ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0167—2018

云计算技术金融应用规范 安全技术要求

Financial application specification of cloud computing technology——

Security technical requirements

2018-08-15 发布 2018-08-15 实施

中国人民银行 发布

目　　次

前　言

本标准是云计算技术金融应用系列标准之一，云计算技术金融应用系列标准包括：

——《云计算技术金融应用规范　技术架构》；

——《云计算技术金融应用规范　安全技术要求》；

——《云计算技术金融应用规范　容灾》。

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准负责起草单位：中国人民银行科技司、中国人民银行济南分行。

本标准参加起草单位：中国互联网金融协会、网联清算有限公司、中国金融电子化公司、中国人民银行西安分行、北京中金国盛认证有限公司、北京移动金融产业联盟、中金金融认证中心有限公司、北京银联金卡科技有限公司、北京软件产品质量检测检验中心、财付通支付科技有限公司、蚂蚁金融服务集团、华为技术有限公司、阿里云计算有限公司、北京百度网讯科技有限公司、新华三技术有限公司、兴业数字金融服务（上海）股份有限公司、亚马逊通技术服务（北京）有限公司、北京京东金融科技控股有限公司、中国工商银行、中国农业银行、中国银行、中国建设银行、中国邮政储蓄银行、招商银行、中国光大银行、中国民生银行、兴业银行、平安银行、国泰君安证券股份有限公司、华泰证券股份有限公司、中国人寿保险（集团）公司、中国人民保险集团股份有限公司、中国银联股份有限公司、北京宏基恒信科技有限责任公司、北京信安世纪科技股份有限公司、天津麒麟信息技术有限公司、深圳证券交易所、上海众人网络安全技术有限公司。

本标准主要起草人：李伟、李兴锋、邬向阳、张宏基、班廷伦、强群力、杨倩、马征、聂丽琴、郭林、胡达川、朱勇、周国林、辛路、杨彬、陈则栋、刘运、秦宇锋、缪凯、杨文斌、任兆麟、吴永强、吴金海、孔令斌、张文涛、莫云飞、陈当阳、李明凯、赵华、符海芳、高志民、高强裔、白阳、于柳绮、居未伟、王晓燕、樊华、王伟、沈锡镛、杨俊、郝轶、罗子强、张国泽、周亚国、张翰林、蒋增增、卞海军、张振猛、胥少龙、来宾、王宇翔、陈晨、陈雪秀、曹伟、穆冬生、宋杰、瞿红来、许涛、王绍斌、张荣典、潘斌、汪宗斌、白雷、侯大鹏、张峻华、张嵩、赵春华、高天游、金怡、钟琪、闫莅、黄敏、葛小宇、王仕、王研娟、林春、郑子洲、周伟然、黄超、高坤、林林、李荣振、李志伟。

云计算技术金融应用规范　　安全技术要求

1　范围

本标准规定了金融领域云计算技术应用的安全技术要求，涵盖基础硬件安全、资源抽象与控制安全、应用安全、数据安全、安全管理功能、安全技术管理要求、可选组件安全等内容。

本标准适用于金融领域的云服务提供者、云服务使用者、云服务合作者等。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0131—2015　金融业信息系统机房动力系统规范

JR/T 0166—2018　云计算技术金融应用规范　技术架构

3　术语和定义

JR/T 0166—2018界定的术语和定义适用于本文件。

4　缩略语

下列缩略语适用于本文件。

API	应用程序编程接口（Application Programming Interface）
CPU	中央处理单元（Central Processing Unit）
DDoS	分布式拒绝服务攻击（Distributed Denial of Service）
DoS	拒绝服务（Denial of Service）
HTTPS	安全超文本传输协议（Hypertext Transfer Protocol Secure）
IaaS	基础设施即服务（Infrastructure as a Service）
IP	互联网协议（Internet Protocol）
MAC	媒体访问控制（Media Access Control）
PaaS	平台即服务（Platform as a Service）
SaaS	软件即服务（Software as a Service）
SQL	结构化查询语言（Structured Query Language）
VPN	虚拟专用网络（Virtual Private Network）
XSS	跨站脚本攻击（Cross-site Scripting）

5　概述

5.1　云计算安全技术要求分级

云计算技术按需使用信息技术和数据资源，降低信息化成本，提高资源利用效率，但同时也带来了服务外包、数据泄露、服务滥用等方面的新风险。云服务使用者应结合信息系统的业务重要性和数据敏感性，充分评估应用云计算技术的科学性、安全性和可靠性，在确保系统业务连续性、数据和资金安全的前提下，谨慎选用云计算技术部署业务系统，选择与业务相适应的部署和服务模式，确保使用云计算技术的金融业务系统安全可控。

