ICS 35.020
CCS L 70

团　　体　　标　　准

T/GDCSA XXX-2026

智能合约安全测评要求

Requirements for Smart Contract Evaluation

（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。

智能合约安全测评要求

1 范围

本文件规定了区块链智能合约安全要求，从智能合约的安全设计、代码安全、访问安全、数据安全、环境安全五个层面提供了智能合约测评要求。

本文件适用于测评服务机构开展安全测评、运营使用单位开展安全自查，以及主管部门开展安全检查的过程提供指导。

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

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

访谈 interview

测评人员通过引导智能合约相关人员进行有目的的（有针对性的）交流以帮助测评人员理解、澄清或取得证据的过程。

[来源:GB/T 28448-2019,3.1]

3.2

核查 examine

测评人员通过对测评对象（如文档、各类源代码以及相关配置）进行观察、查验和分析，以帮助测评人员理解、澄清或取得证据的过程。

[来源:GB/T 28448-2019,3.2]

3.3

测试 test

测评人员使用预定的方法/工具使测评对象产生特定的结果，将运行结果与预期的结果进行比对的过程。

[来源:GB/T 28448-2019,3.3，有修改]

3.4

区块链 blockchain

使用密码链接将共识确认过的区块按顺序追加形成的分布式账本。

注：区块链被设计用来抵抗篡改，并创建最终的、确定的、不可变的账本记录。

[来源:GB/T 43572-2023,3.6]

3.5

智能合约 smart contract

存储在分布式记账技术系统中的计算机程序，该程序的任何执行结果都记录在分布式账本中。

注：智能合约可以在法律上代表合同条款，并在适用司法管辖区的法律下产生可强制执行的义务。

[来源:GB/T 43572-2023,3.72]

4 智能合约安全测评概述

智能合约安全测评是依据相关标准和规范，采用科学、合理的方法和手段，对智能合约的安全性进行全面、系统的评估过程。通过测评，能够及时发现智能合约在安全设计、代码安全、访问安全、数据安全，以及环境安全等方面存在的安全隐患和风险，为智能合约的改进和优化提供依据，确保其在区块链系统中安全、可靠地运行。智能合约安全测评的基本方法是针对智能合约，采用相关的测评手段，遵从一定的测评规范，获取需要的证据数据，给出是否达到特定要求的评判。

5 测评要求

5.1 安全设计

5.1.1 安全设计原则

5.1.1.1 测评单元（01）

该测评单元包括以下要求：

a) 测评指标：应遵循最小权限原则，在智能合约的架构设计与权限分配中，确保所有实体（如用户、合约、系统组件）的权限被严格限定于其职责所需的最小必要范围。

b) 测评对象：智能合约架构设计文档、权限模型说明。

c) 测评实施：

1) 应应核查智能合约的架构设计文档与权限模型说明，是否明确识别并定义了所有交互实体（如用户角色、管理员、外部合约）及其职责，并为其预设了完成职责所需的最小权限集合。

2) 应核查关键操作（如资产转移、权限变更、合约自毁）的访问控制逻辑，是否强制要求了特定高级别权限，并确保该权限未被过度授予。

5.1.1.2 测评单元（02）

该测评单元包括以下要求：

a) 测评指标：应遵循攻击面最小化原则，在满足业务需求的前提下，通过架构设计尽可能减少智能合约与外部环境不必要的交互点与信息暴露范围。

b) 测评对象：智能合约架构设计文档、应用程序接口文件、智能合约源代码。

c) 测评实施：

1) 应核查智能合约的架构设计文档与最终部署的接口文件，确认所有对外暴露的公共和外部函数均为业务所必需，且已识别并论证其存在的合理性。
2) 应核查智能合约源代码，确认非必要的状态变量、函数已被设置为私有或内部可见性，且合约未包含已被弃用但未移除的遗留接口。
3) 应核查合约与外部组件的交互设计，确认其交互链路是必要的且是否实现最小化原则，以避免引入不必要的信任假设和复杂性。

