部署了访问控制措施（如NAT网关、SLB、安全组、云防火墙等），通过访问控制规则仅允许必要的流量通过，而其他流量均被禁止。 部分符合情况：虚拟网络边界处部署访问控制措施（如NAT网关、SLB、安全组、云防火墙等），但不能通过访问控制规则仅允许必要的流量通过，而其他流量均被禁止。 不符合情况：虚拟网络边界处未部署访问控制措施（如NAT网关、SLB、安全组、云防火墙等），不能通过访问控制规则仅允许必要的流量通过，而其他流量均被禁止。
	b)应在不同等级的网络区域边界部署访访问控制机制,设置访问控制规则	云平台边界、云平台内网络区域边界、云服务客户不同业务边界将网络划分为不同等级的安全域，结合边界访问控制技术可以实现整个系统的纵深防御，可以减少未授权访问或运行环境交更的风险。因此，应在不同等级的网络区域边界部署访问控制设备，设置访问控制规则	1)访谈并查阅网络拓扑，记录网络安全区域划分情况 2)检查各网络区域边界处采用的安全控制机制，查看访方问控制列表 3)核查访问控制规则是否有效，并测试验证是否能够拒绝不同区域间的非法访问	在不同等级的网络区域边界部署了边界隔离措施（如云防火墙安全组和VPC），并且设置了访问控制规则。	符合情况：在不同等级的网络区域边界部署了边界隔离措施（如云防火墙安全组和VPC），并且设置了访问控制规则。 部分符合情况：在不同等级的部分网络区域边界部署了边界隔离措施（如云防火墙安全组和VPC），但未设置明确的访问控制规则。 不符合情况：未在不同等级的网络区域边界部署边界隔离措施（如云防火墙安全组和VPC），不能设置访问控制规则。

入侵防范	a）应能检测到云服务客户发起的网络络攻击行为，并能记录攻击类型、攻击时时间、攻击流量等	云平台应能够对云服务客户端发起的访问，进行入口流量镜像分析，对东西向、南北向的攻击行为进行深入分析,并结合相关的云安全产品对异常流量的处理。记录攻击类型、攻击时间、攻击流量等	1）访谈云服务商是否采取了入侵防范措施对网络入侵行为进行防范，如部署API攻击系统、网络回溯系统和网络入侵保护系统等入侵防范设备或相关组件，是否能够对云服务客户发起的网络攻击行为进行检测和报警 2)检查相关入侵检测产品规则库是否进行及时更新，对异常流量和未知威胁的监控策略、报警策略是否有效 3)检查相关入侵检测产品产品白皮书及销售许可证	1)部署流量安全监控设备,通过对云入口镜像流量包的深度解析，实时地检测出各种攻击和异常行为 2)虚拟机层面部署防恶意代码软件(如阿里云安骑士》进行基线检查、并对恶意文件进行扫描、恶意进程查杀,并且提供入侵检测功能，规则库定期更新 3)部署主机入侵检测，实时检测云环境中所有物理服务器主机，并及时发现文件篡改、异常进程、异常网络连接、可疑端口监听等行为，规则库定期更新 4)部署态势感知系统，从攻击者的角度有效捕捉高级攻击者使用的0Day漏洞攻击、新型病毒攻击事件，以及有效展示正在发生的安全攻击行为	符合情况： 能检测到云服务客户发起的网络络攻击行为，并能记录攻击类型、攻击时时间、攻击流量等 部分符合情况：能检测到云服务客户发起的网络攻击行为，但未记录攻击类型、攻击时时间、攻击流量等 不符合情况：不能检测到云服务客户发起的网络攻击行为，不能记录攻击类型、攻击时时间、攻击流量等
	b)应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等	在云计算服务的关键节点如虚拟网络节点出入口实施安全防护，部署应用层，防火墙、入侵检测和防御设备以及流量清洗设备来提升网络攻击防范能力，对虚拟 网络节点的网络攻击行为进行检测，并记录攻击类型、攻击时间、攻击流量等	1)检查是否部署网络攻击行为检测设备或相关组件对虚拟网络节点的网络攻击行为进行防范，并能记录攻击类型、攻击时间、攻击流量 2)核查网络攻击行为检测设备或相关组件的规则库是否为最新	1)通过部署的流量安全监控设备对云入口镜像流量包的深度解析，实时地检测出各种攻击和异常行为 2)部署入侵检测设备并记录相关攻击原始日志，检测到攻击行为本地产生告警log,保存至日志服务（log Service)	符合情况： 能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等 部分符合情况：能检测到对虚拟网络节点的网络攻击行为，但未记录攻击类型、攻击时间、攻击流量等。 不符合情况：不能检测到对虚拟网络节点的网络攻击行为，不能记录攻击类型、攻击时间、攻击流量等
