



中华人民共和国公共安全行业标准

GA/T 2347—2025

信息安全技术 网络安全等级保护 云计算测评指引

Information security technology—Testing and evaluation guidelines for cloud
computing for classified protection of cybersecurity

2025-10-13 发布

2026-02-01 实施

中华人民共和国公安部 发布

目次

前言Ⅲ

引言Ⅳ

1 范围1

2 规范性引用文件1

3 术语和定义1

4 缩略语2

5 概述2

6 信息收集和分析2

7 测评对象确定3

8 确定依据5

参考文献27

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由公安部网络安全保卫局提出。

本文件由公安部信息系统安全标准化委员会归口。

本文件起草单位：公安部第三研究所、公安部网络安全保卫局、公安部第一研究所、深信服科技股份有限公司、华为技术有限公司、阿里云计算有限公司、北京卓识网安技术股份有限公司、中电信数智科技有限公司、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、安徽省电子产品监督检验所、广西网信信息技术有限公司。

本文件主要起草人：张振峰、陶源、伊玮珑、张秀东、任彬、李秋香、刘卜瑜、黄敏、王睿超、刘韧、李景清、刘琛、王理冬、冯伟、张鹏。

引 言

为配合《中华人民共和国网络安全法》的实施,落实国家网络安全等级保护制度,更好地指导网络安全检测评估机构在云计算环境下开展网络安全等级保护测评工作,加强、规范网络安全等级保护测评工作的独立性、客观性、合规性及有效性,依据网络安全等级保护 2.0 相关系列标准,制定网络安全等级保护云计算测评指引。

信息安全技术 网络安全等级保护 云计算测评指引

1 范围

本文件给出了云计算平台和云服务客户的业务应用系统开展网络安全等级保护测评活动的指引。

本文件适用于网络安全检测评估机构对云计算平台和云服务客户的业务应用系统开展网络安全等级保护测评活动,网络安全监管部门参照使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 22239—2019 信息安全技术 网络安全等级保护基本要求
GB/T 28449—2018 信息安全技术 网络安全等级保护测评过程指南
GB/T 31167—2023 信息安全技术 云计算服务安全指南
GB/T 32400—2015 信息技术 云计算 概览与词汇

3 术语和定义

GB/T 22239—2019、GB/T 31167—2023 和 GB/T 32400—2015 界定的以及下列术语和定义适用于本文件。

3.1

云服务商 cloud service provider

提供云计算服务的参与方。

[来源:GB/T 31167—2023,3.4]

3.2

云服务客户 cloud service customer

为使用云计算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。

[来源:GB/T 31167—2023,3.5]

3.3

云计算平台 cloud computing platform

云服务商提供的云计算基础设施及其上的服务软件的集合。

[来源:GB/T 31167—2023,3.8]

3.4

云计算环境 cloud computing environment

云服务商提供的云计算平台,及客户在云计算平台之上部署的软件及相关组件的集合。

[来源:GB/T 31167—2023,3.9]

4 缩略语

下列缩略语适用于本文件。

IaaS:基础设施即服务(Infrastructure as a Service)

PaaS:平台即服务(Platform as a Service)

SaaS:软件即服务(Software as a Service)

5 概述

5.1 网络安全等级保护云计算测评指针对云计算环境中的等级保护对象开展的网络安全等级保护测评。网络安全等级保护测评过程主要包括四个基本测评活动:测评准备活动、方案编制活动、现场测评活动、报告编制活动,应符合 GB/T 28449—2018 的规定。

5.2 云计算环境中的等级保护对象包括以下两类:

——云计算平台;

——云服务客户的业务应用系统。

5.3 云计算平台和云服务客户的业务应用系统的网络安全等级保护测评包括安全通用要求和云计算安全扩展要求。云计算安全扩展要求主要涉及的控制点包括基础设施位置、网络架构、网络边界的访问控制、网络边界的入侵防范、网络边界的安全审计、集中管控、计算环境的身份鉴别、计算环境的访问控制、计算环境的入侵防范、镜像和快照保护、数据完整性和保密性、数据备份恢复、剩余信息保护、云服务商选择、供应链管理和云计算环境管理。

5.4 云计算平台和云服务客户的业务应用系统网络安全等级保护测评宜根据被测系统的类别、部署模式、服务模式、安全主体是否一致、技术实现方式等情况,充分收集和分析被测系统信息、确定被测对象、选择测评指标。

6 信息收集和分析

6.1 云计算平台

被测系统类别为云计算平台时,需明确以下内容:

——云计算平台的定级情况;

——云平台部署模式,包括:公有云、私有云、混合云;

