ICS 35.020
CCS L 70

团　　体　　标　　准

T/GDCSA XXX-2026

智能合约安全测评过程指南

Smart Contract Security Assessment Process Guide

（征求意见稿）

2026-XX-XX 发布　　2026-XX-XX 实施

广东省网络空间安全协会　发布

目　　次

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。

本文件由北京神州绿盟科技有限公司提出。

本文件由广东省网络空间安全协会归口。

本文件起草单位：XXX。

本文件主要起草人：XXX。

智能合约安全测评过程指南

1 范围

本文件规范了智能合约安全测评的工作过程，规定了测评活动及其工作任务。

本文件适用于测评服务机构、运营使用单位以及主管部门开展智能合约安全测评工作。

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 43572-2023 区块链和分布式记账技术 术语

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

3 术语和定义

T/GDCSA XX、T/GDCSA XX、GB/T 43572界定的术语和定义适用于本文件。

4 智能合约安全测评过程概述

智能合约安全测评过程包括测评准备阶段、测评实施阶段、测评结果分析与报告编制阶段、结果反馈与整改跟踪阶段。每一组确定的工作任务，具体如表 1 所示。

表 1 安全测评过程

测评活动	主要工作任务
测评准备阶段	组建测评团队
	收集资料与信息
	制定测评计划
测评实施阶段	环境搭建与部署
	静态代码分析
	动态测试
	形式化验证（可选）
	安全审计
测评结果分析与报告编制阶段	结果汇总与整理
	风险评估与分析
	报告编制
结果反馈与整改跟踪阶段	结果反馈
	整改跟踪

5 智能合约安全测评过程

5.1 测评准备阶段

5.1.1 测评准备阶段主要任务

5.1.1.1 组建测评团队

根据智能合约的复杂程度与业务特点，挑选具备智能合约开发、安全分析、漏洞挖掘、区块链技术等多方面专业知识与经验的人员组建测评团队。团队成员应包括但不限于智能合约安全专家、区块链架构师、测试工程师、安全研究员等，明确各成员的职责与分工，确保测评工作能够高效协同开展。

输入：项目章程、协议

任务描述 ：

a) 根据智能合约的复杂程度与业务特点，挑选具备智能合约开发、安全分析、漏洞挖掘、区块链技术等多方面专业知识与经验的人员组建测评团队。

b) 团队成员应包括但不限于智能合约安全专家、区块链架构师、测试工程师、安全研究员等，明确各成员的职责与分工，确保测评工作能够高效协同开展。

输出/产品 ：测评团队组建报告。

5.1.1.2 收集资料与信息

收集智能合约的相关资料，包括但不限于智能合约的代码、技术文档、业务需求文档、所运行区块链平台的技术说明、以往的安全审计报告（如果有）以及相关法律法规与监管要求等信息。通过对这些资料的全面收集与初步分析，了解智能合约的功能与用途、设计架构、运行环境以及可能面临的安全风险因素，为后续的测评工作奠定基础。

输入内容 ：项目章程、智能合约相关资料（如代码、技术文档、业务需求文档、区块链平台技术说明等）。

任务描述 ：

a) 收集智能合约的相关资料，包括但不限于智能合约的代码、技术文档、业务需求文档、所运行区块链平台的技术说明、以往的安全审计报告以及相关法律法规与监管要求等信息。

b) 对收集到的资料进行全面收集与初步分析，了解智能合约的功能与用途、设计架构、运行环境以及可能面临的安全风险因素。

输出/产品 ：资料收集清单与初步分析报告。

5.1.1.3 制定测评计划

依据收集到的资料与智能合约的安全需求，制定详细的测评计划。测评计划应涵盖测评的目标、范围、依据、方法、时间安排、资源需求以及预期的输出成果等内容。明确每个测评阶段的关键任务与里程碑，合理分配人力、物力资源，确保测评工作按照预定计划有序推进，同时要预留一定的弹性时间，以应对可能出现的意外情况或复杂问题的深入分析。