	c)应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量	为避免异常流量影响虚拟机与宿主机的正常运行，虚拟机与宿主机、虚拟机与虚拟机间的通信，部署流量监测设备、入侵防护系统等对虚拟机与宿主机、虚拟机与虚拟机之间的流量进行实时监测	1)访谈云计算平台是否具备虚拟机与宿主机之间、虚拟机与虚拟机之间的异常流量的检测功能 2)查看异常流量的监测策略，并测试验证对异常流量的监测策略是否有效	虚拟机与虚拟机之间通过云防火墙，虚拟机与宿主机之间通过流量安全监控，对流量进行检测，发现异常流量进行告警，告警日志同步到日志管理平台进行分析	符合情况：能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量 。 部分符合情况： 能检测到部分虚拟机与宿主机、虚拟机与虚拟机之间的异常流量 不符合情况：不能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量
	d)应在检测到网络攻击行为、异常流量情况时进行告警	部署流量监测设备、入侵防护系统等对网络流量进行分析、检测，当检测到网络攻击行为、异常流量时提供告警机制，及时告知相关人员，避免网络攻击行为、异常流量影响系统正常运行	1)核查网络入侵检测措施有哪些 2)检查在检测到网络攻击行为、异常流量时是否进行告警，并查看相关告警记录	1)采取了流量监控、入侵检测措施， 2)在检测到异常事件时会进行短信或邮件告警。	符合情况：能检测到网络攻击行为、异常流量情况时进行告警 部分符合情况：能检测到网络攻击行为、异常流量情况，但不能进行告警。 不符合情况：不能检测到网络攻击行为、异常流量情况时进行告警

安全审计	a)应对服务商或云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启	对特权命令的操作可能超越系统、实体、网络、虚拟机和应用控制的措施，因而需要对特权命令的执行进行严格控制，使用加以限制并严格控制，并对操作进行审计，以防止出现的滥用和破坏	1)访谈是否部署审计工具对云服务和云服务客户执行特权命令进行审计 2）核查审计记录是否包括虚拟机删除、虚拟机重启	1)通过控制台、堡垒机或其他审计工具对云服务和云服务客户执行特权命令进行审计； 2）核查审计记录是否包括虚拟机删除、虚拟机重启。	符合情况：能通过控制台、堡垒机或其他审计工具对云服务和云服务客户执行特权命令进行审计 部分符合情况：通过控制台、堡垒机或其他审计工具对云服务和云服务客户部分执行特权命令进行审计 不符合情况：不能通过控制台、堡垒机或其他审计工具对云服务和云服务客户执行特权命令进行审计
	b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计	云服务商应在云服务客户授权后才能够对云客户系统和数据的访问,为避免云服务商的恶意访问,云服务客户应采取审计机制，对云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)访谈云服务商是否允许访问云服务客户系统和数据 2)是否采取了相关的审计机制，能够记录云服务商对云服务客户系统和数据的操作，并核查审计记录的有效性	1）云服务商对云服务客户系统的操作需提交工单，使用云服务客户的账户，相关操作行为通过云服务客户的管理平平台进行审计	符合情况：云服务商对云服务客户系统和数据的操作可被云服务客户审计。 部分符合情况：云服务商对云服务客户系统和数据的操作部分可被云服务客户审计 不 符合情况：云服务商对云服务客户系统和数据的操作不可被云服务客户审计
身份鉴别	当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制	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。在远程管理云计算平台中的设备时，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，云计算平台不会被非法入侵,大大的提高了云计算平台和终端设备连接的安全性	1)访谈管理员，当远程管理云计算平台中设备时，管理终端和云计算平台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
访问控制	a)应保证当虚拟机迁移时，访问控制策略随其迁移	虚拟机迁移包括不同云平台间的迁移，以及将云平台中的服务器、应用和数据迁移至本地环境。对于虚拟机迁移而言，若缺乏安全保障措施,监听者可能通过监听源与目标服务器间的网络,获得迁移过程中的全部数据，还可能修改传输数据，植入恶意代码，控制虚拟机。因此,为保证迁移安全，可进行加密传输，或通过链路加密模式，同时将访问控制策略同时迁移，以防止未授权的访问	1)访谈管管理员是否对虚拟机进行计移,迁移采取的方式是什么 2)核查虚拟机迁移的过程中是否将控制策略进行随迁，查看迁移记录	提供虚机迁移后的安全组策略的的前后对比截图	符合情况：虚拟机迁移时，访问控制策略随其迁移 部分符合情况：虚拟机迁移时，访问控制策略部分随其迁移 不符合情况：虚拟机迁移时，访问控制策略不能随其迁移