——云计算服务模式,包括:IaaS、PaaS、SaaS;

——云基础设施物理机房地地点/逻辑位置信息及运维地点。

6.2 云服务客户的业务应用系统

被测系统类别为云服务客户的业务应用系统时,需明确以下内容。

——所在云平台部署模式,包括:公有云、私有云、混合云。

——云服务客户的业务应用系统所选用的云计算服务模式。云服务客户的业务应用系统可根据业务选择,选用某一个或多个云服务商的单一或多种混合的服务模式。系统调研时,需明确云服务客户的业务应用系统所选用的云计算服务模式,包括:IaaS、PaaS、SaaS,同时还应了解云服务客户的业务应用系统使用的云产品(服务)情况。

——所部署的云计算平台定级情况及网络安全等级保护测评情况,如云计算平台的网络安全等级保护测评报告编号、网络安全等级保护测评结论以及网络安全等级保护测评主要问题及整改情况。

——所在云计算平台云基础设施逻辑位置信息及云服务客户的业务应用系统的运维所在地。

7 测评对象确定

7.1 确定原则和要点

7.1.1 确定测评对象时宜遵循以下原则：

- 重要性,选择对被测定级对象来说重要的服务器、数据库和网络设备等；
- 安全性,选择对外暴露的网络边界；
- 共享性,选择共享设备和数据交换平台/设备；
- 全面性,选择尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统类型；
- 符合性,选择的设备、软件系统等能符合相应等级的测评强度要求。

7.1.2 针对云计算平台和云服务客户的业务应用系统的不同服务模式,宜重点测评以下内容：

- 虚拟设备,包括虚拟机、虚拟网络设备、虚拟安全设备；
- 云计算服务软件、云业务管理平台、虚拟机监视器、云产品(服务)；
- 云服务客户网络控制器、云应用开发平台等。

7.2 云计算平台

根据云计算平台不同服务模式选择测评对象见表 1。

表 1 云计算平台测评对象

服务模式	安全层面	测评对象
IaaS	安全物理环境	物理机房、云计算基础设施部署的相关机房及基础设施
	安全管理	安全策略、管理制度、岗位设置、人员配备、人员录用、人员离岗、安全建设、安全运维及相关记录
	安全管理中心	云管理平台、云平台监控系统
	安全区域边界	物理网络边界、虚拟网络边界
	安全通信网络	网络架构、物理链路、通信数据
	安全计算环境	云计算服务软件、虚拟机监视器、云业务管理系统、云产品(服务) 虚拟网络/安全设备、虚拟机镜像 云产品(服务)服务器(虚拟机)、宿主机、终端、云管平台服务器 网络设备、安全设备 云业务管理平台数据(业务数据、配置数据、鉴别信息、审计数据、镜像文件、快照数据、个人信息)
PaaS (依托 IaaS 平台构建)	安全管理	安全策略、管理制度、岗位设置、人员配备、人员录用、人员离岗、安全建设、安全运维及相关记录
	安全管理中心	云管理平台、云平台监控系统
	安全区域边界	虚拟网络边界
	安全通信网络	网络架构、虚拟链路、通信数据
	安全计算环境	虚拟机、数据库服务、中间件、云应用开发平台、云产品(服务)等
PaaS (依托非 IaaS 平台物理设备构建)	安全物理环境	物理机房、云计算基础设施部署的相关机房及基础设施
	安全管理	安全策略、管理制度、岗位设置、人员配备、人员录用、人员离岗、安全建设、安全运维及相关记录