为进一步增强标准的适用性和前瞻性，规范按照分级分类管理思路将具体条款分为基本要求、扩展要求和增强要求。基本要求是通用性和基础性的安全要求，云计算技术金融应用均应满足；扩展要求是在通用要求基础上，针对团体云等社会化服务模式提出的扩展性安全技术要求；增强要求是从安全技术的发展趋势和金融用户的前瞻性需求入手提出的增强要求。

5.2 基本要求增强要求云计算安全框架

云计算安全框架由基础硬件安全、资源抽象与控制安全、应用安全、数据安全、安全管理功能以及可选组件安全组成。云服务提供者和使用者共同实现安全保障。云计算安全框架如图1所示，在IaaS、PaaS、SaaS等不同服务类别下云服务提供者和使用者的安全分工有所区别。金融机构是金融服务的最终提供者，其承担的安全责任不应因使用云服务而免除或减轻。

图 1 云计算安全框架

云计算平台作为承载金融领域信息系统的基础平台，其安全要求应不低于所承载业务系统的安全要求。云计算平台本质上仍是一种信息系统，应满足国家和金融行业信息系统安全相关要求，本标准重点从云计算技术角度提出了云计算平台应符合的安全要求。容器、中间件、数据库等云计算平台可选组件的安全要求见附录A，云计算相关安全风险分析参见附录B。

6 基础硬件安全

6.1 机房安全

基本要求：

应保证云计算平台部署的物理数据中心及附属设施符合 JR/T 0131—2015 相关要求。

扩展要求：

a) 对于团体云部署模式，应保证用于服务金融业的云计算数据中心运行环境与其他行业物理隔离；

b) 应保证用于云服务使用者业务运行、数据存储和处理的物理设备位于中国境内；

c) 应保证云计算平台的运维和运营系统部署在中国境内。

增强要求：

无。

6.2 网络安全

基本要求：

a) 应支持网络冗余设计，将网络通信链路和网络设备等冗余部署；

b) 应按照安全需求划分为不同的网络区域，支持网络安全隔离；

c) 应保证云计算平台的业务网络与管理网络安全隔离；

d) 应保证采取网络控制措施防止非授权设备连接云计算平台内部网络，并防止云计算平台物理服务器非授权外联。

扩展要求：

a) 应支持为云服务使用者提供专线或 VPN 接入；

b) 对于团体云部署模式，应保证除广域网外为金融业服务的网络物理硬件不与其他行业共享；

c) 应保证向云服务使用者提供服务的网络资源与其他网络资源安全隔离。

增强要求：

应支持网络带宽优先级分配。

6.3 设备安全

基本要求：

a) 应保证关键设备冗余部署，保证系统可用性；

b) 应对设备运行状态、资源使用等进行监控，能够在发生异常情况时发出告警；

c) 应保证设备和存储介质在重用、报废或更换时，能够对其承载的数据完全清除。

扩展要求：

对于团体云部署模式，应保证用于金融业的物理设备不与其他行业共享。

增强要求：

a) 应保证设备安全启动，即启动时的版本和预期一致，完整性没有受到破坏；

b) 应对设备重要配置文件进行完整性保护。

7 资源抽象与控制安全

7.1 通用要求

本章条要求是网络资源池、存储资源池和计算资源池均应满足的通用要求。

基本要求：

a) 应支持内核补丁检测加固和防止内核提权；

b) 应保证通过 Web 和 API 等接口访问云计算平台时采用安全可靠的身份认证措施。

扩展要求：

a) 应保证采用 HTTPS 协议远程调用 API 接口；

b) 应支持对软件漏洞及时发现并修复。

增强要求：

应保证用户远程访问云计算平台进行管理时采取加密方式，并至少采取两种或两种以上的组合机制进行身份鉴别。

7.2 网络资源池安全

7.2.1 概述

网络资源池安全包括针对网络资源配置和运营的安全要求，也包括对保障网络安全的安全产品、功能或服务的安全要求。云服务使用者从云服务提供者获取网络资源池中的虚拟网络资源和控制权。