5.1.1.3 测评单元（03）

该测评单元包括以下要求：

a) 测评指标：应采用纵深防御策略，在智能合约的代码、访问控制、数据校验及运行环境等多个层面协同部署安全措施，构建冗余互备的防御体系。
a) 测评对象：智能合约安全架构设计文档、智能合约源代码、部署环境配置文档。
b) 测评实施：
   1) 应核查智能合约安全架构概述，确认其明确指出了在代码、访问控制、数据、环境等不同层面所部署的安全措施，并说明了这些措施如何协同提供防护。
   2) 应结合源代码核查，验证针对同一关键风险，如非法输入、重入攻击，是否在多个层面，如输入验证、重入锁、监控告警，设置了互补的防御措施。
   3) 应核查部署环境配置文档或审计日志，确认运行环境层面，如虚拟机安全配置、节点安全策略，的安全措施已启用，并与合约层面的防御形成互补。

5.1.1.4 测评单元（04）

该测评单元包括以下要求：

a) 测评指标：应遵循默认安全原则，确保智能合约的初始状态、默认配置及失败处理模式均处于安全状态，例如异常情况下的状态回滚与访问拒绝。
b) 测评对象：智能合约设计文档、初始化函数/构造函数代码、配置管理文档、错误处理逻辑代码。
c) 测评实施：
   1) 应核查智能合约的构造函数或初始化函数，确认合约部署后的初始状态，如所有权、开关状态、关键参数，是安全且符合预期的，例如管理员地址已正确设置，非关键功能默认处于关闭状态。
   2) 应核查合约的配置项及其默认值，确认在未进行显式配置的情况下，合约会采用一个安全的默认配置运行。
   3) 应核查合约的错误处理与异常管理逻辑，确认在操作失败或遇到未预期异常时，合约会执行状态回滚或采取安全的失败处理模式，如“默认拒绝”，而非进入一个不确定的或不安全的状态。

5.2 代码安全

5.2.1 语言规范与安全性

5.2.1.1 测评单元（01）

该测评单元包括以下要求：

a) 测评指标：应使用经过充分验证、具有良好安全特性的智能合约编程语言进行开发，避免使用存在已知严重安全漏洞的语言版本或特性。
b) 测评对象：智能合约源代码文件、编译器配置文件、项目技术文档。

c） 测评实施：

4) 应核查智能合约选用的编程语言及其具体版本是否属于该语言社区广泛认可、经过充分测试的稳定版本，且无已知可被利用的严重安全漏洞。

5) 应核查合约代码及编译器配置是否主动禁用或规避了所选语言中已知的不安全或高危实验性特性。

6) 应核查项目技术文档是否明确说明了所选编程语言及其版本的安全性和选型依据。

5.2.1.2 测评单元（02）

该测评单元包括以下要求：

a） 测评指标：应遵循该语言的安全编码规范，严格遵循代码格式规范，确保代码可读性与可维护性，便于后续审查与排查潜在问题。

b） 测评对象：智能合约代码、代码格式检查工具的配置文件。

c） 测评实施：

1) 应核查代码是否遵循智能合约开发语言的安全编码规范，可通过代码审查工具或人工核查的方式，查看代码是否存在违反安全编码规范的情况，如是否存在不安全的函数调用、未正确处理异常等。

2) 应核查代码格式是否统一规范，包括缩进、括号位置、变量命名规则等，可通过核查代码格式检查工具的配置文件，查看其是否按照公认的代码格式规范进行配置，以及核查代码是否通过该工具的格式核查。