表 1 云计算平台测评对象（续）

服务模式	安全层面	测评对象
PaaS (依托非 IaaS 平台物理设备构建)	安全管理中心	云管理平台、云平台监控系统
	安全区域边界	物理网络边界、虚拟网络边界
	安全通信网络	网络架构、物理链路、通信数据
	安全计算环境	云计算服务软件、虚拟机监视器、云业务管理系统、云产品(服务) 虚拟网络/安全设备、虚拟机镜像 云产品(服务)服务器(虚拟机)、宿主机、终端、云管平台服务器 网络设备、安全设备 云业务管理平台数据(业务数据、配置数据、鉴别信息、审计数据、镜像文件、快照数据、个人信息) 虚拟机、数据库服务、中间件、云应用开发平台、云产品(服务)等
SaaS (依托 IaaS 平台构建)	安全管理	安全策略、管理制度、岗位设置、人员配备、人员录用、人员离岗、安全建设、安全运维及相关记录
	安全管理中心	云管理平台、云平台监控系统
	安全区域边界	虚拟网络边界
	安全通信网络	网络架构、虚拟链路、通信数据
	安全计算环境	SaaS 业务应用软件 虚拟机、数据库服务、中间件、云应用开发平台、云产品(服务)等
SaaS (依托非 IaaS 平台物理设备构建)	安全物理环境	物理机房、云计算基础设施部署的相关机房及基础设施
	安全管理	安全策略、管理制度、岗位设置、人员配备、人员录用、人员离岗、安全建设、安全运维及相关记录
	安全管理中心	云管理平台、云平台监控系统
	安全区域边界	物理网络边界、虚拟网络边界
	安全通信网络	网络架构、物理链路、通信数据
	安全计算环境	云计算服务软件、虚拟机监视器、云业务管理系统、云产品(服务) 虚拟网络/安全设备、虚拟机镜像 云产品(服务)服务器(虚拟机)、宿主机、终端、云管平台服务器 网络设备、安全设备 云业务管理平台数据(业务数据、配置数据、鉴别信息、审计数据、镜像文件、快照数据、个人信息) SaaS 业务应用软件 虚拟机、数据库服务、中间件、云应用开发平台、云产品(服务)等
SaaS (依托 PaaS 平台构建)	安全管理	安全策略、管理制度、岗位设置、人员配备、人员录用、人员离岗、安全建设、安全运维及相关记录
	安全管理中心	云管理平台、云平台监控系统
	安全计算环境	SaaS 业务应用软件

7.3 云服务客户的业务应用系统

根据云服务客户的业务应用系统所使用的不同服务模式选择测评对象见表 2。

表 2 云服务客户的业务应用系统测评对象

服务模式	安全层面	测评对象
IaaS	安全计算环境	云服务客户的业务应用系统 业务数据 虚拟机、数据库、中间件等 虚拟网络设备、虚拟安全设备 云服务客户的业务应用系统的运维终端
	安全通信网络	虚拟网络架构
	安全区域边界	虚拟网络边界防护服务
	安全管理中心	安全管理平台
	安全管理	安全策略、管理制度、岗位设置、人员配备、人员录用、人员离岗、安全建设、安全运维及相关记录
	平台侧安全	云计算平台网络安全等级保护测评结论/云服务符合性评价
PaaS	安全计算环境	数据库 业务应用系统 业务数据
	安全管理中心	安全管理平台
	安全管理	安全策略、管理制度、岗位设置、人员配备、人员录用、人员离岗、安全建设、安全运维及相关记录
	平台侧安全	云计算平台网络安全等级保护测评结论/云服务符合性评价
SaaS	安全计算环境	业务数据 业务应用系统
	安全管理	安全策略、管理制度、岗位设置、人员配备、人员录用、人员离岗、安全建设、安全运维及相关记录
	平台侧安全	云计算平台网络安全等级保护测评结论/云服务符合性评价

8 确定依据

8.1 概要

8.1.1 对云计算平台和云服务客户的业务应用系统进行测评时,宜合理从 GB/T 22239—2019 中选择符合被测系统场景的要求项作为测评指标,同时使用安全通用要求和云计算安全扩展要求,不宜仅使用云计算安全扩展要求:

- 安全通用要求中安全计算环境的要求项为局部能力要求,作为各测评对象或设备个体能力的测评指标,不宜作为各测评对象或设备整体能力的测评指标;
- 云计算安全扩展要求为全局能力要求,作为各测评对象或设备整体能力的测评指标,不宜作为对某一独立测评对象或设备的测评指标。

8.1.2 测评指标选取时,宜首先确定云计算平台和云服务客户的业务应用系统的保护等级,再在相应级别控制点的基础上考虑以下方面的影响:

- 类别;
- 提供或使用的云计算服务模式;

- 安全主体权限范围；
- 云计算技术实现方式。

8.1.3 表 3 对表 4~表 27 中给出主要场景的云计算平台和云服务客户的业务应用系统测评指标的相关内容进行了约定。

表 3 测评指标约定说明

约定内容	说明
类别	GB/T 22239—2019中的一级条
安全层面	GB/T 22239—2019中的二级条
控制点	GB/T 22239—2019中的三级条
要求	GB/T 22239—2019中的字母列项
场景 1	公有云或云服务商与云服务客户为不同安全主体的私有云
场景 2	云服务商与云服务客户为同一安全主体的私有云
√	“要求”所列内容宜作为本场景测评指标
—	“要求”所列内容不宜作为本场景测评指标