	b)应允许云服务客户设置不同虚拟机之间的访问控制策略	云平台在同一时间段内，承载多个或大量的的租户。若租户虚拟机间无有效的安全访问控制策略可能导致虚拟机非法访问、租户数据泄露，对于多租户环境下，多个用户共享计算、存储、网络等虚拟资源，若共享模块存在漏洞，租户可对其他租户资源发起攻击，或对自己的其他资源，如虚拟机进行攻击。因此，云计算环境下多租户或同一用户间不同虚拟机间应允许访问	1)访谈管理员，不同虚拟间是否允许配置访问控制记录 2)记录配置的访问控制策略，核实策略是否真实有效	提供安全组、云防火墙的访问控制策略	符合情况：云服务客户能设置不同虚拟机之间的访问控制策略 部分符合情况：云服务客户能设置不同虚拟机之间的部分访问控制策略 不符合情况：云服务客户不能设置不同虚拟机之间的访问控制策略
入侵防范	a)应能检测虚拟机之间的资源隔离失效，并进行告警	1)虚拟机和宿主机共享资源，若虚拟机间的资源、内存和存储空间隔离失效，云服务商未采取相应的应对措施检测恶意行为且无告警措施，可能导致虚拟机非法占用资源，从而导致其他虚拟机无法正常运行。因此，对虚拟机间的资源隔离进行实时监控，并在检测到异常时进行告警,从而降低虚拟机出现异常的风险	1)访谈管理员，实现对虚拟机资源隔离的措施 2)核查是否对虚拟机资源进行监控，是否能够检测到虚拟机资源隔离失效并进行告警	提供虚拟机资源监控、隔离措施、以及入侵告警方式和记录	符合情况：能提供虚拟机资源监控、隔离措施以及入侵告警方式和记录； 部分符合情况：能提供虚拟机资源监控、隔离措施，但未提供入侵告警方式和记录； 不符合情况：不能提供虚拟机资源监控、隔离措施且不能提供入侵告警方式和记录；
	b）应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警	规范虚拟机的管理操作，可强化虚拟化环境安全，所有的虚拟机新建或重启应都由系统管理员来创建和保护，若某些用户(如如开发人员、测试人员和培训中）需重启虚拟机，应通过系统管理员创建和管理或进行授权，为避免虚拟机的非授权创建或重启，应对所有虚拟机的运行状态进行检测，并提供异常报警机制;以便能及时发现虚拟机的非法重建和重启	1)核查非授权用户是否有权限新建或重启虚拟机 2)访资管理员是否采取相关措施对虚拟机的新建或重启进行监视，并对虚拟机的新建或重启行为进行安全审计 3)安全监视工具是否能够对虚拟机的新建或重启操作进行告警	提供新建新建或重启虚拟机的机制，部署安全监视工具对新建或重启虚拟机的操作进行监视、审计，提供违规启停客户虚拟数据安全审计记录，提供告警方式及记录	符合情况：能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警 部分符合情况：能检测非授权新建虚拟机或者重新启用虚拟机，但不能进行告警 不符合情况：不能检测非授权新建虚拟机或者重新启用虚拟机，不能进行告警。
	c)应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警	恶意代码感染可能导致虚拟机无法正常运行或被非法利用，虚拟机被非法利用后，可能被作为跳板机，若无有效的虚拟机隔离技术措施，可能导致恶意代码任宿主机或虚拟机间蔓延,从而破坏整改云计算环境，因此对整个云平台进行恶意代码检测，防止恶意代码的入侵，并对恶意代码的感染和蔓延情况进行监测、告警，降低恶意代码感染的风险和损失	1)检查是否部署安全产品或服务对虚拟机进行恶意代码进行检测，并进行告警 2)检查是否采取虚拟机隔离技术或其其他手段有效防止病毒蔓延整个云环境 3)检查是否采用相关安全措施能够检测恶意代码在虚拟机间的蔓延并进行告警。	部署安全产品或服务对虚拟机进行恶意代码进行检测，并进行日志记录，并进行告警	符合情况：部署安全产品或服务对虚拟机进行恶意代码进行检测，并进行日志记录，并进行告警 部分符合情况：部署安全产品或服务对虚拟机进行恶意代码进行检测，并进行日志记录，但不能进行告警 不符合情况：未部署安全产品或服务对虚拟机进行恶意代码进行检测，并进行日志记录，并进行告警

镜像和快照保护	a)应针对重要业务系统提供加固的操作系统镜像像或操作系统安全加固服务	进行操作系统安全如固，关闭不必要的端口、协议和服务，减少系统的攻击面。云计算环境中，所有操作系统均应进行安全加固处理、仅提供必要的端口、协议和服务，以满足业务需求。防恶意代码软件、文件完整性监控、日志记录均应作为基本的操作系统加固需求。通过安全加固，可提升服务器安全性，防止外来用户和木马病毒对服务器的攻击，保护云平台和云用户安全。应鉴于业内最佳实践，参考国际标准规范形成操作系统安全加固指南或手册,并应用到镜像或操作系统，并及时访问权限进行限制	1)核查云服务商是否提供操作系统安全加固基线或相关安全加固服务 2)检查加固基线是否合规，否对基线进行定期更新	提供带防恶意代码软件镜像模板的说明	符合情况：对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务 不符合情况：不对重要业务系统提供加固的操作系统镜像像或操作系统安全加固服务
