附件 2
ICS 35.240.40
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0214—2021

金融网络安全 网络安全众测实施指南

Financial cyber security Guidelines of implementation for crowdsourced cyber security testing

2021－02－10 发布　　2021－02－10 实施

中国人民银行　　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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国人民银行提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国人民银行科技司、中国工商银行股份有限公司、工银科技有限公司、北京中金安服科技有限公司、中国银行股份有限公司、中国农业银行股份有限公司、中国建设银行股份有限公司、中国民生银行股份有限公司、兴业银行股份有限公司、恒丰银行股份有限公司、中央国债登记结算有限责任公司、华泰证券股份有限公司、海通证券股份有限公司、中国平安保险（集团）股份有限公司、中国太平洋保险（集团）股份有限公司、晋商银行股份有限公司、西安银行股份有限公司、江苏银行股份有限公司、北京长亭未来科技有限公司、百度时代网络技术（北京）有限公司、北京奇虎科技有限公司、上海艾芒信息科技有限公司、北京神州绿盟科技有限公司、奇安信科技集团股份有限公司、深信服科技股份有限公司、亚信科技（成都）有限公司、杭州安恒信息技术股份有限公司、北京启明星辰信息安全技术有限公司。

本文件主要起草人：李伟、陈立吾、沈筱彦、车珍、咎新、夏磊、王涛、敦宏程、苏建明、王贵智、蒋家堂、王晓、王金希、郭铮铮、秦磊、俞学浩、何启翱、李远祥、刘红波、宋克亚、詹丹丹、李乐天、翟海超、张爽、江旺、陆颂华、于惊涛、林利钦、张军、周扬、茹华、王楠、王心玉、马男、祁晓丹、何源源、凌墨缘、张屹、张帆、赵波、高继明、潘立亚、罗伟、俞斌、孙林。

引　言

本文件是在收集、分析评估金融机构实施网络安全众测流程以及面临的安全风险点的基础上，形成的一套网络安全众测实施流程指南，内容涉及网络安全众测组织实施架构、网络安全众测实施流程、网络安全众测实施流程中各参与方的职责。

本文件旨在规范金融机构网络安全众测的实施流程，指导金融机构在安全可控的前提下开展网络安全众测。

本文件可作为金融机构网络安全众测实施方法的依据。

金融网络安全 网络安全众测实施指南

1 范围

本文件提供了金融信息系统网络安全众测（以下简称安全众测）工作实施过程的指导，包括安全众测准备、实施、分析与报告编制。

本文件适用于开展安全众测工作的境内金融机构。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

金融信息系统 financial information system

金融行业相关的应用、服务、信息技术资产或其他信息处理组件。

[来源：GB/T 29246—2017，2.39]

3.2

网络安全众测 crowdsourced security testing

企业授权专业机构，召集多名安全测试人员，为企业提供漏洞发现服务，帮助其发现安全漏洞及安全隐患，并参照服务质量与效果，支付服务费用。

4 缩略语

下列缩略语适用于本文件。

OWASP：开放式Web应用程序安全项目（Open Web Application Security Project）

SQL：结构化查询语言（Structured Query Language）

5 众测通则

5.1 众测作用

在金融信息系统上线前或生产运行过程中，金融信息系统的运营或使用单位、主管或监管单位委托专业机构，对金融信息系统实施安全众测，发现并解决潜在的安全问题与隐患，并在此基础上，整改相关安全问题，以提升安全防护能力，满足业务的安全平稳运行。

5.2 重点关注的风险项

5.2.1 测试人员身份背景信赖度

实施安全众测的测试人员来自社会大众或不同的组织机构，对于参与测试的技术人员身份缺少可靠判断，信赖度偏低。

5.2.2 测试人员行为

传统的安全测试模式下，测试人员的行为不可见、不可控、不可审计、不可溯源，一旦在安全众测事中或事后发生安全事件，缺少对事件的定位和溯源条件。

5.2.3 系统运行

在安全众测时，需要模拟黑客对设备和系统进行一定的攻击测试工作，可能对系统的运行造成一定的影响，甚至会影响业务连续性，如OWASP排名前十的操作都具有一定的风险性。

5.2.4 敏感信息泄漏

众测实施过程中，有可能造成被测系统的业务数据或状态敏感信息泄露。如针对核心数据库的SQL注入等操作，造成如客户身份信息、客户账号信息、网络拓扑、IP地址、业务流程、安全漏洞信息、配置参数、运行日志、告警信息等的泄露。

5.3 实施主体和职责

5.3.1 众测需求方

众测需求方（以下简称需求方）：是发起安全众测、授权安全众测行为的组织，一般为金融机构。

5.3.2 众测组织方

众测组织方（以下简称组织方）：是在需求方的授权下，负责众测测试方的召集和管理，并提供测试报告的组织。

组织方宜具备如下条件：

a) 从事相关安全测试或检测评估工作两年以上，无违法记录。
b) 法定代表人及主要业务、技术人员无犯罪记录。
c) 具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度。
d) 对国家安全、社会秩序、公共利益不构成威胁。