5.2.2 逻辑正确性

5.2.2.1 测评单元（01）

该测评单元包括以下要求：

a） 测评指标：智能合约的业务逻辑应精确反映其设计意图，避免逻辑漏洞如条件判断错误、循环终止条件不当等，杜绝可能导致意外行为或资产损失的逻辑缺陷。

b） 测评对象：智能合约代码、业务逻辑设计文档。

c） 测评实施：

1) 应核查智能合约代码与业务逻辑设计文档的一致性，确保代码实现与设计意图相符，可通过对比代码与设计文档中的功能描述、流程逻辑等方式进行核查。

2) 应核查代码中的条件判断语句、循环结构等关键逻辑部分，核查是否存在逻辑漏洞，如条件判断表达式书写错误、循环终止条件设置不合理等情况，可通过代码静态分析工具辅助核查，同时结合人工核查的方式进行详细分析。

5.2.2.2 测评单元（02）

该测评单元包括以下要求：

a） 测评指标：对于涉及资产转移、权限变更等关键操作的逻辑，应进行严谨的数学建模与测试，确保其在所有可能的输入情况下均能正确执行，防止因逻辑偏差引发的漏洞利用。

b） 测评对象：智能合约中关键操作的逻辑代码、数学模型文档、测试用例集合。

c） 测评实施：

1) 应核查关键操作逻辑是否进行了严谨的数学建模，确保其能够全面准确地描述业务规则和操作流程，可通过核查数学模型文档，查看模型是否完整、合理地涵盖了关键操作的所有可能情况。

2) 应测试关键操作逻辑在所有可能的输入情况下是否均能正确执行，可通过测试用例集合

进行功能测试和边界测试，核查在各种输入条件下智能合约的行为是否符合预期，同时可结合形式化验证工具对关键逻辑进行更深层次的测试。

5.2.3 输入验证

5.2.3.1 测评单元（01）

该测评单元包括以下要求：

a) 测评指标：对所有外部输入的数据，包括用户输入、其他合约调用传入的参数等，应进行全面、严格的验证，验证内容应涵盖数据类型、格式、取值范围、合法性等方面，确保输入数据符合预期且不会破坏合约逻辑。

b) 测评对象：智能合约中处理外部输入的代码、输入验证逻辑、测试用例。

c) 测评实施：

1) 应核查智能合约是否对所有外部输入的数据进行了测试，包括用户输入和其他合约调用传入的参数，确保这些数据符合预期的格式、范围和类型，可通过核查代码中的输入验证逻辑，查看其是否全面覆盖了各种可能的输入情况。

2) 应核查智能合约是否对所有外部输入的数据类型、格式、取值范围和合法性进行了全面测试，确保输入数据符合预期。可通过核查代码中的输入验证逻辑，查看其是否全面、严谨地涵盖了所有必要的验证条件。

3) 应测试智能合约在接收到不符合要求的外部输入时的处理方式，核查是否存在因输入验证不当导致的安全漏洞和异常行为，可通过测试用例模拟各种可能的恶意输入情况，观察智能合约的行为是否符合预期，并确保其能够正确地拒绝或处理这些输入。同时可借助自动化测试工具和人工审查的方式，对输入验证逻辑进行详细分析。

5.2.3.2 测评单元（02）

该测评单元包括以下要求：

a) 测评指标：对于不符合验证要求的输入，应采取合理的拒绝处理机制，并记录详细的错误信息，以便后续分析与溯源，防止恶意输入干扰合约正常运行。

b) 测评对象：智能合约中输入验证逻辑、错误处理机制、日志记录功能。

c) 测评实施：

1) 应核查智能合约是否对不符合验证要求的输入采取了合理的拒绝处理机制，确保智能合约能够正确地拒绝无效输入，可通过核查代码中的输入验证逻辑和错误处理代码，查看其是否明确地拒绝不符合要求的输入，并且不会导致合约进入异常状态。

2) 应测试智能合约在拒绝不符合验证要求的输入时，是否记录了详细的错误信息，包括错误类型、时间戳、输入内容等，以便后续分析与溯源，可通过查看日志记录功能，核查其是否完整、准确地记录了相关错误信息。同时，可以使用测试用例模拟不符合验证要求的输入，观察智能合约是否正确记录错误信息，并确保这些信息能够帮助开发人员进行问题排查和分析。

