ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

信息安全技术
云计算服务运行监管框架

Information Security Technology — Operation Supervision Framework of Cloud Computing Service

点击此处添加与国际标准一致性程度的标识

文稿版次选择

（本稿完成日期：）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准主要起草单位：四川大学、中国电子技术标准化研究院、中国电子集团信息技术研究院、中国电子科技集团公司第三十研究所、北京安信天行技术有限公司、西安未来国际信息股份有限公司、北京信息安全测评中心、中国信息安全测评中心、华为技术有限公司、阿里云计算有限公司、腾讯云计算有限公司、中国移动研究院、陕西省信息化工程研究院、杭州安恒信息技术有限公司、广州赛宝认证中心服务有限公司、中国电子科技网络信息安全有限公司、曙光信息产业股份有限公司。

本标准主要起草人：xxxx

引　言

云计算可提供高效、优质的IT服务。随着云计算技术的蓬勃发展，政府对采用云计算技术及云服务有了大量需求，为确保政府部门持续安全地使用云计算服务，确保云服务商的安全能力持续符合国家标准要求，确保云计算服务各相关方能够实时、有效地掌握云计算服务的运行质量和安全状态，保障政府部门的业务和数据采用云计算服务的安全，制定云计算服务持续监管框架。

本标准以GB/T 31167-2014《信息安全技术 云计算服务安全指南》标准为依据、以GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》标准为要求，GB/T 31167-2014面向政府部门，提出了使用云计算服务时的安全管理要求，GB/T 31168-2014面向云服务商，提出了云服务商在为政府部门提供云计算服务时应该具备的安全能力要求。本标准明确规范了政府部门云服务客户在使用云计算服务的过程中，云服务商、运行监管方的相关责任及监管内容，提出了运行监管框架、过程及方式。同时，本标准为云服务商制定和实施云计算服务运行监管策略和计划提供指导，也为运行监管方进行运行监管活动提供指导。

信息安全技术 云计算服务运行监管框架

1 范围

本标准针对云服务商提供云计算服务的运行监管环节，阐述了云计算服务运行监管框架、过程以及方式等内容，用于指导运行监管活动中的云服务商和运行监管机构的监管活动，为云服务商制定和实施云计算服务运行监管策略和计划、为运行监管方进行运行监管活动提供指导，以保障云计算服务安全能力持续达到云计算客户的安全需求。

本标准适用于政府部门采用云计算服务的运行监管活动，也可供重点行业和其他企事业单位使用云计算服务时参考。

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

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

3 术语和定义

GB/T 32400—2015 界定的以及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以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。

3.2

云服务 Cloud Service

通过云计算已定义的接口提供一种或多种能力。

3.3

云服务商 Cloud Service Provider

云计算服务的供应方。

3.4

云服务客户 Cloud Service Customer

为使用云服务而处于一定业务关系中的参与方。

注：业务关系不一定包含经济条款。

3.5

运行监管方 Operation Supervision Organization
独立于云计算服务相关方的专业监管机构。

3.6

第三方评估机构 Third Party Assessment Organizations (3PAO)
独立于云计算服务相关方的专业评估机构。

4 缩略语

下列缩略语适用于本文件。

CSC	Cloud Service Customer
CSP	Cloud Service Provider
OSO	Operation Supervision Organization
3PAO	Third Party Assessment Organization

5 云计算服务运行监管框架

5.1 概述

云计算服务运行监管应确保云服务商的云安全控制措施、重大变更管理及应急响应能力持续满足要求，应为云服务相关方提供云服务平台相关的安全信息以便其能及时地掌握云计算服务的安全状态。

5.2 运行监管框架

云计算服务运行监管框架是基于国家标准 GB/T 31167—2014《信息安全技术 云计算服务安全指南》和 GB/T 31168—2014《信息安全技术 云计算服务安全能力要求》中对云计算服务运行监管的安全要求而提出的。云计算服务运行监管框架如图 1 所示，

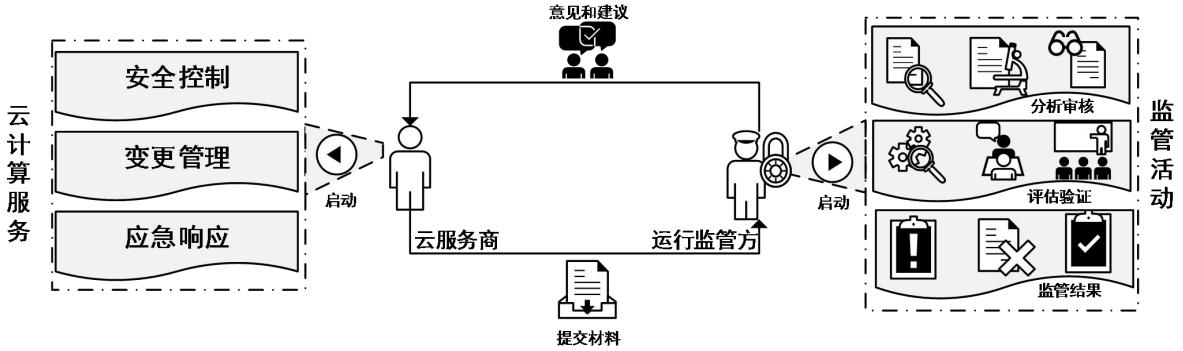

图 1 运行监管框架

云服务商持续监控云计算平台中安全控制、变更管理、应急响应策略、计划、规程及措施的实施，并记录相关信息及实施情况，形成证明材料交付件；云服务商应根据运行监管方需要的频率，定期提交证明材料交付件；运行监管方对云服务商提交的交付件进行分析审核、评估验证等监管活动，形成评估结果；必要时应根据评估结果给出合理的意见和建议。