7.2.2 架构安全

基本要求：

应保证虚拟网络全冗余设计，避免单点故障。

扩展要求：

a) 应支持不同租户网络及同一租户不同网络的隔离；

b) 应支持云服务使用者自行划分安全区域；

c) 应支持 VPC 相关的安全功能，对 VPC 的操作（如创建或删除 VPC，自定义路由、安全组和 ACL 策略等）需要验证云服务使用者凭证；

d) 应支持 VPC 之间以及 VPC 与其他网络建立 VPN 或专线连接；

e) 应支持云服务使用者监控所拥有各网络节点间的流量。

增强要求：

a) 应识别、监控虚拟机之间的流量；

b) 应支持开放接口，允许接入第三方安全产品。

7.2.3 访问控制

基本要求：

a) 应部署访问控制策略，实现虚拟机之间、虚拟机与资源管理和调度平台之间、虚拟机与外部网络之间的安全访问控制；

b) 应对云计算平台管理员访问管理网络进行访问控制；

c) 应实时监控云服务远程管理的访问，并支持对未授权管理连接的处置；

d) 应对远程执行特权命令进行限制。

扩展要求：

a) 应支持云服务使用者通过 VPN 访问云计算平台；

b) 应支持云服务使用者自行在虚拟网络边界设置访问控制规则；

c) 应支持云服务使用者自行划分子网、设置访问控制规则；

d) 应支持云服务使用者自行过滤进出 VPC 的网络流量。

增强要求：

无。

7.2.4 安全审计

基本要求：

a) 应记录虚拟网络运行状况、网络流量、用户行为等日志；

b) 应为安全审计数据的汇集提供支持。

扩展要求：

a) 应根据云服务提供者和云服务使用者的职责划分，实现各自控制部分的审计；

b) 云服务提供者应为云服务使用者进行审计提供必要支持；

c) 审计记录产生时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。

增强要求：

应支持根据特定要求输出特定网络通讯的元数据和报文数据。

7.2.5 入侵防范

基本要求：

a) 应防止虚拟机使用虚假的 IP 或 MAC 地址对外发起攻击；

b) 应识别、监控和处理虚拟机之间的异常流量。

扩展要求：

a) 应检测和防护云计算平台内部虚拟机发起的针对云计算平台的攻击，能够定位发起攻击的虚拟机，记录攻击类型、攻击时间、攻击流量等信息；

b) 应对各类网络攻击行为进行监测和发现，当检测到网络攻击行为时，记录攻击源 IP、攻击类型、攻击时间等信息，在发生严重入侵事件时应进行告警；

c) 通过互联网提供金融服务时，应支持 DoS/DDoS 攻击防护，通过清洗 DoS/DDoS 攻击流量，保障网络、服务器及上层应用的可用性；

d) 通过互联网提供金融服务时，应支持检测 Web 应用漏洞，拦截 SQL 注入、XSS 攻击等多种 Web 应用攻击行为；

e) 应支持防 ARP 欺骗。

增强要求：

a) 应支持禁用未备案域名；

b) 应检测和阻断云服务使用者对外攻击行为，记录攻击类型、攻击时间、攻击流量等信息；

c) 应支持对恶意虚拟机的隔离，支持阻断恶意虚拟机与外部网络以及其他虚拟机的通信。

7.2.6 恶意代码防范

基本要求：

a) 应支持对恶意代码进行检测和清理；

b) 应维护恶意代码特征库的升级和相关检测系统的更新。

扩展要求：

无。

增强要求：

无。

7.3 存储资源池安全

存储资源池安全包括对存储资源配置和运营的安全要求，也包括对保障存储安全的安全产品、功能或服务的安全要求。云服务使用者从云服务提供者获取存储资源池中的虚拟存储资源和控制权。