	b)应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改	虚拟机镜像、快照无论在静止还是运行状态都有被窃取、篡改或替换的危险，攻击者可能是黑客，也可能是云服务商员工。若无法保证虚拟机镜像、快照的完整性，可能被非法篡改、恶意代码植入，或安全合规配置被更改，导致虚拟机被部署运行时，系统遭受攻击,因此必须保证虚拟机镜像、快照的完整性。虚拟机镜像、快照的完整性主要通过哈希校验的方式实现，一旦发生变化,哈希值将改变，因此,在下一次使用虚拟机镜像或快照时,应进行完整性校验，以保证期间未授权的更改。对虚拟机进行补丁更新或安全配置更改,都应进行审计记录并进行报警。虚拟机镜像、快照的完整性验证结果，应即通过电子的方式告知用户	1)核查是否对虚拟机的变更进行检测， 2)若进行检测空是否有相关的检测记录，发现镜像或快照被变更时，是否提供告警方式	ESC、虚拟机镜像和快照的完整性校验记录、结果	符合情况：提供ESC、虚拟机镜像和快照的完整性校验记录、结果 不符合情况：不提供ESC、虚拟机镜像和快照的完整性校验记录、结果
	c)应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资 被非法访问	数据加密技术是最基本的安全技术，被誉为信息安全的核心。采用密码技术将保护信息置换为密文，在存储或传输过程中，即使被非授权人员获得，也可以保证这些信息不为其所知，从而保护信息。对虚拟机镜像、快照采取密码技术进行加密,可有效的保证存在于镜像、快照中的敏感数据的安全性。此外，通过访问控制的方式，限制用户对虚拟机镜像、快照的非法访问，也可以保护其安全性	1)核查是否对虚拟机镜像、快照进行加密，采用了何种加密技术 2)核查是否采取访问控制或其他措施对虚拟机镜像、快照进行保护	采用加密技术对虚拟机镜像、快照进行加密，保证其在传输、存储过程中的安全性，通过访问控制的方式限制虚拟机镜像、快照被非法访问	符合情况：采用加密技术对虚拟机镜像、快照进行加密，保证其在传输、存储过程中的安全性，通过访问控制的方式限制虚拟机镜像、快照被非法访问 不符合情况：未采用加密技术对虚拟机镜像、快照进行加密，保证其在传输、存储过程中的安全性，通过访问控制的方式限制虚拟机镜像、快照被非法访问

数据完整性和保密性	a)应确保云服务客户数据、用户个大信息等存储于中国境内，如需出境应遵循国家相关规定	《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。为满足网络安全法规定，云服务商 提供的存储机制应保证云服务客户数据、用户个人信息等存储于中国境内,若需 要出境，应当满足国家相关的规定	1)查阅相关文档查看云服务客户数据存储方式，访谈客户业务数据、用户个人信息等存储所在的服务器节点以及与其存储相关的设备是否部署在中国境内的机房 2)核查客户业务数据、个人信息等数据是否存在出境的情况，是否依据国家相关规定制定了数据出境的规定	1)机房的部署、数据存储位置均位于中国境内 2)制定云上数据出境的相关规定，符合国家相关规定的要求	符合情况：机房的部署、数据存储位置均位于中国境内；制定云上数据出境的相关规定，符合国家相关规定的要求 部分符合情况：机房的部署、数据存储位置均位于中国境内；未制定云上数据出境的相关规定； 不符合情况：机房的部署、数据存储位置均位于中国境外；未制定云上数据出境的相关规定；
	b)应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据管理权限	为避免云客户数据的非法访问，对数据的管理权限进行控制，仅允许云服务客户管理员访问，若其他用户(云服务商或第三方用户)需对数据进行管理，必须由云服务客户管理员提供授权，方能进行数据管理	1)核查云服务客户的授权机制，如授权流程、授权方式及授权内容 2)检查云计算平台是否有云服务客户数据的管理权限，是否有相关的授权	云服务客户根据账号创建子账号，提供云服务商或第三方使用，云服务客对子账号进行授权和收回	符合情况：只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据管理权限； 部分符合情况：存在部分数据管理权限无需云服务客户授权，云服务商或第三方即可进行管理。 不符合情况：云服务商或第三方未经云服务客户授权下具有云服务客户数据管理权限。