5.2.1 运行监管角色

运行监管框架包含两个角色：

a) 云服务商：已经通过国家网络安全审查并授权提供云服务的供应方；
b) 运行监管方：云服务客户的管理部门（例如：政府信息安全管理部门、云服务客户的主管部门等）或由其指定或委托的第三方独立监管机构。

5.2.2 运行监管目的

运行监管的目的是保障：

a) 云计算服务持续满足国家相关法律法规、行政命令、指令、政策、条例和指导方针；
b) 云服务商严格履行 GB/T 31167—2014《信息安全技术 云计算服务安全指南》规定的运行监管责任；
c) 云计算服务安全能力持续满足国家标准 GB/T 31168—2014《信息安全技术 云计算服务安全能力要求》规定的要求；
d) 云计算服务相关方能够及时地、有效地掌握云计算服务的运行质量和安全状态；
e) 云计算服务的透明及可信；
f) 云计算服务的安全风险持续可控；
g) 云服务商不断提升云服务平台的安全能力。

5.2.3 运行监管内容

运行监管的内容应包含：

a) 云服务商在云服务平台中计划并实施的安全控制措施的有效性，确保云服务平台中的安全控制措施持续有效；
b) 云服务商在云服务平台中计划并实施的重大变更活动的情况，确保云服务平台中的重大变更活动风险可控；
c) 云服务商对云服务平台中的重大安全事件的响应情况，确保云服务平台中的应急响应活动及时充分。

5.2.4 运行监管活动

运行监管方应对云计算服务开展安全控制监管、变更管理监管和应急响应监管等活动，采用的方式可包含：

a) 分析审核：运行监管方对云服务商提交的有关安全控制、变更管理及应急响应相关的证明材料交付件进行分析及审核；
a) 评估验证：运行监管方根据分析、审核结果对云服务平台的安全风险进行评估，必要时应以抽查、核查及测试等方式对交付件中的内容进行验证；
b) 监管结果：运行监管方根据评估验证结论，形成评估报告并告知云服务商评估结果，必要时应给出合理的意见和建议。

5.2.5 运行监管职责

5.2.5.1 云服务商的职责

云服务商的监管职责如下：

a) 严格履行 GB/T 31167—2014《信息安全技术 云计算服务安全指南》中云服务商应承担的运行监管责任；
b) 严格履行 GB/T 31168—2014《信息安全技术 云计算服务安全能力要求》中应承担的监管责任；

c) 严格满足 GB/T 31168—2014《信息安全技术 云计算服务安全能力要求》中的安全能力要求；
d) 制定并实施安全控制策略与计划，确保安全控制措施持续有效；
e) 制定并实施重大变更策略与规程、配置管理计划与配置基线；
f) 制定并实施应急响应计划、重大安全事件处理策略；
g) 制定并实施持续监控策略与计划，针对云平台的控制措施、受控配置及运行状态实施监控；
h) 开展周期性的风险评估，在云平台发生重大安全事件时或实施重大变更后，应重新进行风险评估，将记录有评估结果的风险评估报告提交给运行监管方；
i) 按照运行监管方的要求记录有关安全控制措施、重大变更及应急响应的相关信息及实施情况并归档，以支撑运行监管活动。

5.2.5.2 运行监管方的职责

运行监管方的监管职责如下：

a) 监督云服务商履行 GB/T 31167—2014《信息安全技术 云计算服务安全指南》中应实施的运行监管措施；
b) 监督云服务商履行 GB/T 31168—2014《信息安全技术 云计算服务安全能力要求》中应实施的安全措施；
c) 监督云服务商达到 GB/T 31168—2014《信息安全技术 云计算服务安全能力要求》中的安全能力要求；
d) 制定并维护运行监管策略与计划，对云服务商的云服务平台实施运行监管活动；
e) 制定并维护运行监管活动中所需交付件的内容及格式要求，必要时应提供模版；
f) 定期接收云服务商提交的相关证明材料的交付件，对交付件内容进行分析、评估及审核；
g) 评估云服务商的安全控制策略与计划、安全控制措施并监督其实施情况，必要时应给出合理的意见和建议；
h) 评估云服务商的重大变更策略与规程、配置管理计划与配置基线并监督其实施情况，必要时应给出合理的意见和建议；
i) 评估云服务商的应急响应计划、重大安全事件处理策略并监督其实施情况，必要时应给出合理的意见和建议；
j) 定期对云服务商的云服务平台的安全性、透明性、可用性等安全属性实施全面分析与评估，形成评估报告并归档，必要时应给出合理的意见和建议。

6 云计算服务运行监管过程

6.1 概述

云计算服务运行监管过程主要针对云计算服务的安全控制、变更管理、应急响应的运行监管。云计算服务运行监管过程的一个重要作用就是要求云服务商提供证据以证明其云服务安全能力持续符合 GB/T 31168—2014 《信息安全技术 云计算服务安全能力要求》，证明其实施的安全控制措施的有效性、变更管理的合理性及应急响应的充分性。

云计算服务运行监管的活动包含三个部分：

a) 安全控制监管；
b) 变更管理监管；
c) 应急响应监管。

6.2 安全控制监管

安全控制监管有助于运行监管方对云服务商实施的安全控制措施有全面的认知，同时，方便运行监管方了解并掌握安全控制措施的运行情况，以便运行监管方分析、审核、评估、验证云服务平台的安全性及安全控制措施的有效性。

