



中华人民共和国国家标准

GB/T 34942—2025

代替 GB/T 34942—2017

网络安全技术 云计算服务安全能力评估方法

Cybersecurity technology—

The assessment method for security capability of cloud computing service

2025-08-01 发布

2026-02-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	VII
引言	VIII
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
5.1 评估原则	2
5.2 评估内容	3
5.3 评估证据	3
5.4 评估实施过程	3
5.5 综合评估	5
6 系统开发与供应链安全评估方法	6
6.1 资源分配	6
6.2 系统生命周期	6
6.3 采购过程	7
6.4 系统文档	9
6.5 关键性分析	10
6.6 外部服务	10
6.7 开发商安全体系架构	12
6.8 开发过程、标准和工具	13
6.9 开发过程配置管理	15
6.10 开发商安全测试和评估	16
6.11 开发商提供的培训	20
6.12 组件真实性	20
6.13 不被支持的系统组件	21
6.14 供应链保护	22
7 系统与通信保护评估方法	25
7.1 边界保护	25
7.2 传输保密性和完整性保护	28
7.3 网络中断	29
7.4 可信路径	30
7.5 密码使用和管理	31

7.6	设备接入保护	31
7.7	移动代码	33
7.8	会话认证	34
7.9	恶意代码防护	35
7.10	内存防护	37
7.11	系统虚拟化安全性	37
7.12	网络虚拟化安全性	40
7.13	存储虚拟化安全性	41
7.14	安全管理功能的通信保护	43
8	访问控制评估方法	45
8.1	用户标识与鉴别	45
8.2	标识符管理	46
8.3	鉴别凭证管理	47
8.4	鉴别凭证反馈	49
8.5	密码模块鉴别	49
8.6	账号管理	50
8.7	访问控制的实施	51
8.8	信息流控制	52
8.9	最小特权	54
8.10	未成功的登录尝试	55
8.11	系统使用通知	56
8.12	前次访问通知	56
8.13	并发会话控制	57
8.14	会话锁定	57
8.15	未进行标识和鉴别情况下可采取的行动	58
8.16	安全属性	58
8.17	远程访问	59
8.18	无线访问	60
8.19	外部信息系统的使用	61
8.20	可供公众访问的内容	63
8.21	全球广域网(Web)访问安全	63
8.22	API 访问安全	64
9	数据保护评估方法	65
9.1	通用数据安全	65
9.2	媒体访问和使用	66
9.3	剩余信息保护	69
9.4	数据使用保护	70

9.5 数据共享保护	70
9.6 数据迁移保护	71
10 配置管理评估方法	72
10.1 配置管理计划	72
10.2 基线配置	73
10.3 变更控制	75
10.4 配置参数的设置	78
10.5 最小功能原则	79
10.6 信息系统组件清单	80
11 维护管理评估方法	82
11.1 受控维护	82
11.2 维护工具	84
11.3 远程维护	85
11.4 维护人员	86
11.5 及时维护	88
11.6 缺陷修复	88
11.7 安全功能验证	89
11.8 软件和固件完整性	90
12 应急响应评估方法	91
12.1 事件处理计划	91
12.2 事件处理	93
12.3 事件报告	94
12.4 事件处理支持	95
12.5 安全警报	96
12.6 错误处理	97
12.7 应急响应计划	98
12.8 应急响应培训	100
12.9 应急演练	101
12.10 信息系统备份	102
12.11 支撑客户的业务连续性计划	104
12.12 电信服务	105
13 审计评估方法	106
13.1 可审计事件	106
13.2 审计记录内容	107
13.3 审计记录存储容量	107
13.4 审计过程失败时的响应	108
13.5 审计的审查、分析和报告	109

13.6 审计处理和报告生成	111
13.7 时间戳	112
13.8 审计信息保护	113
13.9 抗抵赖性	114
13.10 审计记录留存	115
14 风险评估与持续监控评估方法	116
14.1 风险评估	116
14.2 脆弱性扫描	117
14.3 持续监控	118
14.4 信息系统监测	120
14.5 垃圾信息监测	122
15 安全组织与人员	123
15.1 安全策略与规程	123
15.2 安全组织	124
15.3 岗位风险与职责	125
15.4 人员筛选	126
15.5 人员离职	126
15.6 人员调动	128
15.7 第三方人员安全	128
15.8 人员处罚	129
15.9 安全培训	130
16 物理与环境安全评估方法	131
16.1 物理设施与设备选址	131
16.2 物理和环境规划	132
16.3 物理环境访问授权	134
16.4 物理环境访问控制	135
16.5 输出设备访问控制	137
16.6 物理访问监控	137
16.7 访客访问记录	138
16.8 设备运送和移除	139
附录 A (资料性) 常见云计算服务脆弱性问题	141
A.1 概述	141
A.2 系统开发与供应链安全	141
A.3 系统与通信保护	142
A.4 访问控制	143
A.5 数据保护	145
A.6 配置管理	147

