团体标准《智能合约安全测评过程指南》编制说明

一、 工作简况

1.1 任务来源

《智能合约安全测评过程指南》由广东省网络空间安全协会归口。

1.2 主要起草单位和工作组成员

本标准由北京神州绿盟科技有限公司牵头，广东电网有限责任公司计量中心、广东省网络空间安全协会、广东新兴国家网络安全与信息化发展研究院、广东关键信息基础设施保护中心、广州华南检验检测中心有限公司、网安联认证中心有限公司、国源天顺科技产业集团有限公司等多家单位共同参与编制。

1.3 主要工作过程

（1）2025 年 8 月，标准正式立项，协会组织参与本标准编写的人员启动项目，成立规范编制组，确立各自分工，对标准进行调研，听取各单位的相关意见；

（2）2025 年 9 月-12 月，编制组召开组内研讨会并结合充分的调研结果，参考各类国家标准和相关政策文件，形成标准草案第一稿；结合各参编单位的反馈意见，修改形成标准草案第二稿；

（3）2026 年 1-3 月，编制组召开组内研讨会，基于前期成果，经多次内部讨论研究，组织完善草案内容，形成征求意见稿。

二、标准编制原则和标准编制详细说明及解决的主要问题

2.1 编制原则

本标准的研究与编制工作遵循以下原则：

（1）符合性原则

本标准使用时能够与法律法规和国家强制性标准的要求保持一致，符合国家相关主管部门的要求。

（2）实用性原则

本标准规范是对实际工作成果的总结与提升，保持整体结果合理且维持原意和功能不变的同时，针对用户群体，做到可操作、可用与实用。

2.2 文档结构

《智能合约安全测评过程指南》标准文档分为前言、范围、规范性引用文件、术语和定义、智能合约安全测评过程概述、智能合约安全测评过程、附录A、参考文献等部分内容。

2.3 整体格式

整体格式根据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》的相关要求，对本标准的各要素进行编写和排版。

在标准内容汇总及整个各方意见过程中，对各编写组成员提交部分，根据GB/T 1.1-2020的编写要求进行了必要的增删改，以确保符合一致性、协调性、易用性等文件的表述原则及相关规定。

2.4 标准名称英文翻译

标准的名称“智能合约安全测评过程指南” 翻译为 Smart contract security assessment process guide。

2.5 术语和定义

术语和定义中所列的术语的英文翻译，如有类似术语的标准，参考了其翻译，没有类似术语标准翻译的，通过百度翻译和谷歌翻译后进行对比，并参考网络相关翻译后进行确定。

2.6 智能合约安全测评过程概述

本章主要介绍了智能合约安全测评的完整流程，将其划分为测评准备、测评实施、结果分析与报告编制、以及结果反馈与整改跟踪四个核心阶段。在准备阶段，主要完成团队组建、资料收集与计划制定；在实施阶段，通过环境搭建、静态代码分析、动态测试、可选的形式化验证及安全审计等手段进行深度检测；随后在结果分析与报告编制阶段对发现的问题进行汇总与风险评估，并形成正式报告；最后通过结果反馈与整改跟踪，确保问题得到有效解决，从而形成一个从准备到闭环的完整安全测评体系。

2.7 智能合约安全测评过程

本章主要介绍了智能合约安全测评的完整流程，将其划分为四个紧密相连的阶段。在测评准备阶段，重点在于组建专业的测评团队、全面收集合约相关资料与信息，并制定详尽的测评计划；进入测评实施阶段后，通过环境搭建与部署、静态代码分析、动态测试、可选的形式化验证以及人工安全审计等多种技术手段，对智能合约进行多维度的深度检测；随后在测评结果分析与报告编制阶段，对所有发现的安全问题进行汇总分类、风险评估，并最终编制成专业的测评报告；最后一个阶段是结果反馈与整改跟踪，核心是将报告反馈给开发者并

协助其理解问题，同时对其整改过程进行监督与复查验证，确保所有安全问题得到有效解决，从而形成一个从准备到闭环的完整安全保障体系。

2.8 附录 A

本章主要介绍了智能合约安全测评的完整工作流程图，将其划分为测评准备、测评实施、结果分析与报告编制、结果反馈与整改跟踪四个阶段，并强调测评相关方之间的沟通与洽谈应贯穿始终。其中，准备阶段包括组建团队、收集资料和制定计划；实施阶段涵盖环境搭建、静态代码分析、动态测试、可选的形式化验证及安全审计；分析与报告阶段进行结果汇总、风险评估和报告编制；反馈与跟踪阶段则将测评结果反馈给开发方并持续监督整改，直至安全风险降至可接受范围。。

2.9 参考文献

本章主要引用了三项关键文档，包括国家标准《GB/T 43579-2023 区块链和分布式记账技术 智能合约生命周期管理技术规范》用于指导智能合约从设计、开发、部署到维护的全生命周期安全管理，引用《T/SIA 029-2021 区块链智能合约一般要求》作为智能合约基本功能和安全性的一般性技术规范依据，同时参考了《智能合约安全指南》(2020年云安全联盟大中华区发布)中关于智能合约安全漏洞分析、最佳实践和风险评估的专业指引，这些文献共同构成了本章节内容的重要理论基础和技术支撑。

三、知识产权情况说明

本标准不涉及专利。

四、采用国际标准和国外先进标准情况

无采用国际标准和国外先进标准情况。

五、与现行相关法律、法规、规章及相关标准的协调性

建议本标准推荐性实施。本标准不触犯国家现行法律法规，不与其他强制性国标相冲突。本标准是在遵循我国《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规的基础上，对智能合约这一特定领域的指导测评、自查以及检查工作进行的专项补充和细化，在智能合约的具体落地指引。

六、重大分歧意见的处理经过和依据

《智能合约安全测评过程指南》编制过程中未出现重大分歧。

七、标准性质的建议

建议《智能合约安全测评过程指南》作为推荐性团体标准发布实施。

八、贯彻标准的要求和措施建议

建议本标准发布后，相关行业协会、联盟组织可开展标准的宣贯培训工作。鼓励智能合约应用的开发和运营企业，依据本标准开展安全体系的自查、建设与优化。建议第三方测评机构可将本标准作为开展智能合约应用安全评估时的重要参考依据。

九、替代或废止现行相关标准的建议

无替代或废止。

十、其他应予说明的事项

无。

《智能合约安全测评过程指南》
标准编制组
2026 年 3 月