8.2 云计算测评指标

8.2.1 第一级系统测评指标

第一级云计算平台和云服务客户的业务应用系统测评指标见表 4~表 9。

表 4 IaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 6.1			√	√
云计算安全扩展要求	安全物理环境	基础设施位置	6.2.1.1 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	6.2.2.1 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	√	√
			6.2.2.1 b) 应实现不同云服务客户虚拟网络之间的隔离	√	√
	安全区域边界	访问控制	6.2.3.1 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	√	√
	安全计算环境	访问控制	6.2.4.1 a) 应保证当虚拟机迁移时,访问控制策略随其迁移	√	√
			6.2.4.1 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	√	—
		数据完整性和保密性	6.2.4.2 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	√	√
	安全建设管理	供应链管理	6.2.5.2 应确保供应商的选择符合国家有关规定	√	√

表 5 PaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 6.1			√	√
云计算安全扩展要求	安全物理环境	基础设施位置	6.2.1.1 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	6.2.2.1 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	√	√
	安全区域边界	访问控制	6.2.3.1 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	√	√
	安全计算环境	数据完整性和保密性	6.2.4.2 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	√	√
	安全建设管理	供应链管理	6.2.5.2 应确保供应商的选择符合国家有关规定	√	√

表 6 SaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 6.1			√	√
云计算安全扩展要求	安全物理环境	基础设施位置	6.2.1.1 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	6.2.2.1 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	√	√
	安全计算环境	数据完整性和保密性	6.2.4.2 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	√	√
	安全建设管理	供应链管理	6.2.5.2 应确保供应商的选择符合国家有关规定	√	√

表 7 IaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 6.1 除“安全物理环境”以外的全部要求			√	√
云计算安全扩展要求	安全区域边界	访问控制	6.2.3.1 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	√	√
	安全建设管理	云服务商选择	6.2.5.1 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	√	√
			6.2.5.1 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	√	—
			6.2.5.1 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	√	—

表 8 PaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 6.1 除“安全物理环境”以外的全部要求			√	√
云计算安全扩展要求	安全区域边界	访问控制	6.2.3.1 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	√	√
	安全建设管理	云服务商选择	6.2.5.1 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	√	√
			6.2.5.1 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	√	—
			6.2.5.1 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	√	—

表 9 SaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 6.1 除“安全物理环境”以外的全部要求			√	√
云计算安全扩展要求	安全建设管理	云服务商选择	6.2.5.1 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	√	√
			6.2.5.1 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	√	—
			6.2.5.1 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	√	—

8.2.2 第二级系统测评指标

第二级云计算平台和云服务客户的业务应用系统测评指标见表 10~表 15。

表 10 IaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 7.1			√	√
云计算安全扩展要求	安全物理环境	基础设施位置	7.2.1.1 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	7.2.2.1 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	√	√
			7.2.2.1 b) 应实现不同云服务客户虚拟网络之间的隔离	√	√
			7.2.2.1 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	√	—

表 10 IaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全区域 边界	访问控制	7.2.3.1 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	√	√
			7.2.3.1 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	7.2.3.2 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	√	√
			7.2.3.2 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	√	√
			7.2.3.2 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	√	√
		安全审计	7.2.3.3 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	√	√
			7.2.3.3 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	√	—
	安全计算 环境	访问控制	7.2.4.1 a)应保证当虚拟机迁移时,访问控制策略随其迁移	√	√
			7.2.4.1 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	√	—
		镜像和快照保护	7.2.4.2 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	√	√
			7.2.4.2 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	√	√
		数据完整性和保密性	7.2.4.3 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	√	√
			7.2.4.3 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	√	—
			7.2.4.3 c)应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	√	√
		数据备份恢复	7.2.4.4 b)应提供查询云服务客户数据及备份存储位置的能力	√	—
		剩余信息保护	7.2.4.5 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	√	√
			7.2.4.5 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	√	√
	安全建设 管理	供应链 管理	7.2.5.2 a)应确保供应商的选择符合国家有关规定	√	√
			7.2.5.2 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	√	—
	安全运维 管理	云计算环 境管理	7.2.6.1 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	√	√

表 11 PaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 7.1			✓	✓
云计算安全扩展要求	安全物理环境	基础设施位置	7.2.1.1 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	7.2.2.1 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	✓	✓
	安全区域边界	访问控制	7.2.3.1 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	✓	✓
			7.2.3.1 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	7.2.3.2 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	✓	✓
		安全审计	7.2.3.3 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	✓	—
	安全计算环境	数据完整性和保密性	7.2.4.3 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	✓	✓
			7.2.4.3 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	✓	—
		数据备份恢复	7.2.4.4 b) 应提供查询云服务客户数据及备份存储位置的能力	✓	—
		剩余信息保护	7.2.4.5 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	✓	✓
	安全建设管理	供应链管理	7.2.5.2 a) 应确保供应商的选择符合国家有关规定	✓	✓
			7.2.5.2 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	✓	—
	安全运维管理	云计算环境管理	7.2.6.1 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	✓	✓

