



中华人民共和国国家标准

GB/T 37972—2019

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

2019-08-30 发布

2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

目 次

前言	I
引言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 云计算服务运行监管目的及框架	1
4.1 运行监管目的	1
4.2 运行监管框架	1
4.3 运行监管的角色及责任	2
5 安全控制措施监管	3
5.1 安全控制措施内容	3
5.2 安全控制措施监管环节	3
6 变更管理监管	3
6.1 变更管理内容	3
6.2 变更管理监管环节	4
7 应急响应监管	4
7.1 应急响应内容	4
7.2 应急响应监管环节	4
8 云计算服务运行监管的实现方式	4
8.1 概述	4
8.2 人工机制	4
8.3 自动机制	5
附录 A (资料性附录) 运行监管交付件模版	6
附录 B (资料性附录) 安全控制措施运行监管列表	10
参考文献	18

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:四川大学、中国电子技术标准化研究院、北京安信天行技术有限公司、北京信息安全测评中心、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、中国移动通信有限公司研究院、广州赛宝认证中心服务有限公司、西安未来国际信息股份有限公司、陕西省信息化工程研究院、中国电子科技网络信息安全有限公司。

本标准主要起草人:陈兴蜀、罗永刚、李想、刘小茵、上官晓丽、钟金鑫、赵章界、葛龙、王伟、王永霞、张磊、沈锡庸、杨思磊、葛小宇、王惠莅、白杨、王启旭、胡影。

引 言

随着云计算技术的蓬勃发展,政府部门及重点行业等对采用云计算服务有了大量需求,为确保云服务客户安全地使用云计算服务,确保云服务商的安全能力符合国家相关标准要求,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,制定云计算服务运行监管框架。

本标准以 GB/T 31167—2014《信息安全技术 云计算服务安全指南》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》为要求,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,本标准为云服务商支撑云计算服务运行监管活动提供指导,为运行监管方开展运行监管提供指导。

信息安全技术

云计算服务运行监管框架

1 范围

本标准确定了云计算服务运行监管框架,规定了安全控制措施监管、变更管理监管和应急响应监管的内容及监管活动,给出运行监管实现方式的建议。

本标准适用于对政府部门使用的云计算服务进行运行监管,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 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 31167—2014 界定的以及下列术语和定义适用于本文件。

3.1

运行监管方 operation supervision organization

独立于云计算服务相关方,且具有专业技术能力,开展运行监管的机构。

4 云计算服务运行监管目的及框架

4.1 运行监管目的

开展云计算服务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、政策和标准;
- b) 云计算服务相关方能够及时、有效地掌握云计算平台的运行质量和安全状态;
- c) 云计算服务的安全风险可控;
- d) 云计算服务的安全能力持续满足要求。

从而确保 GB/T 31167—2014 中 8.1 提出的运行监管主要目标。

4.2 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 和 GB/T 31168—2014 中的运行监管要求而提出的。云计算服务运行监管框架如图 1 所示。