国家标准《信息安全技术 云计算服务安全能力评估方法》（征求意见稿）编制说明

一、工作简况

1.1 任务来源

根据全国信息安全标准化技术委员会2023年下达的国家标准制修订计划建议，《信息安全技术 云计算服务安全能力评估方法》由中国电子技术标准化研究院负责承办，国标计划号：20231926-T-469。本标准由全国信息安全标准化技术委员会归口管理。

1.2 制定背景

云计算是信息技术产业发展的战略重点，国外政府重视云计算在政府部门的应用以及云计算节约资源服务便捷的优势，通过制定云计算发展战略和相关政策法规，为云计算的良性发展提供保障。2010年12月，美国联邦CIO发布《联邦信息技术管理改革25点实施计划》，明确提出联邦政府“云技术”三步走的战略。2011年2月，美国总统奥巴马发布《联邦云计算战略》，同年12月，联邦预算管理局发布《云计算环境信息系统安全授权》，正式启动《联邦风险及授权管理计划（FedRAMP）项目，要求进入政府采购清单目录的云服务商，必须经过FedRAMP的认证。欧盟也在云计算方面提出了云战略等，时至今日，云计算已经在美国、欧盟、日本等国家大量普及。美国也出台了虚拟化安全、云计算访问控制、云计算安全与隐私等10余份文件，欧盟也发布了云计算风险评估、云计算安全框架等多份文档。国际标准化组织ISO/IEC JTC1 SC27也先后发布了ISO 27017和ISO 27018等国际标准，规范云计算安全使用。

目前，云计算技术已经普遍应用于现今的互联网服务中， 金融云、教育云、医疗云等应用形式多种多样，为规范国内云计算服务的安全使用，2019年7月，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部等四部门联合发布了《云计算服务安全评估办法》（2019年 第2号），要求参照国家有关网络安全标准，对为党政机关、关键信息基础设施运营者提供云计算服务的云平台开展安全评估工作，以提高云计算服务平台的安全性、可控性，保障国家安全和社会稳定。2020年4月13日，国家互联网信息办公室等12部委联合

发布了《网络安全审查办法》中也提出对关键信息基础设施运营者采购云计算服务是否可能带来国家安全风险进行分析，影响或可能影响国家安全的应进行网络安全审查，本标准是落实上述规定的主要支撑标准，目前已经在云计算服务安全评估中广泛使用。

2023 年，GB/T 31168-2023《信息安全技术 云计算服务安全能力要求》标准发布，该标准修订了 2014 版。本标准原来版本即 GB/T 34942-2017 版为依据 GB/T 31168-2014 版进行的评估，现根据 GB/T 31168-2023 对 GB/T 34942-2017 进行修订。

1.3 起草过程

标准制定的主要工作过程如下：

1）立项申请

2022 年 11 月至 2023 年 3 月，标准编制团队启动标准修订工作。编制组对国内外云计算服务安全评估的相关政策、标准及目前存在的问题进行了研究。按照信安标委2023年国家标准项目申报要求提交了2023年立项国家标准制定项目立项申请。

2023 年 5 月，标准编制组在信安标委会议周上进行立项汇报并通过。会后，根据工作组成员单位专家意见组织编制组讨论并继续完善草案内容。

2）草案完善

2023 年 8 月，根据《全国信息安全标准化技术委员会 2023 年第一批网络安全国家标准立项的通知》（信安字[2023] 17 号）发布的通知，本标准正式获批为 2023 年网络安全标准修订项目。

2023 年 9 月至 10 月，征集标准编制单位，共收集 23 家单位提交的申请材料并对申请的参编单位进行了遴选。同期征求相关专家意见，召开编制组工作会，对标准草案进行进一步修改完善。

2023 年 11 月，在全国信息安全标准化技术委员会举办的武汉标准周上，标准编制组在大数据安全特别工作组进行了汇报，与会专家讨论投票后，工作组形成转征求意见稿的会议纪要。

3）征求意见稿

2023 年 11 月，标准编制组根据标准周上与会专家意见修改完善，形成征求

意见稿第一版。2023 年 12 月，根据责任专家和责任编辑意见修改完善。

2024 年 1 月 25 日，标准编制组参加了信安标委秘书处组织的征求意见稿专家审查会，并通过专家审查。会后，编制组根据与会专家意见对标准进行了修改完善。

二、标准编制原则和确定主要内容的论据及解决的主要问题

2.1 编制原则

一是充分吸收已有云安全相关标准。《评估方法》充分参考了国际、国内有关云计算安全以及安全评估的先进标准和技术规范。目前，《评估方法》已将美国 FedRAMP 云安全测试用例、NIST 800-53A、ISO/IEC 27017、等级保护测评等相关标准的长处进行了吸收，充分考虑了相关的测试评估方法。

二是重点关注安全评估方法，不涉及安全评价。《评估方法》是在已发布国标《信息安全技术 云计算服务安全能力要求》基础上制定的，而《能力要求》标准是我国云计算服务安全评估的重要依据，在实施过程中需要《评估方法》进行配合。对云计算服务安全能力的评价涉及到多种因素，情况比较复杂，本标准只关注安全评估方法，对于云计算服务安全能力的水平如何不做量化评价。

2.2 主要内容及其确定依据

本文件给出了依据 GB/T 31168－2023《信息安全技术 云计算服务安全能力要求》，开展评估的原则、实施过程以及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，云服务商在对自身云计算服务安全能力进行自评估时也可参考。

标准主要内容的确定既参考了国外相关标准和实践，同时也主要由我国云计算服务安全评估工作的经验凝聚而来。

2.3 修订前后技术内容的对比

本文件代替 GB/T 34942—2017《信息安全技术 云计算服务安全能力评估方法》，与 GB/T 34942—2017 相比，主要变化如下：

——修改标准适用范围，改为“适用于对党政机关和关键信息基础设施运营者使用的云计算服务进行安全管理，还适用于指导云服务商建设安全的云计算平台和提供安全的云计算服务”。

——增加第 5 章，整体评估方法。

——修改第 6 章到第 16 章，按照修订的 GB/T 31168—2023 要求给出具体评估方法。

——增加附录 A，给出常见的云计算服务脆弱性问题。

三、 试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益

3.1 试验验证的分析、综述报告

本标准目前为征求意见稿阶段，拟后续开展标准试点工作。

3.2 技术经济论证

标准用于加强云计算服务的安全管理，以预防由于发生信息安全问题导致的各种损失。

3.3 预期的经济效益、社会效益和生态效益

标准可有利于云计算服务安全评估制度在我国国内的进一步落地推广，有利于提高各种类型组织的云计算服务安全能力。

四、 与国际、国外同类标准技术内容的对比情况，或者与测试的国外样品、样机的有关数据对比情况

国外无相关标准。

五、 以国际标准为基础的起草情况，以及是否合规引用或者采用国际国外标准，并说明未采用国际标准的原因

无。

六、 与有关法律、行政法规及相关标准的关系

本标准符合现有法律法规的要求，并与现有相关标准协调一致。本标准主要为 GB/T 31168-2023《信息安全技术 云计算服务安全能力要求》的配套标准。

七、重大分歧意见的处理经过和依据

无。

八、涉及专利的有关说明

本标准不涉及专利。

九、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议

建议本标准作为推荐性国家标准发布实施。在正式执行本标准前，需要对标准中的条款进行宣贯，以在利益相关方之间达成对标准条款理解上的一致性。

十、其他应当说明的事项

无。

《信息安全技术 云计算服务安全能力评估方法》标准编制组

2024 年 1 月 30 日