输入内容 ：资料收集清单与初步分析报告、项目章程、协议。

任务描述 ：

a) 依据收集到的资料与智能合约的安全需求，制定详细的测评计划。

b) 测评计划应涵盖测评的目标、范围、依据、方法、时间安排、资源需求以及预期的输出成果等内容。

c) 明确每个测评阶段的关键任务与里程碑，合理分配人力、物力资源，确保测评工作按照预定计

划有序推进，同时要预留一定的弹性时间，以应对可能出现的意外情况或复杂问题的深入分析。

输出/产品 ：测评计划书。

5.2 测评实施阶段

5.2.1 测评实施阶段主要任务

5.2.1.1 环境搭建与部署

按照智能合约的实际运行环境要求，搭建与之相匹配的测试环境，包括部署区块链节点、配置智能合约运行所需的虚拟机环境、安装相关的依赖库与工具等。确保测试环境的配置与生产环境尽可能一致，以便准确模拟智能合约在实际运行过程中的行为与状态，提高测评结果的可靠性与相关性。在测试环境中部署待测智能合约，进行初步的功能验证，确保合约能够正常运行并具备基本的业务功能，为后续的安全测评工作提供基础保障。

输入内容 ：测评计划书、智能合约代码及相关配置要求。

任务描述 ：

a) 按照智能合约的实际运行环境要求，搭建与之相匹配的测试环境，包括部署区块链节点、配置智能合约运行所需的虚拟机环境、安装相关的依赖库与工具等。

b) 确保测试环境的配置与生产环境尽可能一致，以便准确模拟智能合约在实际运行过程中的行为与状态，提高测评结果的可靠性与相关性。

c) 在测试环境中部署待测智能合约，进行初步的功能验证，确保合约能够正常运行并具备基本的业务功能，为后续的安全测评工作提供基础保障。

输出/产品 ：测试环境部署报告与功能验证记录。

5.2.1.2 静态代码分析

选择合适的静态代码分析工具，对智能合约代码进行全面扫描，识别代码中的潜在安全漏洞、代码质量缺陷以及不符合安全编码规范的地方，如未使用的变量、不安全的函数调用、缺乏输入验证的代码片段等。工具应具备较高的漏洞检测准确率与召回率，能够覆盖常见的智能合约漏洞类型，并提供详细的漏洞报告与修复建议。

测评人员对工具扫描结果进行人工审查与分析，过滤掉误报信息，深入理解每个潜在漏洞的产生原因与影响范围，结合智能合约的业务逻辑，评估其实际的安全风险程度。对于发现的可疑问题，通过手动代码审查的方式进行进一步确认，必要时编写测试用例进行验证，确保不遗漏任何一个可能的安全隐患。

输入内容 ：智能合约代码、测评计划书、静态代码分析工具。

任务描述 ：

a) 选择合适的静态代码分析工具，对智能合约代码进行全面扫描，识别代码中的潜在安全漏洞、代码质量缺陷以及不符合安全编码规范的地方。

b) 工具应具备较高的漏洞检测准确率与召回率，能够覆盖常见的智能合约漏洞类型，并提供详细的漏洞报告与修复建议。

c) 测评人员对工具扫描结果进行人工审查与分析，过滤掉误报信息，深入理解每个潜在漏洞的产生原因与影响范围，结合智能合约的业务逻辑，评估其实际的安全风险程度。

d) 对于发现的可疑问题，通过手动代码审查的方式进行进一步确认，必要时编写测试用例进行验证，确保不遗漏任何一个可能的安全隐患。

输出/产品 ：静态代码分析报告。

5.2.1.3 动态测试

设计并编写一系列针对智能合约功能与安全特性的测试用例，涵盖正常功能测试用例与恶意攻击测试用例。正常功能测试用例用于验证智能合约在预期的输入与操作下的行为是否符合业务要求，确保合约的基本功能正常；恶意攻击测试用例则模拟各类潜在的攻击场景，如重入攻击、整数溢出攻击、拒绝服务攻击等，检测智能合约在面对恶意输入与操作时的防御能力与安全性。在测试环境中执行测试用例，观察智能合约的行为与响应结果，记录测试过程中的各项数据，包括输入参数、合约状态变化、输出结果、资源消耗情况等。通过分析测试结果，发现智能合约在运行过程中存在的安全漏洞与异常行为，如合约状态未按预期更新、资源消耗异常、出现运行时错误等。对于发现的问题，进行详细的定位与分析，确定问题的根本原因所在。

输入内容 ：智能合约代码、测评计划书、测试用例设计指南、动态测试工具。

任务描述 ：

a) 设计并编写一系列针对智能合约功能与安全特性的测试用例，涵盖正常功能测试用例与恶意攻击测试用例。

b) 正常功能测试用例用于验证智能合约在预期的输入与操作下的行为是否符合业务要求，确保合约的基本功能正常；恶意攻击测试用例则模拟各类潜在的攻击场景，如重入攻击、整数溢出攻击、拒绝服务攻击等，检测智能合约在面对恶意输入与操作时的防御能力与安全性。

c) 在测试环境中执行测试用例，观察智能合约的行为与响应结果，记录测试过程中的各项数据，包括输入参数、合约状态变化、输出结果、资源消耗情况等。

d) 通过分析测试结果，发现智能合约在运行过程中存在的安全漏洞与异常行为，如合约状态未按预期更新、资源消耗异常、出现运行时错误等。对于发现的问题，进行详细的定位与分析，确定问题的根本原因所在。