基本要求：

a) 应支持多层级访问控制；

b) 应记录存储设备运行状况、用户行为等日志；

c) 应为安全审计数据的汇集提供支持。

扩展要求：

a) 应支持分布式存储的数据副本分布在不同的物理机架；

b) 应禁止云计算平台管理员未授权操作租户资源；

c) 应支持租户访问存储资源的安全传输；

d) 应支持跨物理集群服务使用者账号权限管理；

e) 应支持内容加密存储，加密密钥支持租户自管理、云服务提供者管理和第三方机构管理；

f) 应对不同租户的数据隔离；

g) 应根据云服务提供者和云服务使用者的职责划分，实现各自控制部分的审计；

h) 云服务提供者应为云服务使用者进行审计提供必要支持；

i) 审计记录产生时间应由系统范围内唯一确定的时钟产生,以确保审计分析的正确性。

增强要求：

无。

7.4 计算资源池安全

7.4.1 概述

计算资源池安全既包括虚拟机自身安全，也包括保障虚拟机安全的产品、功能和服务的安全要求。云服务使用者从云服务提供者获取计算资源池中的计算资源和控制权。

7.4.2 访问控制

基本要求：

应对访问主体进行必要的身份验证。

扩展要求：

a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b) 应根据安全策略设置登录终端的操作超时锁定；

c) 应禁止云计算平台管理员未授权操作租户资源；

d) 访问控制的粒度应达到主体为用户级或进程级，客体为文件或数据库表级。

增强要求：

应支持使用两种或两种以上组合的鉴别技术对用户进行身份鉴别。

7.4.3 安全审计

基本要求：

a) 应记录虚拟机运行状况、网络流量、用户行为等日志；

b) 应为安全审计数据的汇集提供支持。

扩展要求：

a) 应根据云服务提供者和云服务使用者的职责划分，实现各自控制部分的审计；

b) 云服务提供者应为云服务使用者进行审计提供必要支持；

c） 审计记录产生时间应由系统范围内唯一确定的时钟产生,以确保审计分析的正确性。

增强要求：

无。

7.4.4 入侵防范

基本要求：

应能够检测虚拟机对宿主机资源的异常访问，并进行告警。

扩展要求：

无。

增强要求：

a） 应对虚拟机启动过程进行完整性保护；

b） 应对虚拟机运行过程进行完整性保护；

c） 应对虚拟机重要配置文件进行完整性保护。

7.4.5 恶意代码防范

基本要求：

应支持对后门、木马、蠕虫、webshell 等恶意代码的静态检测和行为检测，并对检测出的恶意代码进行控制和隔离。

扩展要求：

应支持云服务使用者自行安装防恶意代码软件，并支持更新防恶意代码软件版本和恶意代码库。

增强要求：

应提供多层恶意代码防护机制。

7.4.6 资源控制

基本要求：

a） 应保证分配给不同虚拟机的内存资源隔离；

b） 应支持设置并监控虚拟机网络接口带宽；

c） 应对虚拟机进行资源监控，资源监控的内容包括 CPU 利用率、带宽使用情况、内存利用率、存储使用情况等；

d） 应为监控信息的汇集提供支持。

扩展要求：

a） 应支持统一调度与分配物理资源和虚拟资源；

b） 应支持虚拟机和虚拟机管理器间内部通信通道的受限使用；

c） 应保证部分虚拟机崩溃不影响虚拟机管理器及其他虚拟机。

增强要求：

a） 应支持分配给不同虚拟机的存储资源安全隔离；

b） 应支持云服务使用者设置虚拟资源（如CPU、硬盘、内存、网络等）优先级别，优先保障重要业务服务所占用资源。

7.4.7 镜像和快照保护

基本要求：

a) 应支持自动虚拟机快照功能，保证系统能根据快照恢复；
b) 应校验虚拟机镜像、快照的完整性，防止恶意篡改虚拟机镜像和快照；
c) 应对重要业务系统提供加固的操作系统镜像。

扩展要求：

应保证虚拟机镜像和快照文件备份在不同物理服务器。

增强要求：

应采取加密或其他技术措施，防止非法访问虚拟机快照和镜像中可能存在的敏感数据。

8 应用安全

应用安全包括IaaS、PaaS、SaaS等服务类别下的业务应用安全。

基本要求：

a) 应支持资源的访问控制；
b) 应支持应用审计。

扩展要求：

a) 应采取有效措施防范各类应用攻击，包括定期漏洞扫描和安全评估、及时发现并告警异常行为、防范页面篡改和代码注入等；
b) 应审查代码后门，管控代码打包和发布；
c) 应有效屏蔽系统技术错误信息，不将系统产生的技术错误信息直接反馈给客户。

增强要求：

a) 应监控识别应用的异常访问；
b) 应支持限制 API 调用，如限制调用频率和使用白名单等；
c) 应支持检查访问云计算平台的终端的安全状态；
d) 应采取有效措施防止用户输入的敏感信息被窃取。

9 数据安全

9.1 数据产生

基本要求：

a) 应识别敏感数据，根据数据的敏感度进行分类；
b) 应识别个人信息，按照国家与行业主管部门相关规定及标准对个人信息进行保护。

扩展要求：

无。

增强要求：

应分类标识和保护敏感数据。

9.2 数据传输

基本要求：

a) 应采用技术措施保证敏感数据和个人信息传输的保密性；
b) 应能够检测到数据在传输过程中完整性受到破坏。

扩展要求：

a) 应支持云服务使用者实现对关键业务数据和管理数据传输的保密性,关键业务数据的范围和加密强度应符合国家与行业主管部门相关规定；
b) 应保证云服务使用者与云计算平台之间数据传输的完整性。