组织方宜履行如下义务：

a) 遵守国家有关法律法规和技术标准，提供安全、客观、公正的安全众测服务，保证服务质量。
b) 保护在众测活动中知悉的国家秘密、商业秘密和个人隐私。
c) 保障测试人员的身份与背景可靠。
d) 对测试人员进行安全保密教育，与其签订安全保密责任书，规定履行的安全保密义务和承担的法律责任，并负责检查落实。

5.3.3 众测测试方

众测测试方（以下简称测试方）：是通过自身技术在需求方授权的前提下对测试目标进行安全测试，帮助需求方查找计算机系统或网络系统的漏洞的安全测试人员。

测试方宜具备如下条件：

a) 年满18周岁。
b) 无违法及犯罪记录。

测试方宜履行如下义务：

a) 遵守国家有关法律法规和技术标准、需求方和组织方的相关要求，在授权的范围内开展安全众测服务，提供准确、真实、客观的网络安全漏洞。
b) 保护在众测活动中知悉的国家秘密、商业秘密和个人隐私，履行安全保密义务和承担相应的法律责任。

5.3.4 众测审计方

众测审计方（以下简称审计方）：是根据需求方的要求，对安全众测过程进行管控、监控、审计和评价的组织。

审计方宜具备如下条件：

a) 从事相关安全测试审计或评估工作两年以上，无违法记录。
b) 法定代表人及主要业务、技术人员无犯罪记录。
c) 具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度。
d) 对国家安全、社会秩序、公共利益不构成威胁。
e) 审计方与组织方、测试方宜相互权限隔离。

审计方宜履行如下义务：

a) 遵守国家有关法律法规和技术标准，提供安全、客观、公正的安全众测审计服务，保证服务质量。
b) 保护在众测活动中知悉的国家秘密、商业秘密和个人隐私。
c) 履行安全保密义务和承担相应的法律责任。

5.4 实施过程

安全众测实施过程包括众测准备、众测实施和分析、报告编制三个过程。

6 众测准备

6.1 概述

众测准备工作是开展安全众测工作的前提和基础，是整个安全众测过程有效性的保证。众测准备工作是否充分直接关系到后续工作能否顺利开展。其主要任务是确定安全测试对象、时间范围、众测实施方案与安全管理方案，完成测试人员的召集和认证审核、准备安全管控平台等众测基础环境，为众测实施做好准备。