	c)应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到整性受到破坏时采取必要的恢复措施	为确保虚拟机迁移后业务能够正常切换，迅速进行，必须确保数据在迁移过程中完整性。因此，云服务商应对迁移过程中的数据提供完整性校验措施或或手段，且能够在发现数据完整性遭到破坏时提供恢复措施，来保证业务迁移后正常运行	1)核查虚拟机迁移过程中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迁移过程中的完整性 3)核查采用措施是否能够在完整性受到破坏时，提供相应的恢复手段，保业务正常运行	云服务商提供虚拟机迁移技术，保证迁移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，保证业务正常切换	符合情况：提供虚拟机迁移技术，保证迁移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，保证业务正常切换 部分符合情况：提供虚拟机迁移技术，保证迁移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，但不能检测和恢复。 不符合情况：未提供虚拟机迁移技术，保证迁移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，不能保证业务正常切换
	d)应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程	云计算环境中，云服务商和和用户对密钥管理系统具有不同的所有权和控制权，在云服务中，数据的所有权属于云服务客户，数据却保存在云服务商控制的存储资源上，服务客户可自行部署或采用云服务商提供的密钥管理解决方案，实现数据的加解密，云服务商应支持云客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程	1)核查云服务客户是否部署密钥管理解决方案 2)核查云服务商为云服务客户提供的密钥管理解决方案 3)查阅密钥管理解决方案相关文档，核查部署的密钥密钥管理解决方案是否能够保证云服务客户自行实现数据的加解密过程	云服务商或云客户部署经国家密码管理局检测认证的硬件加密机，云服务客户借助此服务实现对加密密钥的完全控制和对数据进行加解密操作	符合情况：部署经国家密码管理局检测认证的硬件加密机，云服务客户借助此服务实现对加密密钥的完全控制和对数据进行加解密操作 不符合情况：未部署经国家密码管理局检测认证的硬件加密机，云服务客户借助此服务实现对加密密钥的完全控制和对数据进行加解密操作
	a)云服务客户应在本地保存其业务数据的备份	数据丢失会对客户业务造成重大巨大影响，在云计算中，用户数据大部分存在云中，有一定的风险。因此，云用户(租户)应将业务数据本地保存备份，防止数据意外丢失	1)核查云服务商是否支持云服务客户将数据本地备份保存 2)检测云服务客户是否对业务数据进行本地备份保存	提供支持open API的说明，云服务商支持云客户本地保存业务数据备份、转存，并有数据备份记录	符合情况：云客户本地保存业务数据备份、转存，并有数据备份记录 部分符合情况： 云客户本地保存部分业务数据备份、转存，并有数据备份记录 不符合情况：云客户未本地保存业务数据备份、转存，并有数据备份记录

数据备份恢复	b）应提供查询云服务客户数据及备份存储位置的能力	在云计算环境中，大量用户数据被存储在不同的物理位置，供应用程序及操使用，在公有云、私有云、混合云中数据都有可能发生移动，其存储地点有可能位于同一数据中不同服务器或不同数据中心，云服务商应为云服务客户提供数据存储及备份位置	1)核查云服务商是否提供数据备份及存储位置查询的接口 2)测试验证是否能够查询到用户数据存储以及备份的位置	提供ECS查询实例所在物理机房的截图；提供RDS查询实例所在宿主机所在机房位置的截图；提供OSS查询Buket所在服务器，和资产系统查询此服务器所在机房地址的说明	符合情况：提供查询云服务客户数据及备份存储位置的能力 部分符合情况：提供查询云服务客户部分数据及备份存储位置的能力 不符合情况：不提供查询云服务客户数据及备份存储位置的能力
	c)云服务商的云存储服务应保证云服务客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	云服务商为云服务客户提供了云存储服务模式，对用户数据进行备份，并将多个副本存在不同的服务节点中。为降低成本，云服务商可能减少数据备份量，网络攻击也可能使多副本数据之间存在不一致，为确保备份数据的可用性、正确性和一致性，应定期核查数据是否多副本存储，并对多副本数据的完整性进行检测，确保各副本间内容的完整性和一致性	1)访谈云服务商为云服务客户提供的云存储模式是否多副本存储，检查多副本是否均可用 2)核查是否对多副本进行一致性比对，是否有对比记录	提供云服务商提供的数据存储说明，多副本进行一致性比对的机制及对比记录和结果	符合情况：提供云服务商提供的数据存储说明，多副本进行一致性比对的机制及对比记录和结果 不符合情况：不提供云服务商提供的数据存储说明，多副本进行一致性比对的机制及对比记录和结果