5.2.4 错误处理与异常管理

5.2.4.1 测评单元（01）

该测评单元包括以下要求：

a) 测评指标：在智能合约中合理设置错误处理机制，针对可能出现的各类异常情况，如资源不足、外部调用失败、数据不一致等，应定义明确的错误处理流程，确保合约在遇到异常时能够准确地处理，避免陷入不可预知的状态或导致系统崩溃。

b） 测评对象：智能合约错误处理逻辑、测试用例集合。

c） 测评实施：

1) 应访谈开发人员，了解异常分类的依据、错误处理流程的设计原则等。

2) 应核查智能合约是否为可能出现的各类异常情况定义了明确的错误处理流程，确保合约能够处理异常情况。可通过核查代码中的错误处理逻辑，查看其是否全面覆盖了各种可能的异常情况，如资源不足、外部调用失败、数据不一致等。

3) 应测试智能合约在遇到异常时是否能够按照定义的错误处理流程正确执行，避免陷入不可预知的状态或导致系统崩溃。可通过测试用例集合模拟各种异常情况，观察智能合约的行为是否符合预期，并确保其能够正确地处理异常。同时，可结合代码审查和调试工具，对错误处理机制进行详细分析。

4) 应核查智能合约在处理异常时是否记录了详细的错误信息，以便后续分析与溯源。可通过查看日志记录功能，核查其是否完整、准确地记录了相关错误信息，包括错误类型、时间戳、错误来源等。同时，可以使用测试用例模拟异常情况，观察智能合约是否正确记录错误信息，并确保这些信息能够帮助开发人员进行问题排查和分析。

5.2.4.2 测评单元（02）

该测评单元包括以下要求：

a） 测评指标：对于关键操作，应在执行前后进行状态检查与校验，利用断言等机制及时捕获逻辑偏差或错误状态，及时终止异常操作并给出明确的错误提示，便于开发者快速定位与修复问题。

b） 测评对象：智能合约关键操作代码、断言实现、测试用例。

c） 测评实施：

1) 应核查智能合约是否在关键操作执行前后进行状态核查与校验，确保操作符合预期状态，可通过核查代码中的状态核查逻辑，查看其是否全面覆盖了关键操作的前后状态。

2) 应测试智能合约是否利用断言等机制及时捕获逻辑偏差或错误状态，确保能够及时终止异常操作并给出明确的错误提示。可通过测试用例模拟各种可能的异常状态，观察智能合约是否能够正确地捕获并终止操作，同时核查其是否提供了清晰的错误提示信息，便于开发者快速定位与修复问题。

5.2.4.3 测评单元（03）

该测评单元包括以下要求：

a） 测评指标： 智能合约的安全设计应结合防御性编程思想与结构化机制，对关键操作实施严格的前置、后置状态校验策略，确保操作在执行前后合约均处于预期且一致的状态，主动预防并拦截异常状态下的操作执行。

b） 测评对象：智能合约源代码、合约架构设计文档、测试用例。

c） 测评实施：

1) 应核查智能合约源代码，确认其是否采用了防御性编程范式。

2) 应核查关键操作的代码逻辑，确认其是否在执行前进行了必要的前置状态校验、后置状态校验。

3) 应核查状态校验失败时的处理机制，确保合约能通过回滚操作、抛出异常并给出明确错误信息的方式，优雅地终止异常流程，使状态恢复至操作前。

4) 应通过模拟异常输入和攻击场景的测试用例，验证状态校验与防御机制能否正确拦截异常操作、触发断言并保持状态一致。

5.3 访问安全

5.3.1 身份认证与授权

5.3.1.1 测评单元（01）

该测评单元包括以下要求：

a) 测评指标：应采用安全可靠的身份认证机制，对调用智能合约的用户、合约或其他实体进行准确的身份识别，如通过数字签名、加密密钥等技术手段验证身份合法性。

b) 测评对象：智能合约身份认证代码、数字签名验证逻辑、加密密钥管理机制。

c) 测评实施：

1) 应核查智能合约是否采用了安全可靠的身份认证机制，确保调用方身份的合法性。可通过核查代码中的身份认证逻辑，查看其是否正确实现了数字签名验证、加密密钥验证等技术手段。