表 12 SaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 7.1			✓	✓
云计算安全扩展要求	安全物理环境	基础设施位置	7.2.1.1 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	7.2.2.1 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	✓	✓
	安全区域边界	入侵防范	7.2.3.2 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	✓	✓

表 12 SaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全计算 环境	数据 完整性和 保密性	7.2.4.3 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	√	√
			7.2.4.3 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	√	—
		数据备份 恢复	7.2.4.4 b)应提供查询云服务客户数据及备份存储位置的能力	√	—
		剩余信息 保护	7.2.4.5 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	√	√
	安全建设 管理	供应链 管理	7.2.5.2 a)应确保供应商的选择符合国家有关规定	√	√
			7.2.5.2 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	√	—
	安全运维 管理	云计算环 境管理	7.2.6.1 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	√	√

表 13 IaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 7.1 除“安全物理环境”以外的全部要求			√	√
云计算 安全扩展 要求	安全计算 环境	数据备份 恢复	7.2.4.4 a)云服务客户应在本地保存其业务数据的备份	√	√
	安全建设 管理	云服务商 选择	7.2.5.1 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	√	√
			7.2.5.1 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	√	—
			7.2.5.1 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	√	—
			7.2.5.1 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	√	—

表 14 PaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 7.1 除“安全物理环境”以外的全部要求			√	√
云计算 安全扩展 要求	安全计算 环境	数据备份 恢复	7.2.4.4 a)云服务客户应在本地保存其业务数据的备份	√	√
	安全建设 管理	云服务商 选择	7.2.5.1 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	√	√

表 14 PaaS 服务模式云服务客户的业务应用系统测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全建设 管理	云服务商 选择	7.2.5.1 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	√	—
			7.2.5.1 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	√	—
			7.2.5.1 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	√	—

表 15 SaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 7.1 除“安全物理环境”以外的全部要求			√	√
云计算 安全扩展 要求	安全计算 环境	数据备份 恢复	7.2.4.4 a)云服务客户应在本地保存其业务数据的备份	√	√
	安全建设 管理	云服务商 选择	7.2.5.1 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	√	√
			7.2.5.1 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	√	—
			7.2.5.1 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	√	—
			7.2.5.1 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	√	—

8.2.3 第三级系统测评指标

第三级云计算平台和云服务客户的业务应用系统测评指标见表 16～表 21。

表 16 IaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 8.1			√	√
云计算 安全扩展 要求	安全物理 环境	基础设施 位置	8.2.1.1 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	8.2.2.1 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	√	√
			8.2.2.1 b)应实现不同云服务客户虚拟网络之间的隔离	√	√
			8.2.2.1 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	√	—

表 16 IaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全通信 网络	网络架构	8.2.2.1 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	√	—
			8.2.2.1 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	√	—
	安全区域 边界	访问控制	8.2.3.1 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	√	√
			8.2.3.1 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	8.2.3.2 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	√	√
			8.2.3.2 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	√	√
			8.2.3.2 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	√	√
			8.2.3.2 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	8.2.3.3 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	√	√
			8.2.3.3 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	√	—
	安全计算 环境	身份鉴别	8.2.4.1 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	8.2.4.2 a)应保证当虚拟机迁移时,访问控制策略随其迁移	√	√
			8.2.4.2 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	8.2.4.3 a)应能检测虚拟机之间的资源隔离失效,并进行告警	√	√
			8.2.4.3 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	√	√
			8.2.4.3 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	8.2.4.4 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	√	√
			8.2.4.4 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	√	√
			8.2.4.4 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	√	√
		数据完整性和保密性	8.2.4.5 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	√	√
			8.2.4.5 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	√	—

表 16 IaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全计算 环境	数据 完整性和 保密性	8.2.4.5 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	√	√
			8.2.4.5 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	8.2.4.6 b)应提供查询云服务客户数据及备份存储位置的能力	√	—
			8.2.4.6 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	√	√
			8.2.4.6 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	8.2.4.7 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	√	√
			8.2.4.7 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	√	√
	安全管理 中心	集中管控	8.2.5.1 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	√	√
			8.2.5.1 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	√	√
			8.2.5.1 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	√	—
			8.2.5.1 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	供应链 管理	8.2.6.2 a)应确保供应商的选择符合国家有关规定	√	√
			8.2.6.2 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	√	—
			8.2.6.2 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	8.2.7.1 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	√	√