6.2 工作流程

众测准备的基本工作流程见图1。

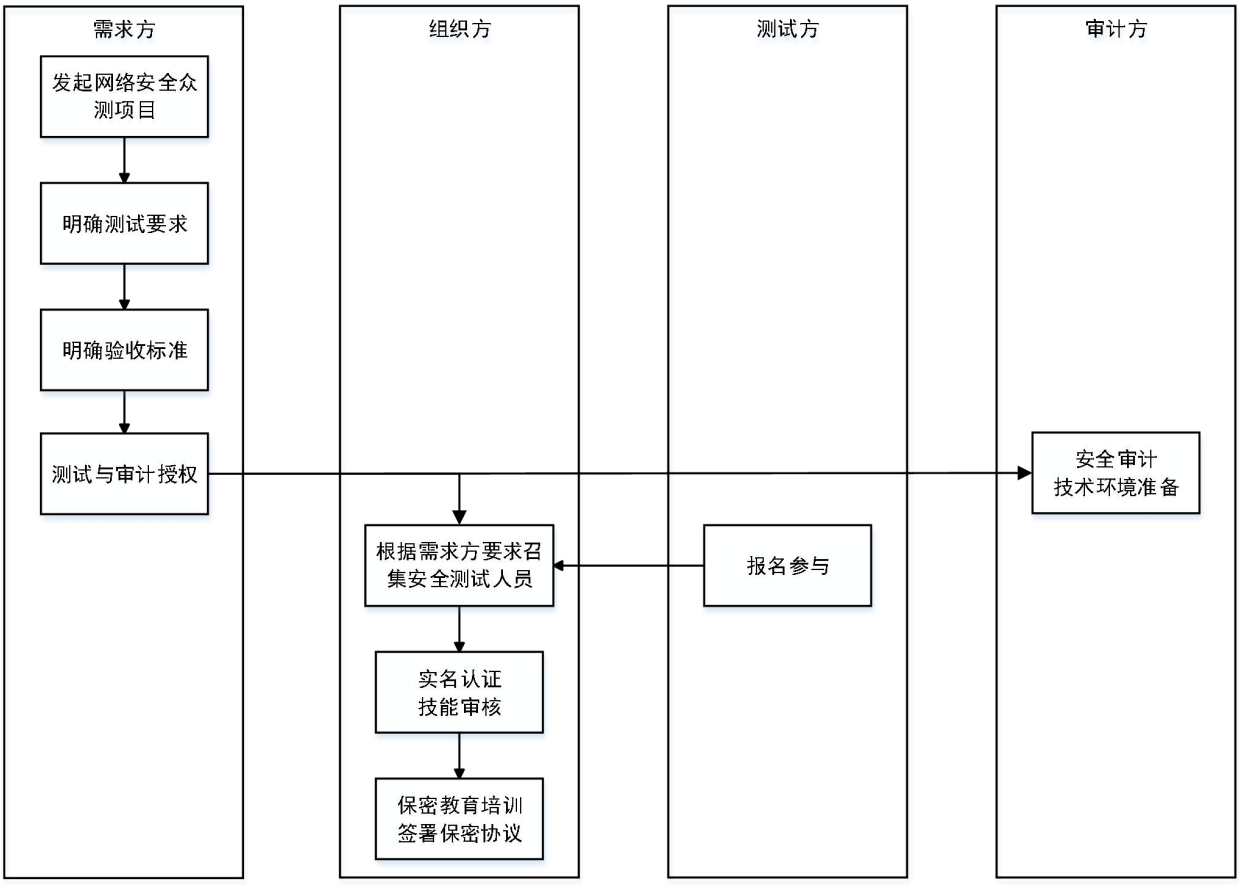

图 1　众测准备工作流程图

6.3　主要任务

6.3.1　项目启动

在项目启动任务中，需求方、组织方和审计方组建安全众测项目组，从基本资料、人员、计划安排等方面为安全众测项目的实施做基本准备。

输入：网络安全众测协议书（见附录A）。

任务描述：根据需求方与组织方和审计方签订的网络安全众测协议书，组织方和审计方组建众测项目组，从人员方面做好准备，并编制项目计划书。项目计划书可包含项目概述、工作依据、技术思路、工作内容和项目组织等。

输出/产品：项目计划书。

6.3.2　明确测试要求

在明确测试要求任务中，需求方向组织方和审计方明确测试对象、测试时间、测试人数限制、测试安全管控方式、测试人员行为准则（见附录B）等安全众测工作的具体测试要求。

输入：网络安全众测协议书。

任务描述：根据需求方与组织方和审计方签订的网络安全众测协议书，需求方向组织方和审计方明确测试对象、测试时间、测试人数限制、测试安全管控方式、测试人员行为准则、审计要求等安全众测工作的具体测试要求。

输出/产品：测试要求。

6.3.3 明确验收标准

在明确验收标准任务中，需求方向组织方和审计方明确项目验收标准、漏洞评级标准、奖励计算方式等安全众测工作的具体验收标准。

输入：网络安全众测协议书。

任务描述：根据需求方与组织方和审计方签订的网络安全众测协议书，需求方向组织方和审计方明确项目验收标准、漏洞评级标准（见附录C）、奖励计算方式等安全众测工作的具体验收标准。

输出/产品：验收标准。

6.3.4 测试和审计授权

在测试和审计授权任务中，需求方以书面的形式向组织方和审计方授权众测和众测审计。

输入：网络安全众测协议书。

任务描述：根据需求方与组织方和审计方签订的网络安全众测协议书，需求方向组织方和审计方以书面的形式向组织方和审计方授权众测和众测审计。

输出/产品：网络安全众测授权委托书（见附录D）。

6.3.5 测试人员组织

在测试人员组织任务中，组织方在需求方的授权和委托下，招募和组织安全测试人员，对安全测试人员进行实名认证和背景调查。

输入：网络安全众测授权委托书。

任务描述：根据需求方向组织方授予的网络安全众测授权委托书，组织方招募和组织安全测试人员，对安全测试人员进行实名认证和背景调查。

输出/产品：安全测试人员清单。

6.3.6 保密教育与保密协议

在保密教育与保密协议任务中，组织方根据需求方对于安全众测项目的要求，对测试人员进行安全保密宣传和教育培训工作，包括项目测试范围、项目测试时间、项目测试行为准则、安全保密要求等，与测试人员签署安全保密协议。

输入：网络安全众测授权委托书/安全测试人员清单。

任务描述：组织方根据需求方要求向测试人员进行安全保密宣传和教育培训工作，与测试人员签署安全保密协议。

输出/产品：培训记录，安全保密协议。

6.3.7 审计平台准备

在审计平台准备任务中，审计方按照需求方对于安全众测项目的要求，准备管控与审计平台环境，以及测试方安全接入所需的账号口令等信息。

输入：网络安全众测授权委托书。

任务描述：根据需求方向审计方授予的网络安全众测授权委托书，审计方准备管控与审计平台环境，以及测试方安全接入所需的账号口令等信息。

输出/产品：审计平台及认证信息。

6.4 各实施主体职责

6.4.1 众测需求方

宜考虑以下工作：

a) 成立众测项目管理团队，包括项目负责人、漏洞审核处理负责人、安全监测负责人。
b) 与组织方、审计方签订网络安全众测授权委托书及安全保密协议。
c) 明确测试对象、测试时间、测试人员数量、测试人员行为准则、漏洞评级标准、漏洞发现奖励方式与标准等众测项目实施参数。
d) 建立测试过程中安全监控机制及突发事件应急预案，协调各部门人员做好测试期间的安全监控和应急响应。
e) 组织开展项目启动会，宣讲项目实施方案，动员内外部做好测试准备工作和测试期间的安全保障工作。