增强要求：

无。

9.3 数据存储

基本要求：

a) 应采用加密技术或其他保护措施实现鉴别信息保密性；
b) 应根据国家与行业主管部门相关规定加密存储敏感数据。

扩展要求：

a) 应支持云服务使用者选择加密算法和密钥长度；
b) 应支持云服务使用者实现对关键业务数据和管理数据的存储保密性,关键业务数据的范围和加密强度应符合国家与行业主管部门相关规定；
c) 应支持云服务使用者对云计算平台上数据加密存储；
d) 应支持云服务使用者选择第三方密钥管理机制加解密数据，密钥支持租户自管理、云服务提供者管理和第三方机构管理。

增强要求：

无。

9.4 数据访问

基本要求：

应针对数据访问进行授权和验证，保证最小访问授权。

扩展要求：

应禁止云服务提供者未经云服务使用者授权访问云服务使用者数据，并对授权访问的行为进行审计。

增强要求：

无。

9.5 数据迁移

基本要求：

a) 云服务使用者应在数据迁移前评估网络连接能力，保证数据迁移的安全实施；
b) 云服务使用者应保证数据迁移不影响业务应用的连续性；
c) 云服务使用者应做好数据迁移的数据备份以及恢复相关工作。

扩展要求：

云服务提供者应根据云服务使用者需求提供数据迁移的技术保障。

增强要求：

无。

9.6 数据清除

基本要求：

a) 应保证云服务使用者鉴别信息的存储空间被释放或再分配给其他用户前完全清除；

b) 对于更换或报废的存储介质，应采取强化消磁或者物理损坏磁盘等方式，防止恢复已清除数据。

扩展要求：

a) 应保证文件、目录和数据库等资源所在的存储空间被释放或重新分配给其他租户前完全清除；

b) 应支持协助清除因业务终止、迁移数据、自然灾害、合同终止等遗留的数据，日志留存时间应符合国家与行业主管部门相关规定；

c) 应支持所有副本数据的清除。

增强要求：

无。

9.7 数据备份和恢复

基本要求：

应支持备份和恢复数据。

扩展要求：

a) 应支持云服务使用者自行备份和恢复数据；

b) 应周期性测试云计算平台的备份系统和备份数据，支持故障识别和备份重建；

c) 应支持云服务使用者查询备份数据存储位置。

增强要求：

无。

10 安全管理功能

10.1 身份和权限管理

基本要求：

a) 应支持云计算平台管理员的角色及其相应权限分配给不同账户；

b) 应支持云计算平台管理员权限分离；

c) 应支持云计算平台管理员权限最小化；

d) 应支持云计算平台管理员首次登录时强制修改初始口令；

e) 应采用两种或两种以上组合的鉴别技术对云计算平台管理员进行身份鉴别。

扩展要求：

a) 应支持租户的身份和访问管理，集中管理租户账户以及租户账户的子账户；对子账户的管理，租户账户可以创建多个子账户，并管理每个子账户的权限；支持租户账户对子账户的分组授权，如基于角色、用户组授权；应支持租户账户下的子账户权限最小化；