	d)应为云服务客户将业务系统和数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程	云服务商为云服务客户提供迁移服务，保证云服务客户业务系统和有关数据迁移到新的服务器上正常运行，云服务商应为云服务客户提供全程的协助，保证迁移活动顺利完成，确保数据在迁移过程中的完整性	1)访谈采用的云服务商是否支持云服务客户业务系统及数据的迁移，云服务商是否提供协助帮助云服务客户完成迁移 2)核查云服务商提供的迁移措施、手段	提供迁云服务的说明及协助说明	符合情况：提供迁云服务的说明及协助说明 不符合情况：不提供迁云服务的说明及协助说明
剩余信息保护	a）应保证虚拟机所使用的内存和存储空间回收时得到完全清除	当用户退出云服务时，用户释放内存和存储空间后，云服务商需要保证安全地删除用户的数据，避免发生数据残留。数据残留是指存储介质中的数据被删除后，并未彻底清除，在存储介质中留下了存储过数据的痕迹，残留的数据信息可能被攻击者非法获取，造成严重损失。一般来说，在数据销毁时可以采用覆盖、消磁、物理破坏等方法。云服务商应保证用户虚拟机释放内存和存储空间安全地删除，且采用了完全清除机制	1)核查虚拟在迁移和删除后，内存和存储空间回收时采用的删除机制是否能够使数据彻底清零 2)核查内存清零机制、数据删除机制、检测是否能够实现数据完全清除	各云租户之间的内存和持久化存储空可相对独立，租户资源释放时能够被释放和清除，内部系统鉴别信息完全清除；物理硬盘报废时使用随机数据多次写入进行数据写入和清除，对于曾经存储过用户数据的内存和磁盘，一旦释放和回收，其上的残留信息将被自动进行零值覆盖；释放的存储空间由分布式文件系统回收， 禁止任何用户访问，并在被再次使用前进行内容擦除(包括云盘每一块上的内容),最大限度保证用户的数据安全性	符合情况：保证虚拟机所使用的内存和存储空间回收时得到完全清除 不符合情况：不保证虚拟机所使用的内存和存储空间回收时得到完全清除
	b)云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除	为防止业务数据意外丢失，云客户业务数据在云上一般多副本存储，当云服务客户删除业务数据时，应采取数据清除机制将云计算平台所有副本全部删除	核查云服务客户在删除业务数据时，采用的删除机制是否能够将云存储中的所有副本删除	使用的数据删除机制保证云服务客户业务数据删除时，云存储中所有副本删除	符合情况：使用的数据删除机制保证云服务客户业务数据删除时，云存储中所有副本删除 不符合情况：未使用的数据删除机制保证云服务客户业务数据删除时，云存储中所有副本删除

集中管控	a)应能对物理资源和虚拟资源按照策略做统一管理调度与分配	云计算通过对物理资源的整合与再分配，提高了资源的利用率，一台物理机的资源可能被多个虚拟机所共享。对物理资源、虚拟资源的统一分配与调度，能 多提高资源利用率	1)核查是否部署了资源调度平台或其他平台对物理资源、虚拟资源进行统一分配与调度 2)核查资源管理平台是否能够实现物理资源、虚拟资源统一分配与调度的	提供资产管理系统的截图，提供物理资源、虚拟资源水位管理的系统的截图	符合情况：能对物理资源和虚拟资源按照策略做统一管理调度与分配 部分符合情况：能对部分物理资源和虚拟资源按照策略做统一管理调度与分配 不符合情况：不能对物理资源和虚拟资源按照策略做统一管理调度与分配
	b)应保证云计算平台管理流量与云服务客户业务流量分离	通过带外管理或策略配置的方式将网管量和业务流量分开，为网管流量建专属的通道，在这个通道中，只传输管理流量，管理流量与业务流量分离，可以提高网管的效率与可靠性，有利于提升管理流量的安全性	1)检查网络架构和配置策略，核查云平台管理流量是否采用带外管理或策略配置等方式 2)核查并测试管理流量与云服条客户业务流量是否分离	云平台管理流量通过带外管理，云服务客户业务流量通过上层网络；管理流量网络层使用的是经典网络，和业务网络默认隔离，云平台管理流量与业务流量完全分离	符合情况：保证云计算平台管理流量与云服务客户业务流量分离 不符合情况：不能保证云计算平台管理流量与云服务客户业务流量分离
	c)应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并 实现各自的集中审计	在云运维方面，为缓解云服务商和云服务客户间的不信任，云服务商和云服务客户应进行明确的职责划分，各自收集各自部分的审计数据，并对审计数据进行集中审计，实现云计算平台全面的信息审计，实现云计算环境下合规性、业务连续性、数据安全性等方面的审计要求，有效控制审计数据在云中面临的风险	1)核查云服务商和云服务客户间是否进行职责划分 2)检查云平台是否支持云服务商和云服务客户收集各自的审计数据 3)检查云服务商和云服务客户是否部署集中审计平台支持各自收集审计数据的集中审计	1)云平台运维侧及租户侧分别部署了不同的审计产品：云平台运维侧的，全部日志，全部传给云盾(安全审计) 2)租户侧部署了租户的审计产品，负责采集租户侧的审计日志，并完成审计功能。	符合情况：云服务商和云服务客户收集各自控制部分的审计数据并实现各自的集中审计。 部分符合情况：云服务商收集控制部分的审计数据并实现集中审计。云服务客户不能收集自身的日志。 不符合情况：云服务商和云服务客户均不收集各自控制部分的审计数据。