6.4.2 众测组织方

宜考虑以下工作：

a) 成立项目实施小组和应急小组，明确项目负责人。
b) 与需求方签署网络安全众测授权委托书及安全保密协议。
c) 对需求方进行认证以及对测试对象进行所有权校验，确保需求方测试对象范围合法，所有权校验需包括但不限于 Web 应用服务、移动 APP。
d) 对测试方进行个人/企业实名认证，并签署安全保密协议。
e) 通过技能考核设置测试方的准入门槛，同时建立测试方的信誉体系及优胜劣汰机制，对不符合相关法律法规及不按需求方要求进行测试的测试方进行处罚及清退，确保身份可信、技能可行。
f) 对测试人员进行安全保密宣传和教育培训工作，包括项目测试范围、项目测试时间、测试行为准则、安全保密要求等，并签署测试协议和安全保密协议。
g) 协助需求方和审计方，完成测试管控平台的账号申请、接入认证账号发放、培训教育等工作。

6.4.3 众测测试方

宜考虑以下工作：

a) 认真学习项目的相关要求，包括项目测试范围、项目测试时间、项目测试行为准则、安全保密要求。
b) 与组织方签署测试协议和安全保密协议。
c) 配合组织方完成身份、技能认证。

6.4.4 众测审计方

宜考虑以下工作：

a) 成立项目实施小组和应急小组，确定项目负责人。
b) 制定安全审计计划，协调审计人员，进行测试前的项目启动会和宣传教育工作。
c) 负责众测审计使用的技术平台的准备工作，包括系统环境搭建、稳定性测试、安全性测试、安全接入账号的创建与配置等。

7 众测实施

7.1 概述

众测实施是开展安全众测工作的核心活动。其主要任务是按照安全众测方案的总体要求，开展安全众测活动，发现并及时提交系统存在的安全漏洞，并及时整改相关安全问题，以提升金融信息系统的安全防护能力，满足业务的安全平稳运行。

7.2 工作流程

众测实施的基本工作流程见图2。

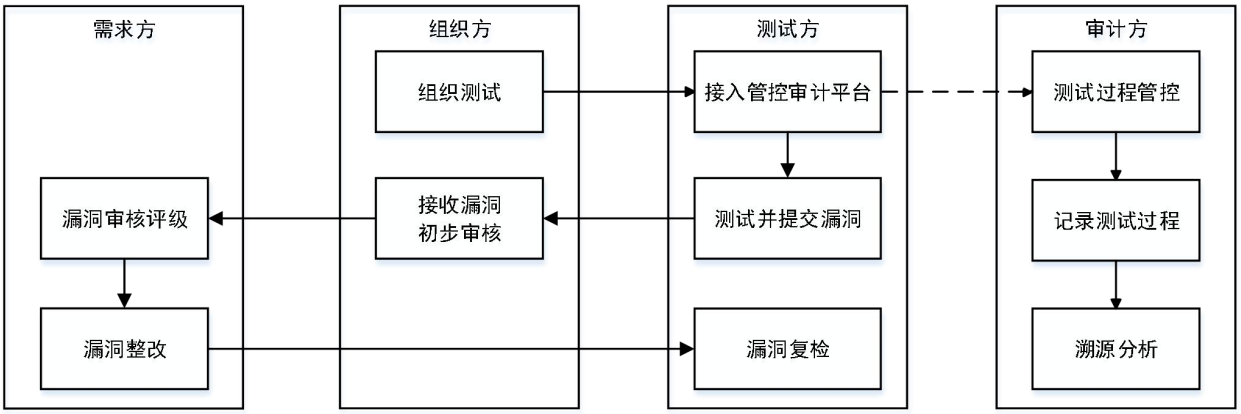

图 2 众测实施工作流程

7.3 主要任务

7.3.1 安全接入与管控

在安全接入与管控任务中，测试方按照需求方对于安全众测项目的要求，通过规定的安全接入渠道和方式进行安全众测，审计方记录测试人员的行为。

输入：审计平台及认证信息。

任务描述：利用审计方提供的审计平台和账号密码等认证信息，测试方可通过规定的安全接入渠道和方式进行安全众测，审计方记录测试人员的行为。

输出/产品：测试行为记录。

7.3.2 测试与漏洞提交

在测试与漏洞提交任务中，测试方按照需求方对于安全众测项目的要求，通过规定的安全接入渠道和方式进行安全众测，挖掘被测金融信息系统的潜在安全漏洞，并提交至组织方。

输入：网络安全众测授权委托书。

任务描述：测试方按照需求方对于安全众测项目的要求，通过规定的安全接入渠道和方式进行安全众测，挖掘被测金融信息系统的潜在安全漏洞，并提交至组织方。

输出/产品：待审核安全缺陷/安全漏洞。

7.3.3 漏洞审核评级

在漏洞审计评级任务中，组织方和需求方按照安全众测项目的要求，分别对测试方提交的待审核安全缺陷/安全漏洞进行漏洞审核定级，确定漏洞的有效性和危害级别。

输入：待审核安全缺陷/安全漏洞。

任务描述：组织方和需求方按照安全众测项目的要求，分别对测试方提交的待审核安全缺陷/安全漏洞进行漏洞审核定级，确定漏洞的有效性和危害级别。

输出/产品：已审核安全缺陷/安全漏洞。

7.3.4 漏洞修复与复检

在漏洞整改与复检任务中，需求方对众测过程中发现的有效安全缺陷/安全漏洞，安排相关人员进行漏洞修复，修复完成后，安排测试人员对漏洞修复情况进行验证。

输入：已审核安全缺陷/安全漏洞。

任务描述：在漏洞整改与复检任务中，需求方对众测过程中发现的有效安全缺陷/安全漏洞，安排相关人员进行漏洞修复，修复完成后，安排测试人员对漏洞修复情况进行验证，复检完成后送至需求方进行最终审核，直至彻底消除隐患。