6.2.1 安全控制监管要求

6.2.1.1 云服务商的要求

a) 云服务商应：根据 GB/T 31168—2014 《信息安全技术 云计算服务安全能力要求》中相关安全能力要求制定安全控制策略与计划，并实施相应的安全控制措施；
b) 制定并实施持续监控策略，对已实施的安全控制措施进行持续监控；
c) 定期维护并更新云服务平台中的安全控制措施，确保其持续有效；
d) 定期对云服务平台中已实施的安全控制措施进行测评并形成测评报告；
e) 记录云服务平台中有关安全控制措施的相关信息及实施情况并归档；
f) 根据运行监管方的要求，提交有关安全控制措施的相关交付件。

6.2.1.2 运行监管方的要求

运行监管方应：
a) 监督云服务商严格履行安全控制策略与计划并实施安全控制措施；
b) 监督云服务商严格履行持续监控策略并对已实施的安全控制措施进行持续监控；
c) 分析、评估、审核云服务商提交的与安全控制措施相关的交付件，确保安全控制措施的合规性；
d) 监督云服务商对不合规的安全控制措施进行整改，并跟踪整改情况；
e) 根据需要的频率，以审查、抽查、测试、评估等方式对云服务商的安全控制措施的有效性进行验证；

6.2.2 安全控制监管的内容

安全控制监管的目的是要求云服务商提供能证明其实施的安全控制措施满足GB/T 31168—2014《信息安全技术 云计算服务安全能力要求》的交付件。通过国家网络安全审查并授权为政府部门提供云计算服务的云服务商，为保证审查结论持续有效，应以与运行监管方约定的时间点（天、周、月、年等）或运行监管方需要的频率定期提交能证明其安全控制措施有效性的交付件。

附录A中所示的是安全控制监管所要求提交的证明材料交付件。

6.2.3 安全控制监管流程

安全控制的监管流程如下：
a) 云服务商制定安全控制策略与计划，并实施安全控制措施；
b) 云服务商制定持续监控策略，并对已实施的安全控制措施进行持续监控；
c) 云服务商定期提交能证明其安全控制措施有效性的相关交付件，例如，运行监管方可根据 GB/T 31168—2014 《信息安全技术 云计算服务安全能力要求》中的相关安全能力要求提供《系统安全计划》、《系统风险持续改进》等证明材料模版，以便云服务商根据要求填写；
d) 运行监管方对云服务商提交的交付件进行分析、评估及审核，并将评审结果告知云服务商，例如，安全控制措施合规或安全控制措施不合规应限期整改等；
e) 云服务商应定期委托第三方评估机构或有评估资质的运行监管方对云服务平台中已实施的安全控制措施进行测评，安全测试内容包括但不限于云平台系统/组件、基础设施、数据库、物理环境等，并提交相应的测评报告给运行监管方，例如，《安全措施测评报告》、《渗透测试报

告》、《脆弱性扫描报告》等；

f) 运行监管方可根据云服务客户要求或安全监管需求，以审查、抽查、测试、评估等方式定期或不定期地对云服务商的安全控制措施的有效性进行验证；

g) 如果云服务商的安全控制措施不合规，运行监管方可要求云服务商对不合规的安全控制措施限期整改并跟踪整改情况，整改完成后重新进行评估、审核。

6.3 变更管理监管

变更管理过程有助于维持云服务平台的安全配置基线，预防重大安全事件的发生。云服务商应制定配置管理计划、变更管理方法、变更实施流程等策略与规程对例行的日常变更、安全变更、需求变更等进行安全地管理。在进行重大变更前，云服务商应对计划实施的变更进行安全影响分析以确保变更不会对云服务平台及客户业务环境的安全产生负面影响。

6.3.1 变更管理监管要求

6.3.1.1 云服务商的要求

云服务商应：

a) 制定并实施重大变更策略与规程、配置管理计划与配置基线；

b) 制定并维护云平台受控配置列表，明确重大变更项及需定期变更的配置项；

c) 定期对病毒库、入侵检测规则库、防火墙规则库、漏洞库等与云平台安全相关的重要配置项进行更新；

d) 在云平台上实施变更之前，应对变更项进行安全影响分析以确保该变更不会对云平台环境或云服务客户业务环境造成潜在的安全影响；

e) 在云平台上实施变更之前，对重大变更项进行测试、验证和记录；

f) 对重大变更实施物理和逻辑访问控制，并对变更动作进行审计；

g) 限制云计算系统开发方和集成方对云服务平台中的信息系统及软硬件和固件进行直接变更；

h) 定期对云计算系统的开发方和集成方掌握的变更权限进行审查和再评估；

i) 记录云服务平台中有关重大变更活动的相关信息及实施情况并归档；

j) 根据运行监管方的要求，提交有关重大变更活动的相关交付件。

6.3.1.2 运行监管方的要求

运行监管方应：

a) 监督云服务商严格履行重大变更策略与规程、配置管理计划与配置基线；

b) 监督云服务商定期更新并维护云平台受控配置列表、重大变更项及受控配置项；

c) 确保云服务商在在云服务平台上实施重大变更前，对变更项实施测试、验证及安全影响分析；

d) 定期对涉及云平台受控配置变更的有关活动进行审查；

e) 分析、审核云服务商提交的与重大变更活动相关的交付件，根据安全影响分析结果给出合理的意见和建议。

6.3.2 变更管理监管内容

重大变更涉及的主要内容包括但不限于：

a) 鉴别（包括身份鉴别和数据源鉴别）和访问控制措施进行变更；

b) 数据存储的实现方法的变更；

c) 云服务平台中软件代码的更新；

d) 备份机制和流程的变更；
e) 与外部服务商网络连接的变更；
f) 安全控制措施的变更；
g) 已部署的商业软硬件产品的替换；
h) 云计算服务分包商的变更，例如 PaaS、SaaS 服务商更换 IaaS 服务商。