	d)应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测	为便于云服商和云服务客户能够及时掌握系统运行情况，云服务商和云服务客户的职责应明确划分，对各自控制的虚拟化资源（虚拟化网络、虚拟机、虚拟化安全设备等）运行状况集中监测	1)核查云服务商和云服务客是否进行职责划分 2)检查云平台是否支持云服务商和云服务客户集中监测各自控制部分虚拟源(虚拟化网络、虚拟机、虚拟化安全设备等)的运行状况	1)云监控中心提供了资源实时监控、告警和通知服务，可以监控云服务器ECS、负载均衡SLB、云数据库RDS和对象存储OSS相关指标 2)云管平台能够对虚拟资源运行状况进行集中监测	符合情况：能够对虚拟资源运行状况进行集中监测 部分符合情况：能够对部分虚拟资源运行状况进行集中监测 不符合情况：不能够对虚拟资源运行状况进行集中监测
	a)应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力	为确保云服务商提供的服务符合安全性需求，云服务客户应当选取安全合规的云服务商，且云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云服务提供商提供的云计算平台的安全服务等级，并核查云计算平台的安全防护等级 2)访谈管理员，业务系统的安全防护等级 3)核查云服务商提提供商提供的云计算平台的安全防护能力能够满足业务应用业务系统需求	云服务商提供云平台安全保护等级说明，云平台安全保护等级具有相应或高于业务应用系统所需求的安全防护能力	符合情况：提供云平台安全保护等级说明，云平台安全保护等级具有相应或高于业务应用系统所需求的安全防护能力 不符合情况：不提供云平台安全保护等级说明，云平台安全保护等级具有相应或高于业务应用系统所需求的安全防护能力
	b)应在服务水平协议中规定云服务的各项服务内容和具体技术指标	云服务商与云服务客户签订协议(如SLA),协议的内容可能会因不同的云服务 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，明确云服务商所提供的云服务内容以及云服务商需提供的技术指标	1)核查是否与云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云服务商所提供的云服务内容和需提供的技术指标进行规定	1)云服务商与云服务客户签订SLA文本 2)SLA文本内容包括了云服务商所提供的云服务内容和需提供的技术指标	符合情况：服务水平协议中规定云服务的各项服务内容和具体技术指标 不符合情况：服务水平协议中未规定云服务的各项服务内容和具体技术指标

云服务商选择	c)应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等	云服务商与云服务客户签订协议(如SLA)中是否对云服务商的权限与责任进行规定，规定内容是否包括云服务商的管理范围，职责划分、访问授权、隐私保护、行为准则、违约责任等	检查云服务商与云服务客户签订协议(如SLA)中是否对云服务商的权限与责任进行规定，规定内容是否包括云服务商的管理范围，职责划分、访问授权、隐私保护、行为准则、违约责任等	1）云服务商与云服务客户签订SLA文本 2) SLA文本内容规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等	符合情况： 服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等 部分符合情况：服务水平协议中规定部分云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等 不符合情况：服务水平协议中未规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等