2) 应测试智能合约在身份认证过程中的安全性，包括数字签名是否难以伪造、加密密钥是否安全存储与管理等。可通过测试用例模拟非法调用情况，观察智能合约是否能够正确识别并拒绝非法调用，同时核查其是否记录了相关错误信息，便于后续分析与溯源。

5.3.1.2 测评单元（02）

该测评单元包括以下要求：

a) 测评指标：应依据最小权限原则，严格限制不同身份主体对智能合约功能与数据的访问权限，明确授权范围，确保每个主体仅能执行其被授权的操作，防止越权访问与操作引发的安全风险。

b) 测评对象：智能合约访问控制代码、智能合约设计文档、权限配置文件、测试用例集合。

c) 测评实施：

1) 应核查智能合约是否依据最小权限原则对不同身份主体的访问权限进行了严格限制，确保每个主体仅能执行其被授权的操作。可通过核查代码中的访问控制逻辑和权限配置文件，查看其是否正确实现了最小权限访问控制，确保不同身份主体的权限范围明确且合理。

2) 应测试智能合约在面对越权访问与操作时的处理机制，确保其能够及时拒绝并记录相关行为。可通过测试用例模拟越权访问情况，观察智能合约是否能够正确地识别并拒绝越权操作，同时核查其是否记录了详细的错误信息，便于后续分析与溯源。

3) 应核查智能合约源代码，验证其权限检查逻辑（如权限修饰符、函数内的条件判断）是否与设计的权限模型严格一致，确保无权限冗余或缺失。

5.3.2 权限管理与变更控制

5.3.2.1 测评单元（01）

该测评单元包括以下要求：

a) 测评指标：应建立完善的权限管理体系，对权限的分配、修改、撤销等操作进行详细记录与审计，确保权限变更过程可追溯。在进行权限调整时，需经过严格的审批流程，避免因权限管理失误导致安全漏洞。

b) 测评对象：权限管理代码、权限变更记录、审批流程文件。

c) 测评实施：

1) 应核查智能合约是否建立了完善的权限管理体系，确保对权限的分配、修改、撤销等操作进行了详细记录与审计，可通过核查权限管理代码和权限变更记录，查看其是否完整、准确地记录了权限变更的时间、操作主体、变更内容等信息，确保权限变更过程可追溯。

2) 应核查审批流程文件，查看其是否明确规定了权限调整的审批步骤和责任人，同时可通过测试用例模拟权限调整操作，观察智能合约是否正确执行审批流程，并确保在未经过审批的情况下无法进行权限调整。
3) 应测试权限调整是否经过严格的审批流程，避免因权限管理失误导致安全漏洞。

5.3.2.2 测评单元（02）

该测评单元包括以下要求：

a) 测评指标：应对智能合约中的关键功能与数据访问点，设置多层次的访问控制策略，如结合时间限制、调用次数限制等动态因素，增强访问控制的灵活性与安全性，适应不同场景下的安全需求变化。
b) 测评对象：智能合约访问控制代码、访问策略配置文件。
c) 测评实施：
1) 应核查智能合约是否在关键功能与数据访问点设置了多层次的访问控制策略，包括时间限制、调用次数限制等动态因素。可通过核查访问控制代码和访问策略配置文件，查看其是否正确实现了多层次访问控制策略，确保不同场景下的安全需求得到满足。
2) 应测试智能合约的访问控制策略在实际操作中的有效性，确保其能够正确执行访问控制规则，防止未经授权的访问。可通过测试用例模拟各种访问场景，观察智能合约是否能够正确地拒绝或允许访问，并核查其是否记录了相关的访问控制日志，便于后续分析与溯源。