表 17 PaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 8.1			√	√
云计算 安全扩展 要求	安全物理 环境	基础设施 位置	8.2.1.1 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	8.2.2.1 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	√	√

表 17 PaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全通信 网络	网络架构	8.2.2.1 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	√	—
	安全区域 边界	访问控制	8.2.3.1 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	√	√
			8.2.3.1 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	8.2.3.2 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	√	√
			8.2.3.2 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	8.2.3.3 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	√	—
	安全计算 环境	身份鉴别	8.2.4.1 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	√	√
		数据 完整性和 保密性	8.2.4.5 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	√	√
			8.2.4.5 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	√	—
			8.2.4.5 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	8.2.4.6 b) 应提供查询云服务客户数据及备份存储位置的能力	√	—
			8.2.4.6 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	√	√
			8.2.4.6 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	8.2.4.7 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	√	√
	安全管理 中心	集中管控	8.2.5.1 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	√	√
			8.2.5.1 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	√	√
			8.2.5.1 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	√	—
			8.2.5.1 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	供应链 管理	8.2.6.2 a) 应确保供应商的选择符合国家有关规定	√	√
			8.2.6.2 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	√	—

表 17 PaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算安全扩展要求	安全建设管理	供应链管理	8.2.6.2 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	8.2.7.1 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	√	√

表 18 SaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 8.1			√	√
云计算安全扩展要求	安全物理环境	基础设施位置	8.2.1.1 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	8.2.2.1 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	√	√
			8.2.2.1 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	√	—
	安全区域边界	入侵防范	8.2.3.2 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	√	√
			8.2.3.2 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	8.2.3.3 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	√	—
	安全计算环境	身份鉴别	8.2.4.1 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	√	√
		数据完整性和保密性	8.2.4.5 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	√	√
			8.2.4.5 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	√	—
			8.2.4.5 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	8.2.4.6 b) 应提供查询云服务客户数据及备份存储位置的能力	√	—
			8.2.4.6 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	√	√
			8.2.4.6 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	8.2.4.7 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	√	√
	安全管理中心	集中管控	8.2.5.1 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	√	√

表 18 SaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景1	场景2
云计算 安全扩展 要求	安全管理 中心	集中管控	8.2.5.1 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	√	√
			8.2.5.1 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	√	—
			8.2.5.1 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	供应链 管理	8.2.6.2 a)应确保供应商的选择符合国家有关规定	√	√
			8.2.6.2 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	√	—
			8.2.6.2 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	8.2.7.1 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	√	√

表 19 IaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景1	场景2
安全通用 要求	GB/T 22239—2019 中 8.1 除“安全物理环境”以外的全部要求			√	√
云计算 安全扩展 要求	安全区域 边界	访问控制	8.2.3.1 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	√	√
			8.2.3.1 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	√	√
	安全计算 环境	身份鉴别	8.2.4.1 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	√	√
		数据备份 恢复	8.2.4.6 a)云服务客户应在本地保存其业务数据的备份	√	√
	安全管理 中心	集中管控	8.2.5.1 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	√	—
			8.2.5.1 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	8.2.6.1 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	√	√
			8.2.6.1 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	√	—
			8.2.6.1 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	√	—

表 19 IaaS 服务模式云服务客户的业务应用系统测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全建设 管理	云服务商 选择	8.2.6.1 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	√	—
			8.2.6.1 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	√	—

表 20 PaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 8.1 除“安全物理环境”以外的全部要求			√	√
云计算 安全扩展 要求	安全区域 边界	访问控制	8.2.3.1 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	√	√
			8.2.3.1 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	√	√
	安全计算 环境	身份鉴别	8.2.4.1 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	√	√
		数据备份 恢复	8.2.4.6 a)云服务客户应在本地保存其业务数据的备份	√	√
	安全管理 中心	集中管控	8.2.5.1 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	√	—
	安全建设 管理	云服务商 选择	8.2.6.1 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	√	√
			8.2.6.1 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	√	—
			8.2.6.1 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	√	—
			8.2.6.1 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	√	—
			8.2.6.1 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	√	—

表 21 SaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 8.1 除“安全物理环境”以外的全部要求			√	√
云计算 安全扩展 要求	安全计算 环境	数据备份 恢复	8.2.4.6 a)云服务客户应在本地保存其业务数据的备份	√	√
	安全管理 中心	集中管控	8.2.5.1 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	√	—

表 21 SaaS 服务模式云服务客户的业务应用系统测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全建设 管理	云服务商 选择	8.2.6.1 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	√	√
			8.2.6.1 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	√	—
			8.2.6.1 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	√	—
			8.2.6.1 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	√	—
			8.2.6.1 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	√	—