6.3.3 变更管理监管流程

重大变更的监管流程如下：

a) 云服务商应制定并实施重大变更策略与规程、配置管理计划与配置基线；
b) 云服务商对云平台受控配置列表中的重大变更项及受控配置项进行持续监控；
c) 云服务商在实施重大变更之前，应以与运行监管方约定的时间提前通知运行监管方；
d) 云服务商在实施重大变更之前，应对变更项进行测试、验证及安全影响分析；
e) 云服务商应根据运行监管方的要求提供有关计划实施的重大变更的交付件，例如，运行监管方提供《重大变更情况》、《重大变更安全影响分析表》、《安全评估计划》等证明材料的模版，以便云服务商根据要求填写；
f) 运行监管方对云服务商提交的交付件进行分析、评估及审核，根据安全影响分析结果给出合理的意见和建议，必要时应协助云服务商更改重大变更计划。例如，如果云服务商计划实施的变更可能会增加安全风险或暴露出不能接受的其他风险，运行监管方应给出意见和建议：
   1) 变更计划合规，建议实施变更计划；
   2) 变更计划不合规，建议更改变更计划，重新提交评审；
   3) 变更存在安全风险，建议撤销变更计划。
g) 云服务商完成重大变更后，应将有关重大变更活动记录在案，在与运行监管方预先约定的时间内提交最新的有关云服务平台的安全评估报告，例如，云服务商委托第三方评估机构或有评估资质的运行监管方对云平台进行测评，然后将重大变更情况和评估结果形成《安全评估报告》、《变更说明》等交付件提交给运行监管方；
h) 运行监管方对云服务商的交付件进行审核，确保云服务商的重大变更活动的相关信息与实施情况与交付件中的内容一致。

6.4 应急响应监管

应急响应的目的是为了确保云服务相关方在发生安全事件时可以相互协调及沟通，并以团队协作的方式快速应对和解决安全事件。

云服务商应制定并维护应急响应计划以证明其有能力对重大安全事件做出及时、充分的响应。一旦发现重大安全事件，例如，拒绝服务攻击、恶意代码感染、非授权访问等，都应及时通知运行监管方，并及时对安全事件进行处理。

6.4.1 应急响应监管要求

6.4.1.1 云服务商的要求

云服务商应：

a) 制定并实施应急响应计划、重大安全事件处理策略；
b) 遵守变更管理过程中制定重大变更策略与规程、配置管理计划与配置基线；
c) 检测到重大安全事件时应及时处理并以适当的方式通知云服务相关方；
d) 记录云服务平台中有关应急响应活动的相关信息及实施情况并归档；

e) 根据运行监管方的要求，提交有关应急响应活动的相关交付件。

6.4.1.2 运行监管方的要求

运行监管方应：

a) 监督云服务商制定并实施应急响应计划、重大安全事件处理策略；
b) 监督云服务商的及时处理安全事件并跟踪处理进展直到闭环；
c) 协助云服务商处理重大安全事件并跟踪事件处理情况直到闭环；
d) 分析、审核云服务商提交的与应急响应活动相关的交付件，必要时应给出合理的意见和建议；

6.4.2 应急响应监管内容

涉及应急响应的安全事件包括但不限于：

a) 非授权访问事件，如对云服务平台下的业务系统、数据或其他计算资源进行非授权逻辑或物理访问等；
b) 拒绝服务攻击事件；
c) 恶意代码感染，如云服务平台被病毒、蠕虫、特洛伊木马等恶意代码感染；
d) 客户违反云计算服务的使用策略，例如发送垃圾邮件等。

6.4.3 应急响应监管流程

应急响应的监管流程如下：

a) 如果云服务商检测到可能会导致云服务客户的业务中断或对云服务客户数据的机密性和完整性有威胁的事件时，应通知可能受影响的云服务客户；
b) 通知完云服务客户后，云服务商应并与运行监管方进行沟通，以便运行监管方获得与此安全事件相关的信息；
c) 如果云服务商需要协助处理安全事件，运行监管方应协助云服务商及时处理安全事件；
d) 运行监管方应确保所有受影响的云服务客户都已经接收到云服务商的通知并知悉安全事件的有关信息、处理情况及安全影响；
e) 运行监管方应记录有关此应急响应活动的相关信息及处理情况；
i) 运行监管方对云服务商的交付件进行审核，确保云服务商的应急响应活动的相关信息与实施情况与交付件中的内容一致。

7 云计算服务运行监管的实现机制

7.1 概述

为了履行在运行监管活动中的责任，并实现运行监管的目的，运行监管方在运行监管过程中需要接收云服务商提交的有关安全能力的交付件。运行监管方应通过有效、准确、及时地方式接收交付件以便对云服务商的云服务安全能力实施分析、评估、审核、验证等活动。因此，云服务商应努力寻求自动化机制以降低人力、物力和时间成本，提升并改进运行监管过程的效率和可靠性，通过将人、过程及技术结合的方式来支撑运行监管活动。

7.2 自动机制

自动机制可增加运行监管过程的安全性并减少运行监管过程中用于处理重复性工作所花费的时间。自动化获取运行监管交付件的机制，可以用于对人与人之间交互的需求较少的处理过程。随着云服务平台自动机制的逐渐成熟与不断提高，最终应使用自动机制支撑整个运行监管过程。

7.2.1 主要内容

自动机制涉及的主要内容包括但不限于：

a) 限制对各类介质的访问，并对介质访问情况进行审计；
b) 对配置项的参数进行集中管理、应用和验证；
c) 检测云计算服务平台中新增的非授权软件、硬件或固件组件；
d) 维护信息系统组件清单；
e) 支持事件处理过程；
f) 支持事件报告过程；
g) 提高事件响应支持资源的可用性；
h) 对审查、分析和报告过程进行整合，以支持对可疑活动的调查和响应；
i) 比较不同时间的脆弱性扫描结果，以判断信息系统漏洞趋势；
j) 更新恶意代码防护机制；
k) 管理账号；
l) 监视和控制远程访问会话，以检测网络攻击，确保远程访问策略得以实现；
m) 对缺陷修复后的组件进行检测；
n) 对攻击事件进行准实时分析；
o) 温湿度控制