5.4 数据安全

5.4.1 数据机密性保护

5.4.1.1 测评单元（01）

该测评单元包括以下要求：

a) 测评指标：对智能合约中涉及的敏感数据，如用户隐私信息、资产密钥、商业机密等，在存储与传输过程中应采用经过认可的加密算法进行加密处理，确保数据的保密性与完整性。
b) 测评对象：智能合约中的敏感数据存储与传输代码、加密算法实现。
c) 测评实施：
1) 应核查智能合约是否对涉及的敏感数据在存储与传输过程中采用了经过认可的加密算法进行加密处理，确保数据的保密性与完整性。可通过核查代码中的加密算法实现，查看其是否使用了如 SM4 等被广泛认可的加密算法。
2) 应测试智能合约在实际操作中加密处理的有效性，确保敏感数据在存储与传输过程中不会被轻易窃取。可通过测试用例模拟敏感数据的存储与传输过程，观察加密处理是否正确执行，可使用专业的加密分析工具对加密算法的实现进行安全性评估。

5.4.1.2 测评单元（02）

该测评单元包括以下要求：

a) 测评指标：根据数据的重要程度与应用场景，合理选择对称加密与非对称加密算法的组合使用，在保证加密强度的同时，兼顾加密解密效率，以适应智能合约在区块链环境中的性能要求。
b) 测评对象：智能合约中的加密算法实现、性能测试结果。
c) 测评实施：
1) 应核查智能合约是否根据数据的重要程度与应用场景合理选择了对称加密与非对称加密算法的组合使用，确保在保证加密强度的同时兼顾加密解密效率。可通过核查加密算法实现，查看其是否正确实现了对称加密算法（如 SM4）和非对称加密算法（如 SM2）的组

合，并评估其是否符合区块链环境中的性能要求。

2) 应测试智能合约在实际操作中的加密解密效率，确保其能够适应智能合约在区块链环境中的性能要求，可使用专业的性能测试工具对智能合约的加密性能进行详细评估。

5.4.2 数据完整性保护

5.4.2.1 测评单元（01）

该测评单元包括以下要求：

a) 测评指标：为防止智能合约数据在存储、传输与处理过程中被篡改，应采用数据完整性验证机制，如哈希算法、数字签名等技术，对关键数据进行完整性校验。在每次数据读取或更新操作时，均需验证数据的完整性，一旦发现数据被篡改，立即采取相应的措施，如回滚操作、记录异常并报警等，确保数据的真实可靠性。

b) 测评对象：智能合约数据完整性验证代码、哈希值计算与存储逻辑、数字签名生成与验证逻辑。

c) 测评实施：

1) 应核查智能合约是否采用了数据完整性验证机制，在关键数据的存储、传输与处理过程中进行完整性校验，确保数据不被篡改，可通过核查代码中的哈希算法和数字签名等实现逻辑，查看其是否正确实施了完整性校验措施，并且确保哈希值计算与存储、数字签名生成与验证等环节无漏洞，并核查其是否记录了详细的篡改事件信息，便于后续分析与溯源。

2) 应测试智能合约在数据读取或更新操作时是否均能正确执行数据完整性验证，确保其能够及时发现数据篡改行为。可通过测试用例模拟数据被篡改的情况，观察智能合约是否能够准确识别篡改行为，并立即采取回滚操作、记录异常信息以及报警等措施，确保数据的真实可靠性。

5.4.2.2 测评单元（02）

该测评单元包括以下要求：

a) 测评指标：应定期对智能合约的数据存储结构进行备份与一致性检查，通过对比备份数据与当前数据的完整性校验值，及时发现并修复潜在的数据损坏或篡改问题，保障智能合约数据的长期可靠性与可用性。

a) 测评对象：数据备份机制、一致性检查代码、完整性校验值存储与对比逻辑。

b) 测评实施：

1) 应核查智能合约是否建立了定期备份数据存储结构的机制，可通过核查备份机制的相关代码和配置文件，查看其是否合理配置了备份的时间间隔以及备份数据的存储位置。同时，核查完整性校验值的存储方式，确保其安全可靠，可通过查看校验值存储与对比逻辑，评估校验值是否被妥善保管，防止被篡改或丢失。

