陕西省地方标准

《云计算平台渗透测试实施指南》

（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03月05日

陕西省地方标准

《云计算平台渗透测试实施指南》

编 制 说 明

一、工作概况

1. 目的意义

自《中华人民共和国网络安全法》出台以来，国家陆续出台了一法律法规来强调网络安全的重要性，包括《关键信息基础设施安全保护条例》、《[中华人民共和国数据安全法](https://www.baidu.com/s?wd=%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E6%95%B0%E6%8D%AE%E5%AE%89%E5%85%A8%E6%B3%95&rsv_idx=2&tn=baiduhome_pg&usm=3&ie=utf-8&rsv_pq=dd17f949002d6678&oq=%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E7%9A%84%E6%B3%95%E5%BE%8B%E6%B3%95%E8%A7%84&rsv_t=4ad8zCLoo7KRD3E5ti1BhryjPBN1oVPNCrbYX1n17+mj2H2NANoeils2vdaIc7O/arJP&sa=re_dqa_zy&icon=1" \t "https://www.baidu.com/_self)》、《中华人民共和国个人信息保护法》等，尤其是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。随着数字化转型的加速，云计算平台已成为国家关键信息基础设施的重要组成部分，确保云计算平台的安全性对于维护国家网络安全至关重要。

随着云计算技术的广泛应用，云计算平台的安全问题日益突出。渗透测试是评估和提升云计算平台安全性的重要手段。通过对云计算平台进行渗透测试，以模拟黑客的攻击方法，主动分析云计算平台的任何弱点、技术缺陷或漏洞。这有助于发现系统中存在的安全隐患和问题，从而及时进行修复，提高系统的安全性。

渗透测试其主要目的在于验证整个云计算平台的技术安全性。通过渗透测试，可以在技术层面定性地分析系统的安全性，从而确保平台在复杂的应用环境中能正常运行而不至于导致安全问题。同时可以及时发现并解决安全问题，确保平台在遭受攻击时能够保持业务连续性，避免因安全问题导致的业务中断和数据泄露。

目前，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实施指南》，对云计算平台渗透测试的具体实施提出指导性建议，填补云计算平台渗透测试标准化领域的空白，明确云计算平台渗透测试实施的过程和方法，提高各类渗透测试机构或被测单位对云计算平台渗透测试项目的监控与管理水平，推动云计算平台渗透测试项目组织、实施、验收等工作的顺利开展，使云计算平台渗透测试工作系统化、规范化、标准化，最终有效提升云计算平台的安全水平，促进云计算产业持续健康发展。

1. 任务来源

目前，云计算相关指南类标准主要为国家标准，研究方向主要集中在云计算服务安全、云服务采购、云平台间应用和数据迁移、服务测试、性能测试、能力评估、质量评价等方面，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一般信息系统和银行信息系统等方面，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实施指南》编制工作（项目编号：SDBXM011-2023），为云计算平台运营机构或第三方服务机构提供提供操作指导，保障云计算平台渗透测试实施质量，规范渗透测试项目的组织、实施和验收等。

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

陕西中认信安技术服务有限公司

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、陕西中认信安技术服务有限公司、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实施指南》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 |
| 赵少飞 | 男 | 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 |
| 马卓元 | 女 | 陕西省网络与信息安全测评中心 | 标准文稿初稿撰写 |
| 胡吉祥 | 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实施指南。

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，可为云计算平台运营机构或第三方服务机构提供操作指导，规范渗透测试项目的组织、实施和验收等。

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、渗透测试实施概述、准备阶段、方案编制阶段、现场实施阶段、报告编制阶段等主要内容。

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，云计算相关指南类标准主要为国家标准，研究方向主要集中在云计算服务安全、云服务采购、云平台间应用和数据迁移、服务测试、性能测试、能力评估、质量评价等方面，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一般信息系统和银行信息系统等方面，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实施指南》，以保障云计算平台渗透测试实施质量，控制云计算平台渗透测试实施风险。

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。