陕西省地方标准

《云计算平台渗透测试技术规范》

（征求意见稿）

编制说明

陕西省网络与信息安全测评中心

2024年2月23日

陕西省地方标准

《云计算平台渗透测试技术规范》

编 制 说 明

一、工作概况

1. 目的意义

党的二十大报告提出，要构建新一代信息技术等一批新的增长引擎，打造具有国际竞争力的数字产业集群。云计算是信息技术发展和服务模式创新的集中体现，是信息化发展的重大变革和必然趋势，是信息时代国际竞争的制高点和经济发展新动能的助燃剂。云计算引发了软件开发部署模式的创新，成为承载各类应用的关键基础设施，并为大数据、物联网、人工智能等新兴领域的发展提供基础支撑。加快推动云计算创新发展，顺应新一轮科技革命和产业变革趋势，是推进中国式现代化进程的关键。

云计算平台是实现云计算主要方式之一。它通过虚拟机化技术，实现硬件资源的共享。同时，根据用户的需求提供弹性的服务，不仅节约了用户成本，也提高了资源的利用率。然而，云计算平台在快速发展的同时，也面临着越来越多安全性的问题。通过对云计算平台进行渗透测试，模拟真实世界中的攻击，发现并利用安全漏洞，进而检验、评估云计算平台实际安全水平，是主动提升云计算平台安全的有力手段，也是保障云计算平台安全的现实需求。

渗透测试虽然是一项基础的安全技术，但在不同的应用场景下又有各自的特殊性。云计算平台具有虚拟化、动态可扩展、灵活性高等特点，且需要非常高的稳定性，不规范的渗透测试不仅无法全面覆盖与云计算平台安全密切相关的核心安全风险，还可能给云计算平台的安全稳定带来负面影响。

因此，在国家层面尚未建立成熟的渗透测试相关标准的情况下，需要结合云计算平台的特点，针对性地制定《云计算平台渗透测试技术规范》，填补云计算平台渗透测试标准化领域的空白，以保障测试质量、控制测试风险，确保测试机构能更加规范地开展云计算平台渗透测试工作，增强用户对云计算平台的信心，营造良好的云计算技术和应用市场环境，推动云计算产业持续健康发展。

1. 任务来源

目前，云计算相关技术类标准主要为国家标准，研究方向主要集中在云计算服务参考架构、级别协议、能力类型、服务模式、部署模式、安全运行能力、供应商安全、业务和数据迁移上云等要求方面，以支撑云服务监管部门、规范云防护服务市场。渗透测试相关标准主要为地方标准和行业标准，研究方向主要侧重于信息系统、金融行业安全等方面，国家层面亦尚未建立成熟的渗透测试相关标准。

因此，按照陕西省市场监督管理局《关于下达2023年度陕西省地方标准制修订项目计划的通知》（陕市监函〔2023〕410号）要求，成立编制组开展陕西省地方标准《云计算平台渗透测试技术规范》编制工作（项目编号：SDBXM010-2023），为云计算平台监管部门、运营机构和第三方服务机构提供渗透测试指导及参考。

1. 承担单位

陕西省网络与信息安全测评中心

陕西正观政务信息技术研究院有限公司

陕西省信息化工程研究院

1. 主要工作过程

自本标准编制任务下达后，陕西省网络与信息安全测评中心、陕西正观政务信息技术研究院有限公司、陕西省信息化工程研究院联合成立标准起草组，明确了工作指导思想，制定了工作原则，确定了起草组成员和任务分工。起草组先后组织成员对国家标准化管理委员会发布的GB/T 31168-2023 《信息安全技术 云计算服务安全能力要求》、GB/T 25069-2022《信息安全技术 术语》、GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》等相关标准进行了研究学习，并对收集的相关资料进行分析整理。同时，采取专家咨询，召开座谈会等形式，对拟制定标准的内容、范围、适用性等进行了充分研讨，明确了《云计算平台渗透测试技术规范》的具体内容。

1. 起草组成员及任务分工

|  |  |  |  |
| --- | --- | --- | --- |
| 姓 名 | 性别 | 工作单位 | 任务分工 |
| 马卓元 | 女 | 陕西省网络与信息安全测评中心 | 负责人、组织协调、  标准文稿初稿撰写 |
| 杨 帆 | 男 | 陕西省网络与信息安全测评中心 | 标准文稿初稿撰写 |
| 赵首花 | 女 | 陕西正观政务信息技术研究院有限公司 | 标准文稿初稿撰写 |
| 杨向东 | 男 | 陕西省网络与信息安全测评中心 | 标准文稿初稿撰写 |
| 靳 倩 | 女 | 陕西省网络与信息安全测评中心 | 标准文稿初稿撰写 |
| 李 严 | 男 | 陕西省网络与信息安全测评中心 | 标准文稿初稿撰写 |
| 张 勇 | 男 | 陕西省信息化工程研究院 | 标准文稿初稿撰写 |

二、标准编制原则和标准主要内容

1. 标准编制所遵循的原则

本标准编制依据《中华人民共和国标准化法》和《地方标准制定规范》的相关规定。

本标准编制遵循适用性、合理性、统一性的原则，系统、全面、科学地提出了云计算平台渗透测试技术规范。

本标准编制遵循面向市场、服务社会，保护环境，自主制定、及时修订、不断完善的原则，可为云计算平台监管部门、运营机构和第三方服务机构等提供渗透测试指导及参考。

本标准编制遵循公正、公开、透明的原则，广泛征求意见，并不断修正、完善标准内容。

2. 标准的结构、要素、技术要求、关键指标的确定依据和主要内容

为保证标准的科学性、公正性、实用性，除了广泛征集省内外企业、高校、研究机构的技术专家和学者的意见外，起草组成员连同合作单位形成了产、学、研的权威阵容，在标准制订过程中做了非常充分的调查、研究、讨论，最终形成了范围、规范性引用文件、术语和定义、云计算平台特性、总则、测试对象、测试方法及工具、测试分类、测试流程、测试内容等主要内容。

三、实证研究

标准内容是基于起草组成员的学术理论知识和产业界遇到的实际情况而编制，且有来自省内外高校、企业、研究机构专家的意见和指导，不断进行修正和完善，并计划组织开展标准相关应用及效果实施评价，以确保达到预期目标。

四、知识产权说明

本标准知识产权归编制单位所有，没有知识产权争议。

五、采标情况

目前，云计算相关技术类标准主要为国家标准，研究方向主要集中在云计算服务参考架构、级别协议、能力类型、服务模式、部署模式、安全运行能力、供应商安全、业务和数据迁移上云等要求方面，以支撑云服务监管部门、规范云防护服务市场。渗透测试相关标准主要为地方标准和行业标准，研究方向主要侧重于信息系统、金融行业安全等方面，国家层面亦尚未建立成熟的渗透测试相关标准。因此，本标准的内容具有一定前瞻性。通过制定《云计算平台渗透测试技术规范》，可规范云计算平台渗透测试工作，有效保障云计算平台安全。

六、重大意见分歧的处理

无重大分歧意见。

七、其他应说明的事项

无。