计算扩展标准测评项适用性判定说明（仅限IAAS服务模式

安全层面	安全控制点	测评项	云平台	云租户
安全物理环境	基础设施位置	应保证云计算基础设施位于中国境内。	●	
安全通信网络	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；	●	
		b)应实现不同云服务客户虚拟网络之间的隔离；	●	
		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、入侵防范等安全机制的能力；	●	
		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；	●	
		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在云计算平台选择第三方安全服务。	●	
		f)应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问；（第四级）	●	
		g）应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式；（第四级）	●	
		h)应为第四级业务应用系统划分独立的资源池。（第四级）	●	
安全区域边界	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；	●	●
		b)应在不同等级的网络区域边界部署访问控制机制，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攻击行为，并能记录攻击类型、攻击时间、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；	●	●
		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；	●	●
		d）应在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）应对云服务商和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；	●	●
		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。	●	●
	身份鉴别	a)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。	●	●
	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；	●	

		访问控制	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。	●	
		入侵防范	a)应能检测虚拟机之前的资源隔离失效，并进行告警；	●	
			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；	●	●
			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。	●	●
		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；	●	
			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源被非法访问。	●	
安全计算环境		数据完整性和保密性	a)应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；	●	●
			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的管理权限；	●	
			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，并在检测到完整性受到破坏时采取必要的恢复措施；	●	
			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。	●	
		数据备份恢复	a)云服务客户应在本地保存其业务数据的备份；		●
			b)应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；	●	
			d)应为云服务客户将业务系统及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。	●	
		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；	●	
			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。	●	
		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；	●	
			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；	●	
安全管理中心			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；	●	●
			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。	●	●

安全建设管理	云服务商选择	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；			●
		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；			●
		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；			●
		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；			●
		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。			●
	供应链管理	a)应确保供应商的选择符合国家有关规定；	●		●
		b)应将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；	●		
		c)应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。	●		
安全运维管理	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。	●		