输出/产品 ：动态测试报告。

5.2.1.4 形式化验证（可选）

对于对安全性要求极高的智能合约，如涉及大量资产转移、关键基础设施控制等场景的合约，可采用形式化验证方法。利用专业的形式化验证工具与数学建模技术，对智能合约的业务逻辑进行严格的数学证明，确保其关键功能与特性在所有可能的输入情况下均能正确无误地执行，不存在逻辑漏洞与安全隐患。形式化验证过程需要专业的数学与逻辑知识，应由具备相关经验的人员进行实施，并与其他测评方法相结合，相互补充验证结果，提高智能合约安全性评估的全面性与可靠性。

输入内容 ：智能合约代码、测评计划书、形式化验证工具。

任务描述 ：

a) 对于对安全性要求极高的智能合约，如涉及大量资产转移、关键基础设施控制等场景的合约，可采用形式化验证方法。

b) 利用专业的形式化验证工具与数学建模技术，对智能合约的业务逻辑进行严格的数学证明，确保其关键功能与特性在所有可能的输入情况下均能正确无误地执行，不存在逻辑漏洞与安全隐患。

c) 形式化验证过程需要专业的数学与逻辑知识，应由具备相关经验的人员进行实施，并与其他测评方法相结合，相互补充验证结果，提高智能合约安全性评估的全面性与可靠性。

输出/产品 ：形式化验证报告。

5.2.1.5 安全审计

测评人员对智能合约进行人工安全审计，从架构设计、代码实现、访问控制、数据管理、与外部系统交互等多个维度对合约进行全面审查。检查智能合约是否遵循了良好的安全设计原则，如最小权限原则、防御纵深原则等；评估代码实现的质量与安全性，是否存在容易被忽视的细微漏洞或安全隐患；分析访问控制机制是否合理有效，能否防止未授权访问与操作；审查数据存储与处理过程中的安全措施是否到位，能否保障数据的保密性、完整性和可用性；检查与外部系统的交互接口是否存在安

全风险，如外部调用的可靠性、返回值处理等。

在安全审计过程中，测评人员应依据自身的专业知识与经验，结合智能合约的实际应用场景，进行深入的思考与分析，挖掘潜在的安全问题。同时，与其他测评方法发现的问题进行交叉验证，形成完整的安全问题清单，确保对智能合约安全状况的全面、准确把握。

输入内容 ：智能合约代码、测评计划书、相关技术文档、相关安全审计标准。

任务描述 ：

a) 测评人员对智能合约进行人工安全审计，从架构设计、代码实现、访问控制、数据管理、与外部系统交互等多个维度对合约进行全面审查。

b) 检查智能合约是否遵循了良好的安全设计原则，如最小权限原则、防御纵深原则等；评估代码实现的质量与安全性，是否存在容易被忽视的细微漏洞或安全隐患；分析访问控制机制是否合理有效，能否防止未授权访问与操作；审查数据存储与处理过程中的安全措施是否到位，能否保障数据的保密性、完整性和可用性；检查与外部系统的交互接口是否存在安全风险，如外部调用的可靠性、返回值处理等。

c) 在安全审计过程中，测评人员应依据自身的专业知识与经验，结合智能合约的实际应用场景，进行深入的思考与分析，挖掘潜在的安全问题。同时，与其他测评方法发现的问题进行交叉验证，形成完整的安全问题清单，确保对智能合约安全状况的全面、准确把握。

输出/产品 ：安全审计报告。

5.3 测评结果分析与报告编制阶段

5.3.1 测评结果分析与报告编制阶段主要任务

5.3.1.1 结果汇总与整理

将通过静态代码分析、动态测试、形式化验证（如有）以及安全审计等不同测评方法发现的安全问题进行汇总整理，按照漏洞的类型、位置、风险等级等维度进行分类统计，形成详细的安全问题清单。对每个安全问题进行清晰、准确的描述，包括问题的产生原因、影响范围、风险等级以及相应的证明信息（如测试用例、代码片段、运行时截图等），确保报告读者能够充分理解问题的严重性与重要性。