输出/产品：安全缺陷/安全漏洞复检结果。

7.4 各实施主体职责

7.4.1 众测需求方

宜考虑以下工作：

a) 组织系统、网络、安全运维团队做好测试期间的系统、网络、安全的监控工作，发现重大安全攻击事件或系统服务中断等突发事件，及时启动相应的应急流程。
b) 做好众测过程突发事件的应急响应工作，包括事件报告、事件分析、事件处置、评估总结等工作。
c) 委派或委托平台指派项目负责人对项目进行实时跟踪，对提交的漏洞及时进行审核和确认，对发现的漏洞进行处理及应急响应，严格管理漏洞的生命周期。
d) 进行漏洞审核时，宜严格按照协议验收，评定漏洞风险。
e) 组织专项工作人员负责跟踪漏洞的处置修复，对于危害较高的漏洞，组织相关人员对漏洞进行快速整改修复，并协调漏洞复检工作。

7.4.2 众测组织方

宜考虑以下工作：

a) 负责项目实施阶段测试人员的协调、安全管理和项目漏洞的管理工作，包括组织具体测试工作、漏洞的审核处置、突发事件的应急响应和处置工作。
b) 提供有效可靠的沟通平台或工具，供组织方、需求方、测试方、审计方能够进行及时沟通。
c) 对需求方提供项目的管理权限。
d) 平台存储的漏洞信息，宜对漏洞信息进行加密存储，且宜仅对参与项目人员提供相应的权限。
e) 确保自身众测平台的安全性，防止因众测平台存在漏洞导致需求方的敏感数据被泄露。
f) 建立测试人员的信誉或积分体系，对不符合相关法律法规及不按需求方要求进行测试的测试方进行处罚及清退。对违反相关法律法规等损害需求方利益的行为，组织方有责任协助需求方及执法机关，对测试方的非法测试行为及其造成的后果进行取证。
g) 在服务过程中，当需求方和测试方对漏洞的判定不一致时，组织方承担纠纷处理职责。
h) 配合需求方和审计方完成众测安全管理和行为审计工作，突发事件时，应配合需求方和审计方完成事件的溯源和处置。

7.4.3 众测测试方

宜考虑以下工作：

a) 严格按照项目要求，在授权的时间范围内，对授权范围内的测试对象，遵守测试行为规范，使用授权范围内的测试方法开展测试工作，包括但不限于：
   1) 未经许可不允许超出项目测试范围对内部网络使用扫描器等自动化工具。
   2) 未经许可不允许使用高并发测试手段及工具。
   3) 未经许可不允许上传具有远程控制功能的恶意程序。
   4) 未经许可不允许私自进入内网越界访问/篡改数据信息。
   5) 未经许可不允许进行高风险操作，包括但不仅限于服务器提权操作等。
   6) 未经许可不允许对业务造成稳定性、可用性受损的操作行为。
   7) 未经许可不允许对交易数据、用户信息等敏感信息进行下载/拖取，收到流量审计系统对数据拖取行为的报警时应立即停止，并配合组织方和审计方等进行责任追溯。
   8) 发现的漏洞应立即上报，禁止私自隐藏漏洞。
b) 测试方实施有可能导致系统机密性、完整性、可用性受到重大影响的操作时，向组织方和需求方报备，在征得需求方的同意后再进行此类操作。
c) 严格按照项目的保密要求，对渗透测试中可能获取的少量网络拓扑信息、应用代码、数据、漏洞等应严格保密，不得用于其他途径，并在项目验收后及时删除。
d) 提交真实且描述清晰的漏洞信息。

7.4.4 众测审计方

宜考虑以下工作：

a) 配合组织方和需求方对测试方未授权行为进行审计，审计方保存原始流量日志以满足追溯要求。
b) 负责众测安全接入和管控系统的运行维护工作，保证系统的稳定平稳运行。
c) 负责解决测试人员在测试过程中遇到众测安全接入和管控系统相关的问题。
d) 记录测试人员访问信息，包括众测环境系统/账号的登录、登出等关键时间，以及众测项目测试时对众测系统所做的行为，包括用户 ID、时间、事件类型、操作的资源、操作的结果、访问发起端的地址或标识。
e) 审计方的审计系统向需求方开放，即需求方有权对测试人员的行为进行实时审计、检查。
f) 负责测试过程中测试人员的安全监控工作，发现异常及时通知需求方和组织方。
g) 负责测试过程中，测试人员安全接入账号的管理工作，包括账号暂停、账号恢复、项目暂停、项目恢复等。
h) 发生突发事件时，协助需求方进行突发事件的溯源分析和应急响应工作。

8 分析与报告编制

8.1 概述

分析与报告编制是给出安全众测工作结果的活动，是安全众测工作的综合评价活动。其主要任务是根据安全众测和众测审计结果，提交测试报告和审计报告，分析安全众测工作的质量和效果以及安全众测过程中测试人员行为的合规性。