b) 应支持租户密码策略管理，密码策略管理应支持密码复杂度策略、密码有效期策略，租户账号的初始密码应支持随机生成，租户首次登录支持强制修改初始密码；

c) 应支持为云服务使用者随机生成虚拟机登录口令或云服务使用者自行设置登录口令；

d) 应支持云服务使用者以密钥对方式登录虚拟机时，自主选择云计算平台生成密钥对或自行上传密钥对；

e) 应支持集中管理租户鉴别凭证；

f) 应支持云服务使用者鉴别凭证的机密性和完整性保护；

g) 应支持修改云服务使用者鉴别凭证前验证租户身份；

h) 应支持检测云服务使用者账户异常并通知云服务使用者；

i) 应支持多种云服务使用者身份鉴别方式；

j） 应支持云服务使用者身份鉴别警示信息，提示可能导致的后果；

k） 应支持云服务使用者自主选择主账号采用两种或两种以上组合的鉴别技术进行身份鉴别；

l） 应支持对接云服务使用者自建身份认证中心。

增强要求：

应对云计算平台管理员及特权账号的权限进行管理，包括限制特权账号的使用时间，可授权特权账号的管理员账号无法使用特权账号的业务操作权限等。

10.2 运维管理

基本要求：

应保证远程运维通信的保密性和完整性，使用的加密算法和密钥长度应符合国家密码管理部门及行业主管部门要求。

扩展要求：

a） 云服务提供者管理员的运维操作权限应经过多级安全审批并固化命令级规则，非固化操作实时审计告警；

b） 云服务提供者应仅能通过特定可审计可授权的设备进行运维管理，支持对运维人员的权限控制，记录所有活动日志；

c） 应对云端资源的访问和运维操作进行审计，支持会话过程重现。

增强要求：

无。

10.3 集中监控

基本要求：

a） 应对云计算平台的设备、资源以及云服务等进行实时监控，应支持对关键指标进行告警；

b） 应对异常行为集中监控分析并告警。

扩展要求：

应集中监控服务质量，并可导出集中监控报告。

增强要求：

应支持远程监控的可视化展示。

10.4 集中审计

基本要求：

a） 应将云计算平台内部系统时钟与国家权威时间源同步；

b） 应保证对云计算平台的操作均可生成审计报告；

c） 应汇集云计算平台所有的日志数据，进行集中审计，并可供第三方机构审计。

扩展要求：

a） 应提供审计接口或支持第三方机构开展独立的全面安全审计的能力；

b） 应保证云服务提供者对云服务使用者系统和数据等资源的操作可被云服务使用者审计。

增强要求：

a） 应提供安全审计产品或服务，对云计算平台上业务及服务进行安全审计；

b） 应支持统计分析海量审计数据；

c） 应支持攻击来源的追溯，对审计数据进行关联性分析和挖掘。

10.5 密钥管理

基本要求：

a) 应保证密钥的安全存储和管理；

b) 应使用经国家密码管理机构认可的商用密码产品；

c) 应保证密钥长度符合国家密码管理部门及行业主管部门要求；

d) 应支持数据加解密和密钥管理，数据加解密、数字签名等技术应符合国家密码管理部门及行业主管部门要求。

扩展要求：

应支持云服务使用者选择第三方密钥加解密数据，密钥支持租户自管理、云服务提供者管理和第三方机构管理。

增强要求：

a) 云服务使用者与云计算平台交互业务时，应使用专用安全硬件数字证书（如 USB Key 等）；

b) 应支持密钥全生命周期统一管理；

c) 应支持硬件安全模块实现密钥管理。

10.6 风险预警

基本要求：

a) 应支持安全漏洞和威胁的识别；

b) 应支持评估云计算平台安全漏洞风险并完成修复。

扩展要求：

应支持评估云服务使用者在云计算平台上应用的安全漏洞风险并协助修复。

增强要求：

a) 应收集并分析安全威胁信息；

b) 应支持预测威胁态势、脆弱性态势和运行态势。

11 安全技术管理要求

11.1 安全策略和管理制度

11.1.1 管理制度

基本要求：

a) 应对安全管理活动中的主要管理内容建立安全管理制度；

b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。

扩展要求：

应对安全管理活动中的各类管理内容建立安全管理制度。

增强要求：

无。

11.1.2 制定和发布

基本要求：

a) 应指定或授权专门的部门或人员负责安全管理制度的制定；

b) 应通过正式、有效的方式发布安全管理制度，并进行版本控制。

扩展要求：

应形成由安全策略、管理制度、操作规程、记录表单等构成的全面信息安全管理制度体系。

增强要求：

无。

11.1.3 评审和修订

基本要求：

应定期论证和审定安全管理制度的合理性及适用性，修订存在不足或需要改进的安全管理制度。

扩展要求：

应建立信息安全管理制度体系持续改进机制。

增强要求：

无。

11.2 安全管理机构和人员

11.2.1 岗位设置

基本要求：

a) 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义部门及各负责人的职责；
b) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位职责；
c) 应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权。

扩展要求：

无。

增强要求：

无。

11.2.2 人员配备

基本要求：

a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；
b) 应配备专职安全管理员，不可兼任。

扩展要求：

无。

增强要求：

a) 关键事务岗位应配备多人共同管理；
b) 应审查管理员资质。

11.2.3 授权和审批

基本要求：

a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批程序。

扩展要求：

应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

增强要求：

无。

11.2.4 审核和检查

基本要求：

a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份情况等；

b) 应在发生重大变更时开展全面安全检查，检查内容包括现有安全技术措施的有效性，安全配置与安全策略的一致性，安全管理制度的执行情况等。

扩展要求：

a) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

b) 应制定安全检查表格，实施安全检查，汇总安全检查数据，形成安全检查报告，并将安全检查结果告知相关方。

增强要求：

无。

11.3 安全建设管理

11.3.1 安全方案设计

基本要求：

a) 应根据云计算平台安全需求选择基本安全措施，依据风险分析的结果补充和调整安全措施；

b) 应论证和审定安全方案的合理性和正确性，经过批准后才能正式实施。

扩展要求：

a) 应根据云计算平台承载业务重要程度、云计算平台与平台之外的业务系统之间的关系，进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；