输入内容 ：静态代码分析报告、动态测试报告、形式化验证报告（如有）、安全审计报告。

任务描述 ：

a) 将通过静态代码分析、动态测试、形式化验证（如有）以及安全审计等不同测评方法发现的安全问题进行汇总整理。

b) 按照漏洞的类型、位置、风险等级等维度进行分类统计，形成详细的安全问题清单。

c) 对每个安全问题进行清晰、准确的描述，包括问题的产生原因、影响范围、风险等级以及相应的证明信息（如测试用例、代码片段、运行时截图等），确保报告读者能够充分理解问题的严重性与重要性。

输出/产品 ：安全问题汇总清单。

5.3.1.2 风险评估与分析

基于建立的安全风险评估模型，对汇总整理后的安全问题进行深入的风险评估与分析，确定每个问题的具体风险等级（如高、中、低风险），并综合评估智能合约整体的安全风险状况。分析风险发生的可能性、影响范围以及对智能合约业务功能与用户资产的潜在危害，为智能合约的开发者提供明确的风险警示与整改优先级建议，帮助其合理分配资源进行安全修复工作。

输入内容 ：安全问题汇总清单、风险评估模型。

任务描述 ：

a) 基于建立的安全风险评估模型，对汇总整理后的安全问题进行深入的风险评估与分析。

b) 确定每个问题的具体风险等级（如高、中、低风险），并综合评估智能合约整体的安全风险状况。

c) 分析风险发生的可能性、影响范围以及对智能合约业务功能与用户资产的潜在危害，为智能合约的开发者提供明确的风险警示与整改优先级建议，帮助其合理分配资源进行安全修复工作。

输出/产品 ：测评报告的安全问题风险分析部分。

5.3.1.3 报告编制

报告应涵盖智能合约的基本信息、测评的目的与依据、测评的范围与方法、测评结果（包括安全问题清单与风险评估结果）、整改建议以及测评结论等内容。报告语言应专业、严谨、客观，数据与事实应准确无误，分析与结论应清晰明了，能够为不同层次的读者（如开发者、使用者、监管者等）提供有价值的信息，帮助其做出合理的决策。

输入内容 ：安全问题汇总清单、测评报告的安全问题风险分析部分、测评计划书、相关标准规范。

任务描述 ：

a) 编制详细的智能合约安全测评报告。

b) 报告应涵盖智能合约的基本信息、测评的目的与依据、测评的范围与方法、测评结果（包括安全问题清单与风险评估结果）、整改建议以及测评结论等内容。

c) 报告语言应专业、严谨、客观，数据与事实应准确无误，分析与结论应清晰明了，能够为不同层次的读者（如开发者、使用者、监管者等）提供有价值的信息，帮助其做出合理的决策。

输出/产品 ：智能合约安全测评报告。

5.4 结果反馈与整改跟踪阶段

5.4.1 结果反馈与整改跟踪阶段主要任务

5.4.1.1 结果反馈

将编制完成的安全测评报告及时反馈给智能合约的开发者以及相关利益方，确保他们能够及时了解智能合约的安全状况与存在的问题。在反馈过程中，测评机构应提供必要的技术支持与解释说明，帮助开发者理解报告内容与问题细节，解答他们在阅读报告过程中产生的疑问，确保反馈信息的有效传递与准确理解。

5.4.1.1 结果反馈

输入内容 ：智能合约安全测评报告。

任务描述 ：

a) 将编制完成的安全测评报告及时反馈给智能合约的开发者以及相关利益方，确保他们能够及时了解智能合约的安全状况与存在的问题。

b) 在反馈过程中，测评机构应提供必要的技术支持与解释说明，帮助开发者理解报告内容与问题细节，解答他们在阅读报告过程中产生的疑问，确保反馈信息的有效传递与准确理解。

输出/产品 ：结果反馈记录。

5.4.1.2 整改跟踪

开发者依据测评报告中的问题与建议，对智能合约进行安全整改与修复工作。测评机构应对开发者的整改过程进行跟踪与监督，要求开发者定期反馈整改进度与结果，必要时提供进一步的技术指导与支持。在开发者完成整改后，测评机构可对整改后的智能合约进行复查，验证整改措施的有效性，确保安全问题得到彻底解决，智能合约的安全性得到显著提升。整改跟踪工作应持续进行，直至智能