7.2.2 注意事项

云服务商在实现自动机制时应考虑：

a) 从各种信息源中提取信息；
b) 使用开放性规范或协议；
c) 提供与其他工具的可交互性；
d) 遵守国家相关法律、行政命令、指令、政策、条例、标准和指导方针；
e) 能够对安全控制、变更管理及应急响应过程中的信息进行整合并格式化输出。

附录 A 安全控制项

安全类	安全项	属性	内容	频率	负责方	交付件类型	备注（章节号）
系统开发与供应链安全	资源分配	一般要求	c）在工作计划和预算文件中，将信息安全作为单列项予以说明。	每年	云服务商	证据	5.2
	采购过程	一般要求	云服务商应根据相关法律、法规、政策和标准的要求，以及可能的客户需求，并在风险评估的基础上，将以下内容列入信息系统采购合同： a）安全功能要求。 b）安全强度要求。 c）安全保障要求。 d）安全相关文档要求。 e）保密要求。 f）开发环境和预期运行环境描述。 g）验收准则。 h）强制配置要求，如功能、端口、协议和服务。	每年	云服务商	证据	5.4
	开发过程、标准和工具	增强要求	c）按照[赋值：云服务商定义的频率]审查开发过程、标准、工具以及工具选项和配置，判定有关过程、标准、工具以及工具选项和配置是否满足[赋值：云服务商定义的安全需求]。 d）要求信息系统、组件或服务的开发商在开发过程的初始阶段定义质量度量标准，并以[选择:[赋值：云服务商定义的频率]；[赋值：云服务商定义的项目审查里程碑]；交付时]为节点，检查质量度量标准的落实情况。	每年	云服务商	证据	5.10
			i）要求信息系统、组件或服务的开发商即使在交付信息系统、组件或服务后，也应跟踪信息系统、组件或服务的漏洞情况，在发布漏洞补丁前便应通知云服务商，且应将漏洞补丁交由云服务商审查、验证并允许云服务商自行安装。	每月	云服务商	证据	
	开发商安全测试和评估	一般要求	a）制定并实施安全评估计划。 b）以[赋值：云服务商定义的深度和覆盖度]执行[选择：单元；集成；系统；回归]测试或评估。	每年	第三方评估机构	报告	5.12
		增强要求	e）要求信息系统、组件或服务的开发商按照[赋值：云服务商定义的约束条件]，以 [赋值：云服务商定义的广度和深度]执行渗透性测试。	每年	第三方评估机	报告	

					构		
				每年	云服务商	报告	
	组件真实性	增强要求	b）向[选择：正品厂商；[赋值：云服务商定义的外部报告机构]；[赋值：云服务商定义的人员和角色]；其他有关方面]报告赝品组件。 f）按照[赋值：云服务商定义的频率] 检查信息系统中是否有赝品组件。	每季度	云服务商	证据	5.15
	供应链保护	一般要求	b）确保[赋值：云服务商定义的重要设备]通过[赋值：政府和行业有关部门已设立的信息安全测评制度]的安全检测。	每年	云服务商	证据	5.17
系统与通信保护	边界保护	一般要求	a）在连接外部系统的边界和内部关键边界上，对通信进行监控；在客户之外的外部人员访问系统的关键逻辑边界和客户访问系统的关键逻辑边界上，对通信进行监控。 b）将允许外部公开直接访问的组件，划分在一个与内部网络逻辑隔离的子网络上。并确保允许外部人员访问的组件与允许客户访问的组件在逻辑层面实现严格的网络隔离。 c）确保与外部网络或信息系统的连接只能通过严格管理的接口进行，根据云服务商的安全架构，该接口上应部署有边界保护设备。	实时	云服务商	证据	
		增强要求	a）为云计算服务搭建物理独立的计算平台、存储平台、内部网络环境及相关维护、安防、电源等设施，并经由受控边界与外部网络相连。 g）构建物理上独立的管理网络，连接管理工具和被管设备或资源，以对云计算平台进行管理。	每年	云服务商	证据	6.2
			c）采取以下措施： 1）对每一个外部的电信服务接口进行管理。 2）为每一个接口制定通信流策略。 3）采取有关措施对所传输的信息流进行必要的保密性和完整性保护。 4）当根据业务需要，出现通信流策略的例外情况时，将业务需求和通信持续时间记录到通信流策略的例外条款中。 5）按照[赋值：云服务商定义的频率]，对网络通信流策略中的例外条款进行审查，在通信流策略中删除不再需要的例外条款。	根据需要	云服务商	证据	