A.7 维护管理	149
A.8 应急响应	150
A.9 审计	151
A.10 风险评估与持续监控评估方法	152
A.11 安全组织与人员	154
A.12 物理与环境安全	155
附录 B (资料性) 单项安全要求评估描述	156
参考文献	157

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。

本文件代替 GB/T 34942—2017《信息安全技术 云计算服务能力评估方法》,与 GB/T 34942—2017 相比,除结构调整和编辑性改动外,主要技术变化如下:

- a) 更改了范围的适用界限(见第 1 章,2017 年版的第 1 章);
- b) 增加了不同能力级别评估要求和综合评估要求(见 5.2、5.5);
- c) 更改了具体评估方法(见第 6 章~第 8 章、第 10 章~第 14 章,2017 年版的第 5 章~第 14 章);
- d) 增加了数据保护评估方法(见第 9 章)。

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中国电子技术标准化研究院、中国网络安全审查认证和市场监管大数据中心、国家信息技术安全研究中心、中国信息安全测评中心、中国信息通信研究院、中国科学技术大学、四川大学、神州网信技术有限公司、中电长城网际系统应用有限公司、国家信息中心、国家工业信息发展研究中心、国家计算机网络应急技术处理协调中心、中国电子科技集团公司第十五研究所、中国科学院软件研究所、中国科学院信息工程研究所、杭州安恒信息技术股份有限公司、北京航空航天大学、北京工业大学、重庆邮电大学、西安电子科技大学、北京化工大学、中国人民大学、中国传媒大学、清华大学、上海市信息安全测评认证中心、中国电子科技集团第三十研究所、重庆市市场监督管理局档案信息中心、内蒙古数字经济安全科技有限公司、中国移动通信有限公司研究院、华为云计算技术有限公司、阿里云计算有限公司、天翼云科技有限公司、亚信科技(成都)有限公司。

本文件主要起草人:杨建军、王惠莅、贾大文、何延哲、伍扬、胡华明、卢夏、张丽娜、刘佳良、张建军、李京春、左晓栋、陈兴蜀、闵京华、周亚超、史大为、陈永刚、张立武、杨晨、方勇、曹玲、张明天、吴槟、马庆栋、曲平、张东举、吉磊、李燕伟、霍珊珊、伍前红、杨震、黄永洪、马文平、习宁、杨力、裴庆祺、王明彦、秦波、杨洋、葛晓园、晏敏、姜正涛、李娜、蔡宇渊、刘彦、葛振鹏、范晓晖、肖敏、韩雪峰、李连磊、高强、徐御、靳嵩、张玲、李峰风、方强、司渤洋、廖双晓。

本文件及其所代替文件的历次版本发布情况为:

——2017 年首次发布为 GB/T 34942—2017 ;

——本次为第一次修订。

引　　言

GB/T 31168—2023《信息安全技术　云计算服务安全能力要求》提出了云服务商在保障云计算环境中客户信息和业务的安全时应具备的安全能力,该标准将云计算服务安全能力要求分为一般要求、增强要求和高级要求,增强要求和高级要求是对其低一级要求的补充和强化。根据云计算平台上的信息敏感度和业务重要性的不同,云服务商应具备相适应的安全能力。

本文件是 GB/T 31168—2023 的配套评估标准,对应 GB/T 31168—2023 中第 6 章～第 16 章规定的要求,本文件也从第 6 章～第 16 章给出了相应的评估方法。本文件主要为第三方评估机构开展云计算服务安全能力评估提供指导。第三方评估机构可制定相应安全评估方案,采用访谈、检查、测试等多种方式实施安全评估。本文件也可为云服务商开展自评估提供参考。

网络安全技术 云计算服务安全能力评估方法

1 范围

本文件确立了依据 GB/T 31168—2023 开展评估的原则、实施过程,描述了针对各项具体安全要求进行评估的方法。

本文件适用于第三方评估机构对云服务商提供云计算服务时具备的安全能力进行评估,也为云服务商在进行自评估时提供参考。

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 20984—2022 信息安全技术 信息安全风险评估方法
- GB/T 25069—2022 信息安全技术 术语
- GB/T 31167—2023 信息安全技术 云计算服务安全指南
- GB/T 31168—2023 信息安全技术 云计算服务安全能力要求
- GB/T 35273 信息安全技术 个人信息安全规范
- GB/T 37972 信息安全技术 云计算服务运行监管框架
- GB 50174 数据中心设计规范

3 术语和定义

GB/T 25069—2022、GB/T 31167—2023 和 GB/T 31168—2023 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**

通过网络访问可扩展的、灵活的物理或虚拟资源池,并按需自助获取和管理的模式。

注: 资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[来源:GB/T 31168—2023,3.1]

3.2

云计算服务 **cloud computing service**

使用定义的接口,借助云计算(3.1)提供一种或多种资源的能力。

[来源:GB/T 31168—2023,3.2]

3.3

云服务商 **cloud service provider**

提供云计算服务(3.2)的参与方。