8.2 工作流程

分析与报告编制的基本工作流程见图3。

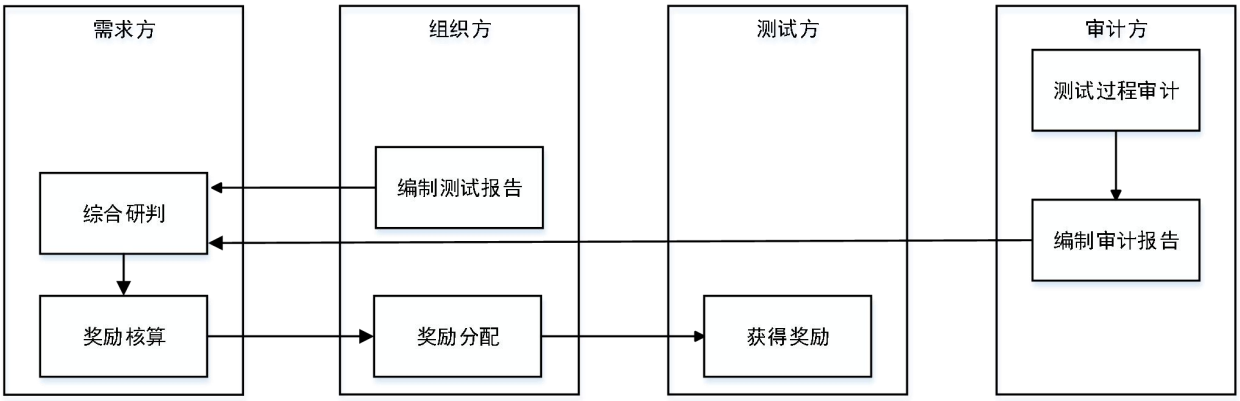

图 3　分析与报告编制工作流程

8.3　主要任务

8.3.1　众测审计

在众测审计任务中，审计方根据测试过程中记录的测试流量等，对测试方的测试行为和流量进行审计。

输入：测试行为记录。

任务描述：

a)　审计方根据测试过程中记录的测试流量日志等，对测试方的测试行为和流量进行审计。

b)　审计结果建议以审计报告的形式交付给需求方说明安全测试审计情况，需求方获取审计报告之后，根据审计结果，对组织方提出改进建议，组织方积极采纳改进建议并对相关组织和管理工作进行管理加强和技术提高。

c)　安全审计报告的内容包括但不限于测试范围、测试时间、测试人员、审计内容及审计结果等。

输出/产品：安全审计报告。

8.3.2　编制测试报告

在编制测试报告任务中，组织方根据众测过程中发现的有效的安全缺陷和安全漏洞，编制安全众测项目的测试报告。

输入：已审核安全缺陷/安全漏洞。

任务描述：组织方根据众测过程中发现的有效的安全缺陷和安全漏洞，编制安全众测项目测试报告。

输出/产品：测试报告。

8.3.3　综合研判

在综合研判任务中，需求方根据组织提交的测试报告、审计方提交的安全审计报告，依据项目前期确认的测试要求，检查测试方是否按照相关安全要求进行测试并提交漏洞，对安全众测项目进行综合研判。

输入：测试报告/安全审计报告/测试要求。

任务描述：需求方根据组织方提交的测试报告、审计方提交的安全审计报告，依据项目前期确认的测试要求，检查测试方是否按照相关安全要求进行测试并提交漏洞，对安全众测项目进行综合研判。

输出/产品：综合研判结果。

8.3.4　项目验收

在项目验收任务中，需求方根据项目前期确认的验收标准和交付物，组织项目验收工作。
输入：项目验收标准/项目交付物。
任务描述：需求方根据项目前期确认的验收标准和交付物，组织项目验收工作。
输出/产品：验收报告。

8.4 各实施主体职责

8.4.1 众测需求方

宜考虑以下工作：
a) 对审计方提供的审计报告进行分析总结和研判，识别违规行为和操作。
b) 根据组织方提供的测试报告和审计方提供的安全审计报告，对生产系统进行复检，检查测试留存的相关木马后门是否清理。
c) 根据项目前期确认的验收标准和交付物，组织项目验收工作。

8.4.2 众测组织方

宜考虑以下工作：
a) 以测试报告的形式交付测试成果。
b) 配合需求方完成项目验收工作。

8.4.3 众测测试方

宜考虑以下工作：
a) 协助组织方完成测试报告编制。
b) 清除上传的木马、后门、工具等，并将添加或修改的测试账号恢复原状。

8.4.4 众测审计方

宜考虑以下工作：
a) 对测试过程中留存的日志等记录进行审计。
b) 编写安全审计报告，安全审计报告的内容包括但不限于：
   1) 审计测试人员是否按照要求使用授权的测试接入途径进行安全测试。
   2) 审计整体的测试过程，量化测试人员测试工作量、测试目标范围。
   3) 审计测试人员使用的攻击手法。
c) 审计测试人员的高风险行为操作，溯源攻击过程。
d) 向需求方交付审计报告，说明安全测试审计情况，帮助需求方提升对测试方的管控能力。
e) 配合需求方完成项目验收工作。
f) 审计测试方是否清除测试过程中上传的木马、后门、工具等以及添加或修改的测试账号是否恢复。
g) 备份测试流量和行为等审计信息，建议保存 6 个月以上，以满足安全众测后期事件溯源的需要。