8.2.4 第四级系统测评指标

第四级云计算平台和云服务客户的业务应用系统测评指标见表 22~表 27。

表 22 IaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 9.1			√	√
云计算 安全扩展 要求	安全物理 环境	基础设施 位置	9.2.1.1 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	9.2.2.1 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	√	√
			9.2.2.1 b) 应实现不同云服务客户虚拟网络之间的隔离	√	√
			9.2.2.1 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	√	—
			9.2.2.1 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	√	—
			9.2.2.1 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	√	—
			9.2.2.1 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	√	—
			9.2.2.1 g) 应提供通信协议转换或通信协议隔离等的的数据交换方式,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	√	—
			9.2.2.1 h) 应为第四级业务应用系统划分独立的资源池	√	√
	安全区域 边界	访问控制	9.2.3.1 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	√	√

表 22 IaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全区域 边界	访问控制	9.2.3.1 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	9.2.3.2 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	√	√
			9.2.3.2 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	√	√
			9.2.3.2 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	√	√
			9.2.3.2 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	9.2.3.3 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	√	√
			9.2.3.3 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	√	—
	安全计算 环境	身份鉴别	9.2.4.1 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	9.2.4.2 a)应保证当虚拟机迁移时,访问控制策略随其迁移	√	√
			9.2.4.2 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	9.2.4.3 a)应能检测虚拟机之间的资源隔离失效,并进行告警	√	√
			9.2.4.3 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	√	√
			9.2.4.3 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	9.2.4.4 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	√	√
			9.2.4.4 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	√	√
			9.2.4.4 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	√	√
		数据完整性和保密性	9.2.4.5 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	√	√
			9.2.4.5 b)应保证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	√	—
			9.2.4.5 c)应使用校验技术或密码技术保证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	√	√
			9.2.4.5 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	√	—

表 22 IaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全计算 环境	数据备份 恢复	9.2.4.6 b) 应提供查询云服务客户数据及备份存储位置的能力	√	—
			9.2.4.6 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	√	√
			9.2.4.6 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	9.2.4.7 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	√	√
			9.2.4.7 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	√	√
	安全管理 中心	集中管控	9.2.5.1 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	√	√
			9.2.5.1 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	√	√
			9.2.5.1 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	√	—
			9.2.5.1 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	供应链 管理	9.2.6.2 a) 应确保供应商的选择符合国家有关规定	√	√
			9.2.6.2 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	√	—
			9.2.6.2 c) 应保证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	9.2.7.1 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	√	√

表 23 PaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 9.1			√	√
云计算 安全扩展 要求	安全物理 环境	基础设施 位置	9.2.1.1 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	9.2.2.1 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	√	√
			9.2.2.1 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	√	—
			9.2.2.1 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	√	—

表 23 PaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全通信 网络	网络架构	9.2.2.1 g) 应提供通信协议转换或通信协议隔离等的交换方式, 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	√	—
			9.2.2.1 h) 应为第四级业务应用系统划分独立的资源池	√	√
	安全区域 边界	访问控制	9.2.3.1 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	√	√
			9.2.3.1 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	9.2.3.2 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	√	√
			9.2.3.2 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	9.2.3.3 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	√	—
	安全计算 环境	身份鉴别	9.2.4.1 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	√	√
		数据 完整性和 保密性	9.2.4.5 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	√	√
			9.2.4.5 b) 应保证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	√	—
			9.2.4.5 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	9.2.4.6 b) 应提供查询云服务客户数据及备份存储位置的能力	√	—
			9.2.4.6 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	√	√
			9.2.4.6 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	9.2.4.7 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	√	√
	安全管理 中心	集中管控	9.2.5.1 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	√	√
			9.2.5.1 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	√	√
			9.2.5.1 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	√	—
			9.2.5.1 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	供应链 管理	9.2.6.2 a) 应确保供应商的选择符合国家有关规定	√	√
			9.2.6.2 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	√	—

表 23 PaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算安全扩展要求	安全建设管理	供应链管理	9.2.6.2 c) 应保证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	9.2.7.1 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	√	√

