ICS 35.020
L70

DB37

山　　东　　省　　地　　方　　标　　准

DB 37/T 3304—2018

信息安全技术 云计算运维安全管理规范

2018－06－12 发布　　2018－07－12 实施

山东省质量技术监督局　　发布

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由潍坊市质量技术监督局提出并归口。

本标准起草单位：潍坊市智慧潍坊建设办公室、山东瑞宁信息技术股份有限公司、山东省计算中心（国家超级计算济南中心）、山东省经济和信息化发展研究院、山东华国信息安全技术有限公司、山东信息协会、山东电子商会、山东正中信息技术股份有限公司。

本标准主要起草人：胡延年、李刚、汉京宁、王洋、周鸣乐、朱少伟、朱珊珊、李旺、冯正乾、李波、李敏、丁艳艳、李强、张玉瑞、张建成、柴力、刘波、戚元华、王玮、刘一鸣、潘洪华、牟宁芳。

本标准为首次发布。

信息安全技术 云计算运维安全管理规范

1 范围

本标准规定了云计算环境下运维安全管理的术语和定义、参考模型、安全管控、本地监控等内容。

本标准适用于提供公有云、私有云和混合云运维安全管理的机构及有云计算环境运维安全需求的用户。

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，仅所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。

GB/T 32400-2015 信息技术 云计算 概览与词汇

3 术语和定义

下列术语和定义适用于本文件。

3.1

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池按需自服务的方式供应和管理的模式。

注：资源包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 32400-2015,定义3.2.5]

3.2

云计算运维安全 cloud computing operation and maintenance security

在公有云、私有云和混合云环境中云计算基础设施及虚拟资源的运维安全。

3.3

云服务 cloud service

通过云计算已定义的接口提供的一种或者多种能力。

[GB/T 32400-2015,定义3.2.8]

3.4

云服务提供者 cloud service provider

提供云服务的参与方。

[GB/T 32400-2015,定义3.2.15]

3.5

云安全管控系统 cloud security reining system

一种部署在云计算环境中，对云计算环境中的运维过程安全进行管控的系统。

注：包括租户云安全管控系统和云服务提供者云安全管控系统。

3.6

混合云 hybrid cloud

至少包含两种不同的云部署模型的云部署模型。

[GB/T 32400-2015,定义3.2.23]

3.7

私有云 private cloud

云服务仅被一个云服务客户使用，且资源被云服务客户控制的一种云部署模型。

[GB/T 32400-2015,定义3.2.32]

3.8

公有云 public cloud

云服务可被任意云服务客户使用，且资源被云服务提供者控制的一种云部署模式。

[GB/T 32400-2015,定义3.2.33]

3.9

租户 tenant

对一组物理和虚拟资源进行共享访问的一个或者多个云服务用户。

[GB/T 32400-2015,定义3.2.37]

3.10

第三方监控 third-party supervision

通过第三方机构或组织，对云服务提供者提供的云计算服务过程进行安全审计监督，向租户提供可信的云计算安全审计报告。

3.11

看守器 guard

一种对云安全管控系统提供守护、监测、告警等功能的装置。

4 缩略语

下列缩略语适用于本文本。

VPN　虚拟专用网络（Virtual Private Network）

SSL　安全套接层（Secure Sockets Layer）

HTTPS　安全套接层超文本传输协议(Hyper Text Transfer Protocol over Secure Socket Layer)
WEB　万维网(World Wide Web)
APP　应用程序(Application)

5　安全管理参考模型

5.1　云计算运维安全管理参考模型如图 1 所示，模型中有云服务提供者、租户和第三方监控机构三种角色。

5.2　租户通过专属的云安全管控系统，采用技术手段，对所购买的云计算资源进行管控、运维管理，对租户购买的云计算资源的所有操作均应通过租户的授权审批，并应记录和审计所有操作。云服务提供者通过专属的云安全管控系统对云计算基础设施运维管理。