b) 应组织相关部门和有关安全专家论证和审定安全整体规划及其配套文件，经过批准后才能正式实施。

增强要求：

无。

11.3.2 测试验收

基本要求：

a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

b) 应在软件开发生命周期各阶段进行安全测试，并出具安全测试报告；

c) 应验证或评估安全措施的有效性。

扩展要求：

无。

增强要求：

无。

11.3.3 供应链管理

基本要求：

应确保供应链安全事件信息或威胁信息能够及时告知云服务使用者。

扩展要求：

a) 应确保将供应商的重要变更及时告知云服务使用者，并充分评估变更带来的安全风险，采取有效措施控制风险；

b) 应注明外包服务或采购产品对云服务安全性的影响。

增强要求：

a) 与供应商签订的服务水平协议中的相关指标，不低于拟与客户所签订的服务水平协议中的相关指标；

b) 当变更供应商时，对供应商变更带来的安全风险进行评估，采取有效措施控制风险。

11.3.4 安全资源管理

基本要求：

a) 应指定专门的部门或人员定期维护各种设备（包括备份和冗余设备）、线路等 IT 基础资源；

b) 应对配套设施、软硬件维护做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。

扩展要求：

a) 应根据资产的重要程度和价值对资产进行标识管理，并选择相应的管理措施；

b) 应确保信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时，对重要数据进行加密；

c) 含有存储介质的设备在报废或重用前，应进行完全清除，确保该设备上的敏感数据和授权软件无法被恢复重用。

增强要求：

无。

11.3.5 服务关闭

基本要求：

无。

扩展要求：

a) 云服务使用者应与云服务提供者协商制订并执行退出计划；

b) 云服务使用者退出云计算平台时，云服务提供者应安全返还云计算平台的云服务使用者数据；

c) 云服务提供者应在约定时间内，完全清除云计算平台存储的云服务使用者数据和相关运行信息；

d) 云服务提供者应为云服务使用者信息迁移提供技术手段，并协助完成迁移。

增强要求：

在数据和业务系统迁移过程中，应保证业务的可用性和连续性，如采取原业务系统与新部署业务系统并行运行一段时间等措施。

11.4 安全运维管理

11.4.1 风险管理

基本要求：

应采取必要的措施识别安全风险，对发现的安全风险及时进行修补或评估可能的影响后进行修补。

扩展要求：

应定期开展安全测评，形成安全测评报告，并对发现的安全问题采取应对措施。

增强要求：

无。

11.4.2 变更管理

基本要求：

应明确变更需求，变更前制定变更方案，变更方案经过审批后方可实施。

扩展要求：

a) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；

b) 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练；

c) 对于可能会产生重大影响的变更应通知云服务使用者。

增强要求：

无。

11.4.3 监控管理

基本要求：

a) 应确保信息系统的监控活动符合关于个人信息保护的相关政策法规；

b) 应制定相关策略，持续监控设备、资源、服务以及安全措施的有效性。

扩展要求：

云服务提供者应将安全措施有效性的监控结果定期提供给云服务使用者。

增强要求：

无。

11.4.4 业务连续性管理

基本要求：

a) 应建立业务连续性组织架构，明确日常管理组织架构和应急处置组织架构；

b) 应定期开展业务影响分析、连续性风险评估；

c) 应定期开展业务连续性计划演练，检验应急预案的完整性、可操作性和有效性，验证业务连续性资源的可用性，提高运营中断事件的综合处置能力；

d) 应制定运营中断事件等级划分标准，根据事件影响范围、持续时间和损失程度定义事件等级，开展应急响应处置工作。

扩展要求：

a) 应定期开展业务连续性管理审计工作；

b) 应建立业务连续性管理持续改进机制。

增强要求：

无。

11.4.5 应急响应

基本要求：

a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。

扩展要求：

a) 按照国家和行业主管部门要求制定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

b) 应定期对原有的应急预案重新评估，修订完善；