附 录 A
（资料性）
网络安全众测协议书

网络安全众测协议书宜包含相关方的权利和义务、信息安全、知识产权、保密条款等内容。具体如下：

a) 相关方的权利和义务宜包括但不仅限于以下内容：
   1) 需求方授权组织方及审计方开展安全众测工作，并授权组织方组织测试方进行测试的权利，授权审计方对测试方进行审计的权利。
   2) 需求方对需要测试、审计的服务范围内的域名/IP/系统拥有合法、正当、适当的权利或已获得必要的授权，需求方有权授权或委托组织方、测试方、审计方对服务范围内的域名/IP/系统进行测试、审计。
   3) 每次测试服务周期内，组织方对漏洞及漏洞评级结果进行初步确认，需求方对漏洞及漏洞评级结果进行最终确认，测试方对结果存在异议的，可以再次审核、评级，如未在约定期限内提出异议的，均视为对本次漏洞及漏洞评级结果的确认。
   4) 每次测试服务结束后，测试方协助组织方编写漏洞详情报告、组织方向需求方提供漏洞详情报告，审计方向需求方提供审计报告，漏洞详情报告、审计报告不合格的，需求方有权要求修订。
b) 信息安全宜包括但不仅限于以下内容：
   1) 为满足需求方实际需求，加强对需求方金融信息系统的安全保护，组织方、审计方接受需求方的委托和授权，按照法律规定、本协议书约定、需求方的指令对待测系统进行组织漏洞测试和审计。
   2) 组织方宜对测试方进行保密教育培训。
   3) 测试方不宜进行破坏性操作，如删除目标系统文件、修改和下载数据库数据、损坏引导扇区、主动扩散、感染文件、造成服务器宕机等操作，不宜使用具有破坏性和感染性的病毒、蠕虫和木马。
   4) 测试方按要求接收审计方审计，审计方如果发现异常，有权通知组织方，叫停测试的攻击行为。
c) 知识产权宜包括但不仅限于以下内容：
   1) 需求方、组织方、测试方、审计方均应保护其他方的知识产权，未经对方书面同意，任何一方不得将对方的资料及文件擅自修改、复制、向第三方转让或用于本协议书之外的其他目的。
   2) 需求方、组织方、测试方、审计方各自拥有本协议书生效前已经存在并合法拥有或控制的所有知识产权。
   3) 合作中产生的知识产权归属及使用，需求方、组织方、测试方、审计方宜通过具体合作协议补充规定。
d) 保密条款包括但不仅限于以下内容：
   1) 需求方、组织方、审计方、测试方对缔结和履行本协议书过程中获知的其他方的专有信息承担保密义务。未经书面许可，任何一方不得以明示或暗示的任何方式，或以任何媒体、宣传渠道包括但不限于官方网站、报纸、宣传材料、广播、电视、杂志等，发布与相关方的任何合作信息。合作信息包括但不限于各方的合作关系、合作领域、合作金额、当前合

作项目、客户信息，各方正在或即将进行某种磋商、缔结某种合作关系的可能性，或各方即将缔结、已缔结，或已终止某种合作关系的事实等。

2) 双方所承担的保密义务不因本协议书的无效、履行完毕、终止或解除而免除，保密期限为无限期的，直至相关信息实际已经合法公开为止。

附 录 B
（资料性）
测试方行为准则参考

安全测试人员参与众测项目需严格按照项目规则进行测试，遵守不影响正常线上业务、不泄露任何项目信息的准则开展测试。具体如下：

a) 提供本人真实有效的身份信息并配合组织方完成身份认证。
b) 未经测试需求方许可，不泄露任何项目相关的敏感信息。
c) 严格按照项目规定的测试时间，仅通过获得授权的安全接入方式，并仅针对获得明确授权的测试对象开展测试。
d) 经许可在众测实施过程中可实现非授权访问或用户权限越权，在完成非授权逻辑、越权逻辑验证时，不再批量获取和留存用户信息和金融信息系统文件信息。
e) 经许可在众测实施过程中可执行数据库查询条件，在获得数据库实例、库表名称等信息证明时，不再批量查询涉及个人信息、业务信息的详细数据。
f) 经许可在众测实施过程中可获得系统主机、设备高权限，在获得当前用户系统环境信息证明时，不再获取其他用户数据和业务数据信息。
g) 不利用当前主机或设备作为跳板，对测试对象以外区域进行扫描测试。
h) 应充分估计目标网络、系统的安全冗余，不进行有可能导致目标网络、主机、设备瘫痪的大流量、大规模扫描。
i) 未获得需求方的明确授权不执行可导致本地、远程拒绝服务危害的技术验证用例。
j) 不执行有可能导致整体业务逻辑扰动、有可能产生用户经济财产损失的技术验证用例。
k) 经许可可获得金融信息系统后台功能操作权限，在获得当前用户角色属性证明时，不再利用系统功能实施编辑、增删、篡改等操作。
l) 经许可可获得系统主机、设备、数据库高权限，在获得当前系统环境信息证明时，不再执行文件、程序、数据的编辑、增删、篡改等操作。
m) 经许可可在金融信息系统上传可解析、可执行文件，在获得解析和执行权限逻辑证明时，不驻留带有控制性目的程序、代码。
n) 及时提交真实完整的漏洞信息，不将同一漏洞拆分提交。
o) 未经需求方许可，不将发现的漏洞信息透漏给任何组织或个人。
p) 众测项目完成后，及时删除所获取、留存的项目相关敏感信息。