表 24 SaaS 服务模式云计算平台测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用要求	GB/T 22239—2019 中 9.1			√	√
云计算安全扩展要求	安全物理环境	基础设施位置	9.2.1.1 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	9.2.2.1 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	√	√
			9.2.2.1 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	√	—
			9.2.2.1 h) 应为第四级业务应用系统划分独立的资源池	√	√
	安全区域边界	入侵防范	9.2.3.2 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	√	√
			9.2.3.2 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	9.2.3.3 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	√	—
	安全计算环境	身份鉴别	9.2.4.1 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	√	√
		数据完整性和保密性	9.2.4.5 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	√	√
			9.2.4.5 b) 应保证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	√	—
			9.2.4.5 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	9.2.4.6 b) 应提供查询云服务客户数据及备份存储位置的能力	√	—
			9.2.4.6 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	√	√
			9.2.4.6 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	9.2.4.7 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	√	√

表 24 SaaS 服务模式云计算平台测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全管理 中心	集中管控	9.2.5.1 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	✓	✓
			9.2.5.1 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	✓	✓
			9.2.5.1 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	✓	—
			9.2.5.1 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	供应链 管理	9.2.6.2 a) 应确保供应商的选择符合国家有关规定	✓	✓
			9.2.6.2 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	✓	—
			9.2.6.2 c) 应保证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	9.2.7.1 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	✓	✓

表 25 IaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 9.1 除“安全物理环境”以外的全部要求			✓	✓
云计算 安全扩展 要求	安全通信 网络	网络架构	9.2.2.1 h) 应为第四级业务应用系统划分独立的资源池	✓	✓
	安全区域 边界	访问控制	9.2.3.1 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	✓	✓
			9.2.3.1 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	✓	✓
	安全计算 环境	身份鉴别	9.2.4.1 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	✓	✓
		数据备份 恢复	9.2.4.6 a) 云服务客户应在本地保存其业务数据的备份	✓	✓
	安全管理 中心	集中管控	9.2.5.1 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	✓	—
			9.2.5.1 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	9.2.6.1 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	✓	✓

表 25 IaaS 服务模式云服务客户的业务应用系统测评指标（续）

类别	安全层面	控制点	要求	场景 1	场景 2
云计算 安全扩展 要求	安全建设 管理	云服务商 选择	9.2.6.1 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	√	—
			9.2.6.1 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	√	—
			9.2.6.1 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	√	—
			9.2.6.1 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	√	—

表 26 PaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景 1	场景 2
安全通用 要求	GB/T 22239—2019 中 9.1 除“安全物理环境”以外的全部要求			√	√
云计算 安全扩展 要求	安全通信 网络	网络架构	9.2.2.1 h)应为第四级业务应用系统划分独立的资源池	√	√
	安全区域 边界	访问控制	9.2.3.1 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	√	√
			9.2.3.1 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	√	√
	安全计算 环境	身份鉴别	9.2.4.1 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	√	√
		数据备份 恢复	9.2.4.6 a)云服务客户应在本地保存其业务数据的备份	√	√
	安全管理 中心	集中管控	9.2.5.1 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	√	—
	安全建设 管理	云服务商 选择	9.2.6.1 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	√	√
			9.2.6.1 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	√	—
			9.2.6.1 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	√	—
			9.2.6.1 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	√	—
			9.2.6.1 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	√	—

表 27 SaaS 服务模式云服务客户的业务应用系统测评指标

类别	安全层面	控制点	要求	场景1	场景2
安全通用要求	GB/T 22239—2019 中 9.1 除“安全物理环境”以外的全部要求			√	√
云计算安全扩展要求	安全通信网络	网络架构	9.2.2.1 h)应为第四级业务应用系统划分独立的资源池	√	√
	安全计算环境	数据备份恢复	9.2.4.6 a)云服务客户应在本地保存其业务数据的备份	√	√
	安全管理中心	集中管控	9.2.5.1 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	√	—
	安全建设管理	云服务商选择	9.2.6.1 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	√	√
			9.2.6.1 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	√	—
			9.2.6.1 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	√	—
			9.2.6.1 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	√	—
			9.2.6.1 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	√	—

8.2.5 第五级系统测评指标

略。

参 考 文 献

- [1] GB/T 25069—2022 信息安全技术 术语
 - [2] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
 - [3] GB/T 31168—2023 信息安全技术 云计算服务安全能力要求
 - [4] 张振峰,张志文,王睿超.网络安全等级保护 2.0 云计算安全合规能力模型.信息网络安全[J]. 2019,11,1-7.
-

中华人民共和国公共安全
行 业 标 准
信息安全技术 网络安全等级保护
云计算测评指引
GA/T 2347—2025

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)

网址 www.spc.net.cn

总编室:(010)68533533 发行中心:(010)51780238

读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

*

开本 880×1230 1/16 印张 2.25 字数 52 千字

2025年12月第1版 2025年12月第1次印刷

*

书号: 155066 • 2-39574 定价 59.00 元

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话:(010)68510107



GA/T 2347-2025