2) 应测试智能合约的一致性检查代码的有效性，确保其能够准确对比备份数据与当前数据的完整性校验值，及时发现数据损坏或篡改问题。可通过测试用例模拟数据损坏或篡改的情况，观察智能合约是否能够及时发现并记录相关问题。

5.4.3 隐私保护

5.4.3.1 测评单元（01）

该测评单元包括以下要求：

a) 测评指标：在智能合约设计阶段，充分考虑用户隐私保护需求，采用隐私增强技术，如零知识证明、同态加密等，在不泄露用户敏感信息的前提下，实现智能合约的业务功能，确保用户在参与区块链系统时的隐私权益得到有效保障。

a) 测评对象：智能合约设计文档、隐私增强技术实现代码、零知识证明与同态加密逻辑。
b) 测评实施：
   1) 应核查智能合约设计文档是否充分考虑了用户隐私保护需求，确保在设计阶段就明确了隐私保护的目标和措施。可通过核查设计文档中的隐私保护部分，查看其是否详细描述了采用的隐私增强技术及其应用场景。
   2) 应核查相关代码实现，查看其是否正确应用了隐私增强技术，如零知识证明和同态加密等。
   3) 应测试智能合约是否正确实现使用了隐私增强技术，如零知识证明和同态加密等，确保其在不泄露用户敏感信息的前提下能够正常实现业务功能。

5.4.3.2 测评单元（02）

该测评单元包括以下要求：
b) 测评指标：对于涉及多方数据共享的智能合约场景，应明确数据共享的范围、目的与条件，通过制定严格的隐私政策与数据共享协议，规范数据共享行为，防止用户隐私数据在未经允许的情况下被过度收集、使用或传播。
a) 测评对象：智能合约中的数据共享逻辑、隐私政策文件、数据共享协议。
b) 测评实施：
   1) 应核查智能合约是否明确了数据共享的范围、目的与条件，确保数据共享行为符合隐私政策和协议的要求。可通过核查数据共享逻辑和相关的隐私政策文件、数据共享协议，查看其是否详细规定了数据共享的具体规则和限制条件。
   2) 应测试智能合约在数据共享过程中的行为是否符合规定，防止用户隐私数据被过度收集、使用或传播。可通过测试用例模拟数据共享场景，观察智能合约是否正确执行了数据共享的规则。

5.5 环境安全

5.5.1 部署安全

5.5.1.1 测评单元（01）

该测评单元包括以下要求：
a) 测评指标：在智能合约部署前，应对合约代码进行彻底的静态安全分析与测试，利用专业的智能合约安全分析工具扫描代码中的潜在漏洞，如整数溢出、重入攻击、随机数生成漏洞等，并对发现的问题进行修复。同时，对合约的依赖项进行严格审查，确保所依赖的库、框架等组件不存在已知安全漏洞，避免因第三方组件问题引入安全隐患。
b) 测评对象：智能合约代码、静态分析工具报告、依赖项清单。
c) 测评实施：
   1) 应核查是否使用专业的静态安全分析工具对智能合约代码进行了全面扫描，确保能够发现潜在的漏洞，如整数溢出、重入攻击、随机数生成漏洞等。可通过核查静态分析工具生成的报告，查看其是否详细列出了发现的问题，并核查是否对这些问题进行了及时修复。
   2) 应测试智能合约的依赖项是否经过严格核查，确保所使用的库、框架等组件不存在已知的安全漏洞。