	恶意代码防护	一般要求	c）配置恶意代码防护机制，以： 1）按照[赋值：云服务商定义的频率]定期扫描信息系统，以及在[选择：终端；网络出入口]下载、打开、执行外部文件时对其进行实时扫描。 2）当检测到恶意代码后，实施[选择：阻断或隔离恶意代码；向管理员报警；[赋值：云服务商定义的活动]]。 d）及时掌握系统的恶意代码误报率，并分析误报对信息系统可用性的潜在影响。	每季度	云服务商	证据	6.11
访问控制	鉴别凭证管理	一般要求	a）通过以下步骤管理鉴别凭证： 4)针对鉴别凭证的初始分发、丢失处置以及收回，建立和实施管理规程。 6）明确鉴别凭证的最小和最大生存时间限制以及再用条件。	每两年	云服务商	证据	7.5
			a）通过以下步骤管理鉴别凭证： 7）对[赋值：云服务商定义的鉴别凭证]，强制要求在[赋值：云服务商定义的时间段]之后更新鉴别凭证。 b）对于基于口令的鉴别： 4)强制执行最小和最大生存时间限制，以满足[赋值：云服务商定义的最小生存时间和最大生存时间]。	每季度	云服务商	证据	
	账号管理	一般要求	i）按照[赋值：云服务商定义的频率]，检查账号是否符合账号管理的要求。	每年	云服务商	证据	7.8
		增强要求	b）在[赋值：云服务商定义的时间段]后自动[选项：删除；禁用]临时和应急账号。 c）在[赋值：云服务商定义的时间段]后自动关闭非活跃账号。	每季度	云服务商	证据	
	无线访问	一般要求	云服务商应禁用无线网络直接访问云计算平台。	实时	云服务商	证据	7.20
	可供公共访问的内容	一般要求	d）按照[赋值：云服务商定义的频率]审查公开发布的信息中是否含有非公开信息，一经发现，立即删除。	每季度	云服务商	证据	7.23

配置管理	配置管理计划	增强要求	a）制定并实施云计算平台的配置管理计划。 b）在配置管理计划中，规定配置管理相关人员的角色和职责，并详细规定配置管理的流程。 c）在系统生命周期内，建立配置项标识和管理流程。 d）定义信息系统的配置项并将其纳入配置管理计划。 e）保护配置管理计划，以防非授权的泄露和变更。	每年	云服务商	证据	8.2
	变更控制	一般要求	d）审查所提交的信息系统受控配置的变更事项，根据安全影响分析结果进行批准或否决，并记录变更决定。 e）保留信息系统中受控配置的变更记录。 f）按照[赋值：云服务商定义的频率]对与系统受控配置的变更有关的活动进行审查。	每年	云服务商	证据	8.4
	最小功能原则	增强要求	a）按照[赋值：云服务商定义的频率]，对信息系统进行审查，以标识不必要或不安全的功能、端口、协议或服务。 b）关闭[赋值：云服务商定义的不必要或不安全的功能、端口、协议和服务]。 c）信息系统应按照[选择：[赋值：云服务商定义的软件使用与限制策略]；对软件使用的授权规则]，禁止运行相关程序。 d）按照白名单策略，确定[赋值：云服务商定义的在云计算平台上允许运行的软件]，禁止非授权软件在云计算平台上运行，并按照[赋值：云服务商定义的频率]，审查和更新授权软件列表。	每月	云服务商	证据	8.6
	信息系统组件清单	一般要求	a）制定和维护信息系统组件清单，该清单应满足下列要求： 1）能准确反映当前信息系统的情况。 2）与信息系统边界一致。 3）达到信息安全管理所必要的颗粒度。 4）包含[赋值：云服务商定义的为实现有效的资产追责所必要的信息]。 b）按照[赋值：云服务商定义的频率]，审查并更新信息系统组件清单。	每年	云服务商	证据	8.7
		增强要求	a）按照[赋值：云服务商定义的频率]，使用自动机制检测云计算服务平台中新增的非授权软件、硬件或固件组件。	实时	云服务商	证据	
维护	远程维护	一般要求	f）对所有远程维护和诊断活动进行审计，按照[赋值：云服务商定义的频率]对所有远程维护和诊断会话的记录进行审查。	每年	云服务商	证据	9.4

	维护人员	一般要求	a）建立对维护人员的授权流程，对已获授权的维护组织或人员建立列表。	每年	云服务商	证据	9.5
	缺陷修复	一般要求	a）标识、报告和修复云计算平台的缺陷。 b）在与安全相关的软件和固件升级包发布后，及时安装升级包。	每月	云服务商	证据	9.7
		增强要求	云服务商应使用自动检测机制，按照[赋值：云服务商定义的频率]对缺陷修复后的组件进行检测。	每月	云服务商	证据	
	安全功能验证	一般要求	a）验证[赋值：云服务商定义的安全功能]是否正常运行。	每月	云服务商	证据	9.8
	软件、固件、信息完整性	增强要求	a）按照[赋值：云服务商定义的频率]对云计算平台进行完整性扫描，并重新评估软件、固件和信息的完整性。	每月	云服务商	证据	9.9
应急响应与灾备	事件处理计划	一般要求	a）制定信息系统的事件处理计划，该计划应： 1）说明启动事件处理计划的条件和方法。 2）说明事件处理能力的组织结构。 3）定义需要报告的安全事件。 4）提供组织内事件处理能力的度量目标。 5）定义必要的资源和管理支持，以维护和增强事件处理能力。 6）由[赋值：云服务商定义的人员或角色]审查和批准。 b）向[赋值：云服务商定义的人员、角色或部门]，发布事件处理计划。 c）按照[赋值：云服务商定义的频率]，审查事件响应计划。 d）如系统发生变更或事件响应计划在实施、执行或测试中遇到问题，及时修改事件处理计划并通报[赋值：云服务商定义的人员、角色或部门]。 e）防止事件处理计划非授权泄露和更改。	每年	云服务商	证据	10.2
	事件处理	一般要求	c）将当前事件处理活动的经验，纳入事件处理、培训及演练计划，并实施相应的变更。	每年	云服务商	证据	10.3
	事件报告	一般要求	a）根据应急响应计划，监控和报告安全事件。 b）当发现可疑的安全事件时，在[赋值：云服务商定义的时间段]内，向本组织的事件处理部门报告。 c）建立事件报告渠道，当发生影响较大的安全事件时，向国家和地方应急响应组织及有关信息安全主管部门报告。	实时	云服务商	证据	10.4
				根据需要	云服务商	报告	