合约的安全风险降低到可接受的范围内，保障智能合约在安全的状态下运行。

输入内容 ：智能合约安全测评报告、整改反馈信息。

任务描述 ：

a) 开发者依据测评报告中的问题与建议，对智能合约进行安全整改与修复工作。

b) 测评机构应对开发者的整改过程进行跟踪与监督，要求开发者定期反馈整改进度与结果，必要时提供进一步的技术指导与支持。

c) 在开发者完成整改后，测评机构可对整改后的智能合约进行复查，验证整改措施的有效性，确保安全问题得到彻底解决，智能合约的安全性得到显著提升。

d) 整改跟踪工作应持续进行，直至智能合约的安全风险降低到可接受的范围内，保障智能合约在安全的状态下运行。

输出/产品 ：整改跟踪报告与复查验证记录。

附 录 A
（规范性）
智能合约安全测评工作流程

测评准备阶段涵盖组建专业测评团队、收集资料与信息以及制定详细测评计划；测评实施阶段包括环境搭建与部署、静态代码分析、动态测试、形式化验证（可选）和安全审计；测评结果分析与报告编制阶段需完成结果汇总与整理、风险评估与分析以及报告编制；结果反馈与整改跟踪阶段则涉及反馈测评结果并持续跟踪整改情况，直至智能合约安全风险降至可接受范围，保障其安全运行；测评相关方之间的沟通与洽谈应贯穿整个安全测评过程。具体如图 1 所示。

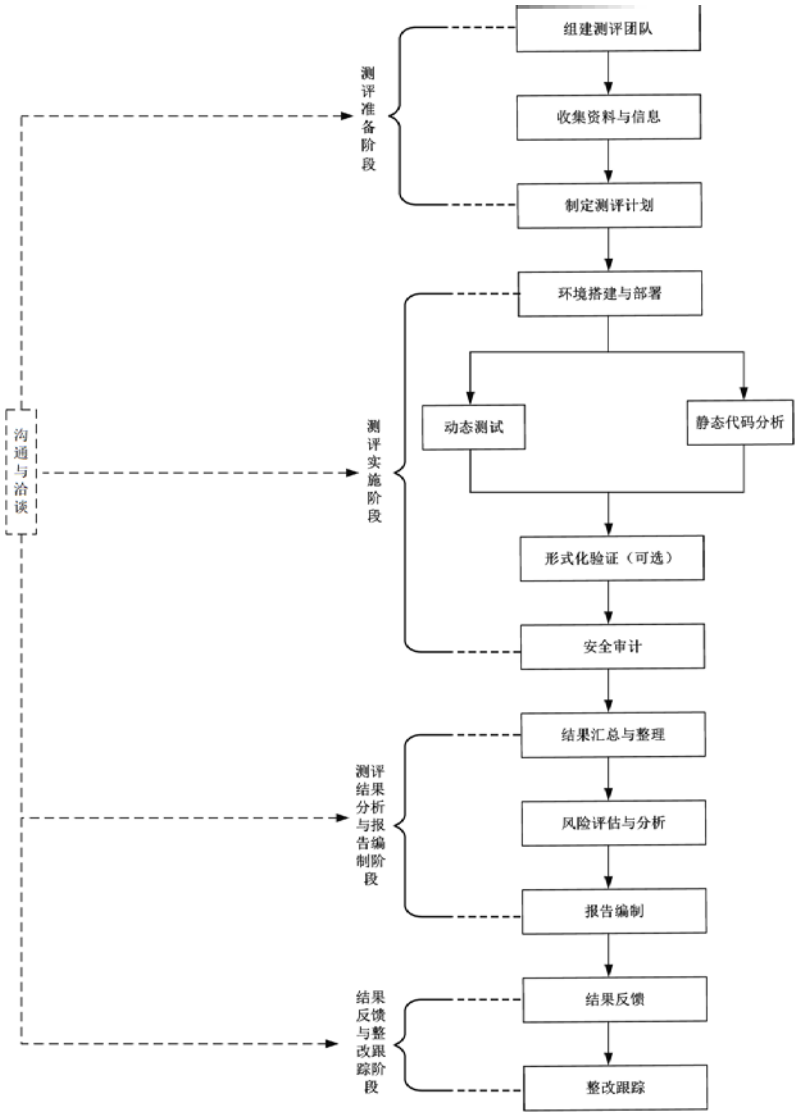

图 1 安全测评工作流程图

参 考 文 献

[1] 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
[2] T/SIA 029-2021 区块链智能合约一般要求
[3] 智能合约安全指南（2020年云安全联盟大中华区发布）