5.5.1.2 测评单元（02）

该测评单元包括以下要求：
a) 测评指标：智能合约的部署过程应遵循安全的部署流程，在安全的部署环境中进行操作，如使用安全的编译工具、部署节点等，防止在部署过程中合约代码被篡改或遭受中间人攻击。

b） 测评对象：部署流程文档、编译工具、部署节点环境配置。

c） 测评实施：

1) 应核查智能合约的部署流程是否遵循了安全规范，确保在安全的部署环境中进行操作。可通过核查部署流程文档，查看其是否详细规定了使用安全的编译工具和部署节点等要求。

2) 应测试编译工具和部署节点环境的安全性，确保其不被篡改或不存在安全风险。

5.5.1.3 测评单元（03）

该测评单元包括以下要求：

a） 测评指标：智能合约部署完成后，对合约的部署状态进行验证，确保合约已正确部署且初始配置符合安全要求。

b） 测评对象：智能合约部署状态、初始配置参数。

c） 测评实施：

1) 应核查智能合约的部署状态是否正确，确保合约能够正常运行。可通过调用合约的基本功能进行测试，验证其是否按预期执行。

2) 应测试智能合约的初始配置是否符合安全要求，包括权限设置、默认参数等。

5.5.2 运行环境安全

5.5.2.1 测评单元（01）

该测评单元包括以下要求：

a） 测评指标：区块链平台应为智能合约提供安全可靠的运行环境，包括但不限于安全的虚拟机、稳定的共识机制、有效的网络通信安全防护等，虚拟机应具备良好的隔离性与安全性，防止不同合约之间相互干扰或恶意攻击，确保每个合约在独立、安全的沙箱环境中运行。

b） 测评对象：区块链平台的虚拟机、共识机制、网络通信安全防护机制。

c） 测评实施：

1) 应核查区块链平台的虚拟机是否具备良好的隔离性与安全性，确保不同合约之间不会相互干扰或遭受恶意攻击。可通过核查虚拟机的设计文档和安全测试报告，查看其是否实现了合约间的有效隔离，并评估其安全性。

2) 应核查区块链平台的网络通信安全防护机制是否有效，防止外部攻击和数据泄露。可通过核查网络通信协议和安全防护措施，查看其是否采用了加密传输、身份认证等技术手段。

3) 应测试区块链平台的共识机制是否稳定，确保智能合约的执行结果能够可靠地达成一致。可通过分析共识机制的实现和运行数据，评估其稳定性和抗攻击能力。

5.5.2.2 测评单元（02）

该测评单元包括以下要求：

a） 测评指标：应定期对区块链平台的运行环境进行安全更新与维护，及时修补系统漏洞，提升运行环境的整体安全性。

b） 测评对象：区块链平台的安全更新日志、漏洞管理记录。

c） 测评实施：

1) 应核查区块链平台是否定期进行安全更新与维护，确保系统漏洞能够及时得到修补。可通过核查安全更新日志和漏洞管理记录，查看其是否定期发布和应用了安全更新。

2) 应测试安全更新与维护的实际效果，确保其能够有效提升运行环境的整体安全性。

5.5.2.3 测评单元（03）

该测评单元包括以下要求：

a） 测评指标：应对智能合约的运行状态进行实时监控与审计，及时发现并处理异常的合约行为，如异常的资源消耗、频繁的外部调用等，保障智能合约在安全、稳定的环境中持续运行。

b） 测评对象：智能合约监控系统、审计日志。

c） 测评实施：

1) 应核查是否建立了智能合约运行状态的实时监控系统，确保能够及时发现异常行为。可通过核查监控系统的配置和功能，查看其是否覆盖了关键的运行指标和异常行为模式。

2) 应测试审计日志的完整性和准确性，确保智能合约的所有关键操作都被记录下来，以便进行后续的分析和溯源。可通过核查审计日志的内容和格式，确认其是否详细记录了合约的运行状态和异常事件。

3) 应评估智能合约的运行状态监控与审计机制的有效性，确保其能够及时发现并处理异常行为。可通过模拟异常场景，观察监控系统是否能够及时发出警报。

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）