	应急响应计划	一般要求	c）按照[赋值：云服务商定义的频率]更新应急响应计划。	每年	云服务商	证据	10.8
			d）如系统发生变更或应急响应计划在实施、执行或测试中遇到问题，及时修改应急响应计划并向[赋值：云服务商定义的人员、角色或部门]及客户进行通报。	根据需要	云服务商	证据	
	应急培训	一般要求	a）向[赋值：云服务商定义的人员或角色]提供应急响应培训。 b）当信息系统变更时，或按照[赋值：云服务商定义的频率]，重新开展培训。	每年	云服务商	证据	10.9
	应急演练	一般要求	a）至少每年制定或修订应急演练计划，并与客户充分协商，听取客户意见。 b）按照[赋值：云服务商定义的频率]，执行应急演练计划，并且至少在演练开始前[赋值：云服务商与客户确定的时间]之前通知客户和相关部门。	每年	云服务商	证据	10.10
	信息系统备份	一般要求	a）具备系统级备份能力，按照[赋值：云服务商定义的频率]，对信息系统中的系统级信息进行备份，如系统状态、操作系统及应用软件。 e）具有验证信息系统备份连续有效的方法，并按照[赋值：云服务商定义的频率]进行验证。	每年	云服务商	证据	10.11
审计	可审计事件	一般要求	c）制定信息系统内需连续审计的事件清单，并确定各事件的审计频率，该清单为上述可审计事件清单的子集。	每年	云服务商	证据	11.2
		增强要求	云服务商应按照[赋值：云服务商定义的频率]对可审计清单进行审查和更新。	实时	云服务商	证据	
	审计的审查、分析和报告	一般要求	a）按照[赋值：云服务商定义的频率]对审计记录进行审查和分析，以发现[赋值：云服务商定义的不当或异常活动]，并向[赋值：云服务商定义的人员或角色]报告。	每周	云服务商	证据	11.6
风险评估与持续监控	策略与规程	一般要求	b）按照[赋值：云服务商定义的频率] 或当需要时，审查和更新综合风险管理策略、风险评估策略、持续性的监控策略及相关规程。	每三年	云服务商	证据	12.1
				根据需要	云服务商	证据	
	风险评估	一般要求	b）按照[赋值：云服务商定义的频率]定期开展风险评估，或者在信息系统或运行环境发生重大变更（包括发现新的威胁和漏洞）时，或者在出现其他可能影响系统安全状态的条件时，重新进行	每年	云服务商	证据	12.2

			风险评估。 c）将评估结果记录在风险评估报告中，并将风险评估结果发布至[赋值：云服务商定义的人员或角色]。 d）根据风险评估报告，有针对性地对云计算平台信息系统进行安全整改，将风险降低到[赋值：云服务商定义的可接受的水平]。	根据需要	云服务商	证据	
	脆弱性扫描	一般要求	a）使用脆弱性扫描工具和技术，按照[赋值：云服务商定义的频率]对云计算平台信息系统及其上的应用程序进行脆弱性扫描，并标识和报告可能影响该系统或应用的新漏洞。 b）根据风险评估或脆弱性扫描结果，在[赋值：云服务商定义的响应时间段]内修复漏洞。	每月	云服务商	证据	12.3
		增强要求	a）确保所使用的脆弱性扫描工具具有迅速更新漏洞库的能力。 b）按[选择：[赋值：云服务商定义的频率]；启动新的扫描前；新的漏洞信息发布后]更新信息系统漏洞库。	实时	云服务商	证据	
			d）在脆弱性扫描活动中，使用特权账号对[赋值：云服务商定义的信息系统组件]进行[赋值：云服务商定义的脆弱性扫描行动]，以实现更全面扫描。	每月	云服务商	证据	
			c）确保所使用的脆弱性扫描工具能够展现扫描所覆盖的广度和深度（如已扫描的信息系统组件和已核查的漏洞）。	每月	云服务商	报告	
				每年	第三方评估机构	报告	
	持续监控	一般要求	a）制定持续性的监控策略，并实施持续性监控，内容包括： 1）确定待监控的度量指标。 2）确定监控频率。 c）根据持续性监控策略，对已定义的度量指标进行持续的安全状态监控。 d）对评估和监控产生的安全相关信息进行关联和分析。 e）对安全相关信息分析结果进行响应。	实时	云服务商	证据	12.4
			f）按照[赋值：云服务商定义的频率]向[赋值：云服务商定义的人员或角色]报告信息系统安全状态。	每月	云服务商	证据	
		增强	云服务商应每年安排实施未事先声明的渗透性测	每年	云服	证据	

		要求	试以及深度检测，以验证系统的安全状态。		务商		
				每年	第三方评估机构	报告	
	信息系统监测	一般要求	a）能够针对[赋值：云服务商定义的监测目标]，发现攻击行为。 b）能够检测出非授权的本地、网络和远程连接。 c）能够通过[赋值：云服务商定义的技术和方法]，发现对信息系统的非授权使用。 d）能够对入侵监测工具收集的信息进行保护，防止非授权访问、修改或删除。 e）当威胁环境发生变化、信息系统风险增加时，提升信息系统监测级别。 f）确保信息系统监控活动符合关于隐私保护的相关政策法规。 g）按照需要或[赋值：云服务商定义的频率]，向[赋值：云服务商定义的人员或角色]提供[赋值：云服务商定义的信息系统监控信息]。	实时	云服务商	证据	12.5
		增强要求	a）使用自动工具对攻击事件进行准实时分析。 b）信息系统应按照[赋值：云服务商定义的频率]监测进出的通信，以发现异常或非授权的行为。 c）当下述迹象发生时，信息系统应向[赋值：云服务商定义的人员或角色]发出警报： 1）受保护的信息系统文件或目录在没有得到正常的变更或配置管理渠道通知的情况下被修改。 2）当发生异常资源消耗时。 3）审计功能被禁止或修改，导致审计可见性降低。 4）审计或日志记录在无法解释的情况下被删除或修改。 5）预期之外的用户发起了资源或服务请求。 6）信息系统报告了管理员或关键服务账号的登录失败或口令变更情况。 7）进程或服务的运行方式与系统的一般情况不符。 8）在生产系统上保存或安装与业务无关的程序、工具、脚本。 d）防止非授权用户绕过入侵检测和入侵防御机制。 e）对信息系统运行状态（包括CPU、内存、网络）进行监视，并能够对资源的非法越界使用发出警	实时	云服务商	证据	

