

标准研究

2023 年第 9 期（总第 31 期）

证标委秘书处

2023 年 11 月 21 日

《证券期货业信息系统渗透测试指南》行业标准的研制和探析

【摘要】 证券期货业信息系统的安全性与资本市场平稳运行息息相关，《证券期货业信息系统渗透测试指南》的推广应用解决了行业机构渗透测试流程规范性的问题，有效增强行业机构风险防范能力，助力资本市场平稳运行。

关键词：渗透测试 标准研制 应用价值

2023年2月7日,《证券期货业信息系统渗透测试指南》(JR/T 0276—2023)(以下简称为《指南》)金融行业标准经证监会批准发布。《指南》的制定与实施,提高了行业机构开展渗透测试的规范性和稳定性,强化了信息系统安全运行保障,有效提高证券期货行业网络安全防护能力,为资本市场的平稳运行提供助力。

一、 研制背景

证券期货业信息系统涉及证券账户、资金账户、交易记录等多种敏感信息,其安全性与资本市场平稳运行息息相关。而部分证券期货机构尚未建立健全的制度要求,无法规范化开展渗透测试工作;渗透测试执行方式缺乏对证券期货行业的针对性,导致系统安全性缺乏保障,市场风险防控难度较高。

上交所技术有限责任公司牵头相关机构制定《指南》,提供了规范化的框架参考,明确渗透测试流程和实施原则,解决行业机构开展渗透测试不规范的问题;根据证券期货业信息系统有别于其他行业的共性,提出通用方案,解决了缺乏行业针对性的问题。

二、 主要内容

《指南》主要适用于证券期货业机构开展渗透测试,适用主体包括证券期货交易所、证券期货公司。《指南》在规范证券期货业信息系统建设过程中规范开展渗透测试

整体流程的同时，分析行业信息系统区别于其他行业的相同属性，以适应证券期货行业信息系统安全性更高的需求。在标准制定过程中对流程合理性、保障测试质量、把控风险管理等多个方面进行了深入研究；标准制定过程中参考、查阅多项国家标准及行业标准，对于现有标准中已存在的要求和定义，采用直接引用的方式，保证本指南与现行标准的一致性，避免相关标准修订对本指南带来的影响。

《指南》遵循完整性、兼容性和可扩展性的原则，通过综合分析证券期货行业业务的共性特点以及证券和期货的差异项的点，结合国内证券期货行业业务现状制定。内容涵盖需求明确、方案制定、渗透测试执行、结果交付、风险管理等环节，对渗透测试流程中各个环节的执行过程进行统一规范，最大限度做到完整、准确的定义和描述。

三、推广应用价值

《证券期货业信息系统渗透测试指南》推广应用的主要价值与成效体现在以下几个方面：

一是规范化证券期货市场开展渗透测试。《指南》明确了证券期货机构信息系统建设如何规范开展渗透测试，弥补了原来证券期货行业没有统一规范的空缺，从明确渗透测试需求、制定渗透测试方案、执行渗透测试、交付渗透测试结果、管理渗透测试风险等方面提出实施原则要求，推动证券期货行业规范、安全、稳定地开展渗透测试工作。

二是提高证券期货市场风险防控能力。证券期货行业不同机构均参考《指南》要求执行，有效强化了行业机构对信息系统的安全管理，有助于持续增强行业机构渗透测试能力，保障信息系统的安全性，提高了证券期货行业的风险防控能力。

三是助力资本市场平稳运行。资本市场的平稳运行和证券期货行业信息系统的安全性紧密相关，《指南》为行业机构的渗透测试提供指引和要求，稳中有进地提升行业安全防护建设的基本能力，有效保障了证券期货市场的安全、稳定运行。

（上交所技术有限责任公司网络安全部经理沙明、安全测试组组长李佶、安全测试工程师樊芳供稿）