5.3　为保证云安全管控系统的安全，应在租户端设置看守器，实时监控用户端安全管控系统的自身安全。

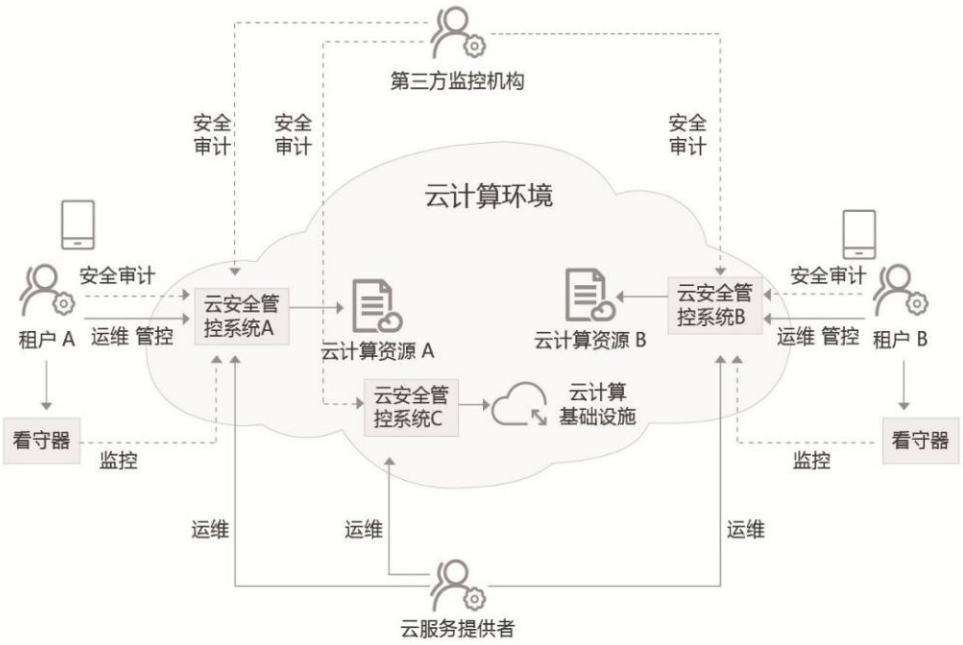

图1　云计算运维安全管理参考模型

6　安全管控

6.1　云计算资源运维统一入口

云安全管控系统作为租户和云服务提供者对云计算资源进行集中运维管控的统一入口，应：

a)　集中管控云计算资源访问人员和运维管理操作的人员；
b)　集中管理云计算资源的账号权限，并提供单点登录功能；
c)　由租户自行管理云安全管控系统的管理权限；
d)　提供认证、授权、访问控制、审计的能力；

e) 适应主流的云计算技术和环境；
f) 支持移动 APP、WEB 等方式。

6.2 云计算资源的安全掌控

租户通过云安全管控系统可获得云计算资源的安全掌控，包括：
a) 对所有运维访问进行授权；
b) 对所有运维操作的授权进行审批；
c) 对危险操作进行实时告警；
d) 对所有运维操作进行审计；
e) 对报表进行实时在线查询。

6.3 看守器

为保证云安全管控系统的安全，在租户本地部署看守器：
a) 看守器为独立硬件设备，支持双机热备功能；
b) 一个云安全管控系统使用一个看守器；
c) 一个看守器可监控多个云安全管控系统；
d) 看守器可安装在租户处，也可安装在第三方监控机构；
e) 看守器实时监控云安全管控系统的环境安全，监控信息包括不限于中央处理器信息、内存信息、用户登录信息等；
f) 看守器应实时报警，报警方式包括不限于短信告警、电子邮件告警等；
g) 可通过水印、数据加密、心跳监测、时间戳等手段确保看守器的安全。

7 本地监控

租户通过本地看守器监控云安全管控系统的状态。当出现异常时，看守器实时报警，并阻止通过云安全管控系统的运维行为。

8 第三方监控

第三方监控机构通过云安全管控系统对云基础设施运维工作进行安全审计。同时，第三方监控机构也可利用云安全管控系统的分级审计功能，对各租户的云计算资源的运维进行安全审计和监督。