	d)应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除	云服务商与云服务客户签订协议(如SLA)中内容应包括业务关系到期和受影响的用户数据的处理方案，当云服务客户与云服务商服务合约到期后，云服商应向云服务客户提供完整的数据，且制定相关规定保证相关数据在云计算平台上完全清除	1)核查云服务商应与云服务客户签订协议(如SLA)中是否规定业务关系到期和受其影响的用户数据的处理方案，是否规定合约到期后云服务商向云服务客户提供完整的数据 2)核查云服务商应与云服务客户签订协议是否规定合约到期后云服务商清除云计算平台上的数据	1)云服务商与云服务客户签订SLA文本 2)SLA文本内容规定云服务商的权限与责任，规定业务关系到期和受其影响的用户数据的处理方案，规定合约到期后云服务商向云服务客户提供完整的数据	符合情况： 服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除 部分符合情况：服务水平协议中规定服务合约到期时，完整提供云服务客户数据，但不承诺相关数据在云计算平台上清除 不符合情况：服务水平协议中未规定服务合约到期时，完整提供云服务客户数据，不承诺相关数据在云计算平台上清除
	e)应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据	云服务客户应与云服务商签署保密协议，协议中应规定云服务商不得以任何理由泄露云服务客户数据	1)访谈云服务客户是否与云服务商签订保密协议 2)核查保密协议是否规定云服务商不得以任何理由泄露云服务客户数据	1)云服务客户与云服务商签订保密协议 2)保密内容明确规定数据归云服务客户所有，云服务商不得以任何理由泄露云服务客户数据	符合情况：签署保密协议，要求其不得泄露云服务客户数据 不符合情况：未签署保密协议，要求其不得泄露云服务客户数据
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。 云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，以保持云计算安全服务的而持续性和合规性，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)访谈确认选择的云服务商 2)核查云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

	b)应提供应链安全事件信息或安全威胁信息及时传达到云服务客户	云服务商应及时向云服务客户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)核查云服务商是否定期向云服务客户通报安全事件 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	云服务商推送最新的安全事件信息，以保证第一时间传达给云服务客户	符合情况：云服务商推送最新的安全事件信息，以保证第一时间传达给云服务客户 不符合情况：云服务商不推送最新的安全事件信息，不保证第一时间传达给云服务客户
	c)应将供应商的重要变更及时的传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制	云服务商与云服务客户应建立供应链协议（如SLA),如果云服务商所进行的的任何变更，可能对云服务客户造成影响，应评估变更带来的安全风险，告知云服务客户，或事前得到客户授权，以便于云服务客户能够制定相应的措施应对可能引发的风险	1)检查云服务商与云服务户之间的供应链协议(如SLA),核查云服务商所进行的任何变更是否及时告知客户或事前得到客户授权 2)检查云服务客户是否对变更的风险进行安全评估，是否采取相应的安全措施应对安全风险	(1)云服务商通过云管平台推送通知和公告，云服务客户通过自己的控制台查看相关风险和控制变更的信息 (2)云服务商对所有变更均有变更流程控制，云服务客户可以根据需求定制、选择自己感兴趣的风险信息	符合情况：服务商通过云管平台推送通知和公告，云服务客户通过自己的控制台查看相关风险和控制变更的信息 不符合情况：服务商不通过云管平台推送通知和公告，云服务客户不能通过自己的控制台查看相关风险和控制变更的信息
云计算环境管理	a)云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定	云计算平台的运维地点原则应位于中国境内，若确实因业务需求，需通过境外对境内的云计算实施运维操作，应满足国家相关规定	1)访谈管理员运维地点，核查运维地点是否在中国境内 2)访谈管理员是否存在境内对境外云计算平台的运维操作，若存在，核查是否满足国家相关规定	1)提供仅允许在中国境内进行运维操作，其他区域禁止运维操作的规定 2)若存在境外运维操作，提供相关运维制度，并提供符合国家相关规定的说明	符合情况：云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作遵循国家相关规定 不符合情况：云计算平台的运维地点应位于中国境外，境外对境内云计算平台实施运维操作不遵循国家相关规定