c) 云服务提供者应将应急预案提前告知云服务使用者。

增强要求：

无。

11.4.6 审计管理

基本要求：

a) 应详细记录运维日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

b) 应确保提供给云服务使用者审计数据的真实性和完整性。

扩展要求：

a) 应指定专门的部门或人员对日志、监测和告警数据等进行分析、统计，及时发现可疑行为；

b) 应严格控制系统变更，变更过程中应保留不可更改的审计日志。

增强要求：

无。

附 录 A
（规范性附录）
云计算平台可选组件的安全要求

A.1 容器安全

基本要求：

a) 应具备容器隔离机制，通过操作系统内核机制等保证不同容器进程、网络、消息、文件系统和主机名相互隔离和资源限制；

b) 应支持镜像仓库安全机制，能够保证镜像仓库链路安全，对镜像文件数据进行签名；

c) 云计算平台应支持镜像配置安全机制，保证数据库、中间件、安全设备的连接安全。

扩展要求：

无。

增强要求：

无。

A.2 中间件安全

中间件是一种独立的系统软件或服务程序。云计算环境下，不同的应用场景需要不同功能的中间件，主要包括消息处理中间件、缓存中间件、数据访问中间件等。中间件组件应具备高性能，支持独立的集群部署、完善的日志记录、多租户隔离，并提供良好的用户管理界面和用户操作审计功能。

基本要求：

a) 应提供身份识别和登录控制功能；

b) 针对中间件的所有操作，应提供完整的审计功能；

c) 应提供基于安全网络协议的接入方式。

扩展要求：

a) 应对运行在中间件中的不同租户之间的服务实例提供隔离机制；

b) 对中间件不同服务的通信，可提供协议和接口的安全控制。

增强要求：

应支持会话全生命周期的安全管理，包括会话的生成、隔离、保持、结束等环节，实现对会话信息的加密存储。

A.3 数据库安全

基本要求：

a) 应提供用户操作审计功能；

b) 应进行数据库安全加固，防止用户访问物理服务器上运行的其他用户的数据库实例；

c) 应支持用户可设定只允许云服务器从内网访问数据库服务；

d) 应提供白名单设置功能，用户可以设置 IP 白名单，仅允许指定源 IP 访问用户的数据库实例服务。

扩展要求：

应支持每个云服务使用者拥有自己的数据库管理员权限，数据库实例不可共用。

增强要求：

应支持每个云服务使用者的数据库部署在不同的存储设备上。

附 录 B
（资料性附录）
云计算的安全风险

B.1 安全责任风险

传统信息系统的安全责任主体是一个机构，安全责任较明确。在云计算环境下，信息系统由云服务使用者、云服务提供者等多方合作建设，其安全防护需要多方联合采取措施。不明确的安全责任划分、不科学的安全任务分工等可能使原本严密的防护机制产生安全缝隙，给云计算环境下的信息系统安全来一定挑战。

B.2 数据所有权风险

用户使用云服务时，不可避免地将数据存储到云计算平台上，使得云服务提供者具有访问和操作云服务使用者数据的能力。一方面，云服务提供者内部人员失职、云计算平台遭受攻击等多种原因，均可能导致数据丢失或隐私泄露；另一方面，云服务提供者掌握使用者的登录记录、操作习惯、访问轨迹、资源使用等大量数据，能够通过数据分析获取用户不愿公布的隐私信息。

B.3 服务滥用风险

云计算技术本身虽是中性的，但也容易被不法分子利用成为犯罪工具。不法分子可利用云服务获取大量廉价的主机、网络、存储等资源，进而从事DDoS攻击、暴力密码破解、非法信息传播、恶意软件发布等违法活动。

B.4 资源共享风险

为提升资源利用效率，云服务将软硬件资源分配给多个用户共享。从空间维度上，不同用户有可能共用一台物理服务器的内存、硬盘等资源，如隔离措施失效，可能干扰其他用户应用运行或导致信息泄露；从时间维度上，同一软硬件资源在不同时间被不同用户使用，如果资源在被重分配给新用户之前，没有进行完全的数据清除，新用户可能通过数据恢复技术还原之前用户的数据，从而带来数据泄露风险。

B.5 服务集中的风险

云计算平台汇集了大量用户的应用和数据资源，开放性高且基于网络提供服务，放大了系统故障或漏洞的危害。服务集中使云计算平台更易成为不法分子的攻击目标，一旦发生问题将导致大量用户服务的异常终止和数据泄露。

B.6 不安全接口的风险

云服务按照硬件、平台和应用软件等层次将标准API接口开放给用户，由用户按需与上层应用进行集成。由于这些标准API接口直接通过网络对外开放，并且用户可以使用各类终端设备通过互联网获取

云服务，因此存在注入攻击、密钥窃取、安全漏洞等安全性风险，同时也直接影响云计算平台的整体安全性。