			报。				
	垃圾信息监测	一般要求	a）在系统的出入口和网络中的工作站、服务器或移动计算设备上部署垃圾信息监测与防护机制，以检测并应对电子邮件、电子邮件附件、web 访问或其他渠道的垃圾信息。 b）在出现新的发布包时，及时更新垃圾信息监测与防护机制。	实时	云服务商	证据	12.6
安全组织与人员	安全组织	一般要求	a）建立管理框架来启动和控制组织内信息安全的实现： 1）设立[赋值：云服务商定义的人员或角色]作为信息安全的第一负责人，由本组织最高管理层人员担任。 2）设立[赋值：云服务商定义的部门]作为信息安全的责任部门，并通过[赋值：云服务商定义的机制]与本组织其他业务部门协调。 b）建立[赋值：云服务商定义的机制]，以保持与[赋值：云服务商定义的外部组织]的适当联系。 c）实施内部威胁防范程序，包括跨部门的内部威胁事件处理团队。	每两年	云服务商	证据	13.2

	安全规章制度	一般要求	a）制定信息安全规章制度，并传达至内外部相关人员。 b）在信息安全策略或计划发生变更时，或者按照[赋值：云服务商定义的频率]，评审和更新信息安全规章制度，以确保其持续的适用性和有效性。	每年	云服务商	证据	13.4
	人员筛选	一般要求	a）确保授权访问信息系统的人员已经经过筛选，人员背景信息和筛选结果应可供客户查阅。 b）按照[赋值：云服务商定义的再筛选条件和频率]，审查访问人员的再筛选结果。	每五年	云服务商	证据	13.6
	访问协议	一般要求	a）制定云计算平台的访问协议。 b）按照[赋值：云服务商定义的频率]，评审和更新该访问协议。 c）确保云计算平台的访问人员： 1）在被授予访问权之前，签署合适的访问协议。 2）根据工作需要，或者按照[赋值：云服务商定义的频率]，重新签署访问协议。	每年	云服务商	证据	13.9
	安全培训	一般要求	a）在以下情况下为信息系统用户（包括管理层人员和合同商）提供基础的安全意识培训： 1）作为新用户初始培训的一部分。 2）在因信息系统变更而需要时。 3）按照[赋值：云服务商定义的频率]。 b）在以下情况下为被分配了安全角色和职责的人员提供基于角色的安全技能培训： 1）在授权访问信息系统或者执行所分配的职责之前。 2）在因信息系统变更而需要时。 3）按照[赋值：云服务商定义的频率]。 d）按照[赋值：云服务商定义的时间段]，保存人员的培训记录。	每年	云服务商	证据	13.12
物理与环境安全	物理环境访问授权	一般要求	a）制定和维护具有机房访问权限的人员名单。	每三年	云服务商	证据	14.4
			c）按照[赋值：云服务商定义的频率]对授权人员名单和凭证进行审查。	每年	云服务商	证据	
	物理环境访问控制	一般要求	a）对所有机房的[赋值：云服务商定义的机房出入点]实施物理访问授权，具体包括：在准许进入机房前验证其访问授权、使用[赋值：云服务商定义的物理访问控制系统或设备]或警卫实施机房出入控制等。 b）制定和维护[赋值：云服务商定义的出入点]的物理访问审计日志。	每年	云服务商	证据	14.5

			f）按照[赋值：云服务商定义的频率]对[赋值：云服务商定义的物理访问设备]进行盘点。 g）按照[赋值：云服务商定义的频率]或在钥匙丢失、访问凭证受损以及相关人员发生变动的情况下，更换钥匙和访问凭证。	每年	云服务商	证据	
				根据需要	云服务商	证据	
	物理访问监控	一般要求	b）按照[赋值：云服务商定义的频率]，或当[赋值：云服务商定义的事件发生或有迹象发生]时，对物理访问日志进行审查。	每月	云服务商	证据	14.8
	访客访问记录	一般要求	a）制定和维护云计算平台机房的访客访问记录，并保留至[赋值：云服务商定义的时间段]。 b）按照[赋值：云服务商定义的频率]对访问记录进行审查。	每月	云服务商	证据	14.9
	温湿度控制能力	一般要求	a）维护云计算平台所在机房的温湿度，使其符合GB 50174-2008《电子信息系统机房设计规范》的相关规定。 b）实时监控温湿度水平。	实时	云服务商	证据	14.13

参考文献

[1] GB/T 32400-2015 信息技术 云计算 概览与词汇

[2] GB/T 31167—2014 信息安全技术 云计算服务安全指南

[3] GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

[4] GB/T 32399-2015 信息安全技术 云计算参考架构

[5] GB/T 24363—2009 信息安全技术 信息安全应急响应计划规范

[6] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

[7] FedRAMP Continuous Monitoring Strategy & Guide. Version 2.0, June 6, 2014

[8] FedRAMP Incident Communications Procedure. Version 1.0, April 8, 2013

[9] NIST Specail Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. September 2011