附 录 C
（资料性）
金融行业漏洞评级参考

漏洞评级标准宜参考国际组织OWASP漏洞标准来制定，同时根据金融行业实际主营业务和漏洞类型侧重点进行适当调整。

高危漏洞评级方法如下：

a) 直接获取系统权限（服务器端权限、客户端权限、数据库权限）的漏洞。包括但不限于：远程命令执行、任意代码执行、SQL 注入获取系统权限、缓冲区溢出等。

b) 越权访问和操作。包括但不限于：绕过认证直接访问管理后台可操作、核心业务非授权访问、核心业务后台弱密码，增删查改任意用户信息或状态等重要交互的越权行为等。

c) 重要业务的严重逻辑设计缺陷和流程缺陷，会影响客户账号安全或影响客户资金安全。包括但不限于：任意账号登录和密码修改、任意账号资金消费、任意金额订单支付等支付交易流程的漏洞等。

d) 可直接盗取金融行业关键系统及其用户私密数据、有大范围数据泄露影响的漏洞。包括重点页面的存储型跨站脚本攻击、客户重要敏感信息越权查询等。

e) 直接导致重要业务拒绝服务的漏洞。包括通过该远程拒绝服务漏洞直接导致线上应用、系统、服务器无法继续提供服务的漏洞。

中危漏洞评级方法如下：

a) 需交互方可影响用户的漏洞。包括但不限于：一般页面的存储型跨站脚本攻击、反射型跨站脚本攻击、重要操作跨站请求伪造攻击等。

b) 普通越权操作。包括但不限于：不正确的直接对象引用。

c) 普通信息泄漏。包括但不限于：客户端明文存储密码。

d) 普通的逻辑设计缺陷和流程缺陷。

低危漏洞评级方法如下：

a) 本地拒绝服务漏洞。包括但不限于：客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃），由安卓组件权限暴露、普通应用权限引起的问题等。

b) 轻微信息泄漏。包括但不限于：路径信息泄漏、异常信息泄露，以及客户端应用本地 SQL 注入（仅泄漏数据库名称、字段名、缓存内容）、日志打印、配置信息、异常信息等。

c) 难以利用但存在安全隐患的漏洞。包括但不限于：难以利用的 SQL 注入点、需构造部分参数且有一定影响的跨站请求伪造攻击等。

附 录 D
（资料性）
网络安全众测授权委托书

网络安全众测测试授权委托书样例见下表。

表 网络安全众测授权委托书示例

<table>
<tr><th colspan="4">网络安全众测授权委托书</th></tr>
<tr><td>授权方名称</td><td colspan="3"></td></tr>
<tr><td>联系人姓名</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>E-mail</td><td colspan="3"></td></tr>
<tr><td>被授权方名称</td><td colspan="3"></td></tr>
<tr><td>授权委托事项</td><td colspan="3">授权方委托被授权方在约定时间内按照测试评估方法对服务范围里的系统进行网络安全众测服务</td></tr>
<tr><td>服务时间</td><td colspan="3">年 月 日 -- 年 月 日
每天的测试时间段___:00-__:00</td></tr>
<tr><td colspan="4">服务范围（域名/IP/系统）：</td></tr>
<tr><td colspan="4">测试评估方法：
被授权方测试评估方法遵循业界通用标准，包括但不限于：口令穷举，身份验证突破，策略配置漏洞，Web 应用漏洞利用，访问控制突破，系统用户提权，内外网混联检测，溢出漏洞攻击等。</td></tr>
<tr><td colspan="4">授权方声明：
授权方认可被授权方提供的测试评估方法，知晓并接受测试评估可能带来的后果（如系统负载上升，数据库异常等），并提前做好必要的备份和风险应对措施准备。对因测试评估而导致的意外事件，双方将协商共同配合解决。</td></tr>
<tr><td colspan="4">注：1.授权方在本授权委托书中填写的联系信息需与授权方实际被测试系统上公布的联系信息一致，若相关联系信息发生变更应及时通知被授权方。
2.本授权委托书中授权方名称需要与公章和被测试系统上公布的单位名称一致。

授权方（公章）：
法定代表人/授权代表：
时间： 年 月 日</td></tr>
</table>

参 考 文 献

[1] GB/T 29246 信息技术 安全技术 信息安全管理体系 概述和词汇
[2] GB/T 15532—2008 计算机软件测试规范
[3] GB/T 28458—2012 信息安全技术 安全漏洞标识与描述规范
[4] GB/T 30276—2013 信息安全技术 信息安全漏洞管理规范
[5] GB/T 30279—2013 信息安全技术 安全漏洞等级划分指南
[6] GB/T 32421—2015 软件工程 软件评审与审核
[7] GB/T 33561—2017 信息安全技术 安全漏洞分类
[8] JR/T 0101—2013 银行业软件测试文档规范
[9] JR/T 0171—2020 个人金融信息保护技术规范