

《证券期货业网络安全能力成熟度模型》

编制说明

《证券期货业网络安全能力成熟度模型》标准起草组

二〇二五年四月

一、背景及意义

1. 背景

随着证券期货业信息化建设的深入推进、云计算与大数据等技术的广泛应用，系统边界模糊、数据交互增多、数据集中化现象日趋凸显，随之而来的信息安全问题也日趋复杂。一方面，网络钓鱼、病毒木马等传统安全问题屡见不鲜；另一方面，数据泄露、勒索软件等新型安全问题层出不穷，这促使行业机构重新审视并深入思考网络安全问题。

同时，在证券期货业机构数字化转型过程中必须持续保障信息系统安全，这需要管理层从安全相关的人员、技术和过程管理等方面全盘考虑。因此，证券期货业亟需一套能够立足于信息技术安全能力建设全过程的高弹性、可扩展、可度量的信息技术安全能力评估标准，识别当前信息技术安全能力建设的薄弱环节，指导网络安全防护能力建设。

2. 目的和意义

根据已有安全建设成果，基于 CMM 的质量控制思想，参考 WPDRRC 信息系统安全保障体系建设模型、ATT&CK 安全技术战术知识库框架、ASA2.0 自适应安全框架，结合证券期货业信息安全管理最佳实践，研究设计一套可落地的证券期货业网络安全能力成熟度模型，为机构提供一个便利的自我评价工具，指导数字时代的网络安全能力建设。

二、工作简况

1. 任务来源

文件起草单位：郑州商品交易所、上海证券交易所、深圳证券交易所、中证信息技术服务有限责任公司、中信建投证券股份有限公司、国金证券股份有限公司、北京长亭科技有限公司、国泰君安期货有限公司、华安基金管理有限公司。

文件主要起草人信息及主要工作职责具体如下：

序号	姓名	单位	主要工作内容/职责
1	刘相富	郑商所	作为主笔人参与标准起草关键问题决策，统筹标准编制工作。
2	王世福	郑商所	作为课题组联络员，参与标准的撰写、审核、进展督导和协调，统筹标准编制整体进度，负责撰写标准第 5 章“证券期货业信息技术安全能力成熟度模型”。

3	张倜	郑商所	参与标准撰写，整体行文结构调整梳理及格式规范，负责撰写标准第1章-第4章。
4	沙明	上交所	参与标准撰写及评审，主要参与第6章“核心保护对象安全”章节中“事件响应能力”子章节的标准撰写。
5	刘昌瑞	深交所	参与标准撰写及评审，主要参与第6章“核心保护对象安全”章节中“诱捕溯源能力”子章节的标准撰写。
6	崔世达	中证技术	参与标准撰写及评审，主要参与第6章“核心保护对象安全”章节中“事件检测能力”子章节的标准撰写。
7	朱成	中信建投证券	参与标准撰写及评审，主要参与第6章“核心保护对象安全”章节中“攻击预防能力”子章节的标准撰写。
8	李宜为	中信建投证券	参与标准撰写及评审，主要参与第6章“核心保护对象安全”章节中“攻击预防能力”子章节的标准撰写。
9	刘宏	国金证券	参与标准撰写及评审，主要参与第6章“核心保护对象安全”章节中“安全加固能力”子章节前7项能力的标准撰写。
10	马晓鹏	国金证券	参与标准撰写及评审，主要参与第6章“核心保护对象安全”章节中“安全加固能力”子章节前7项能力的标准撰写。
11	尹振玺	长亭科技	参与标准撰写及评审，主要参与第6章“核心保护对象安全”章节中“安全加固能力”子章节后6项能力、“人员管理能力”子章节的标准撰写。
12	饶建俊	国泰君安期货	参与标准撰写及评审，主要参与第6章“核心保护对象安全”章节中“关联分析能力”子章节的标准撰写。
13	蔡炯	华安基金	参与标准撰写及评审，主要参与第6章“核心保护对象安全”章节中“安全运营能力”子章节的标准撰写。

文件起草依据和来源：证券期货机构日常网络安全能力建设中的痛点问题，以及总结的安全能力建设最佳实践经验。

2. 主要工作过程

（一）项目启动

证券期货业作为信息化程度较高的行业，对信息系统可靠性有极高的要求，核心系统仅支持通过专线访问，互联网暴露面较少。基于证券期货业网络安全建设特点，传统网络安全评估服务难以真实有效的发现安全建设的薄弱环节，在此基础上进行的安全投入收效甚微。为了能够有效评估网络安全能力建设水平，“对症下药”，有针对性地增强核心安全能力，保证安全投入的有效性和持续性，郑商所调研了多家行业机构（中信建投、国金证券等），经过充分调研和必要性论证后，于2024年4月18日向证标委秘书处报送了《证券期货业网络安全能力成熟度模型》标准立项申请材料。

（二）标准立项下达

2024 年 7 月 18 日，证标委秘书处下发了《证券期货业网络安全能力成熟度模型》金融行业标准立项计划的通知，文号：证标委秘发〔2024〕113 号，项目计划编号：P2024003，项目正式进入草案编制阶段。

（三）成立标准起草工作组

2024 年 8 月，郑商所牵头成立《证券期货业网络安全能力成熟度模型》标准起草工作组，成员单位包括郑商所、上交所、深交所、中证技术、中信建投证券、国金证券、长亭科技、国泰君安期货、华安基金等，覆盖了行业会管单位、证券、期货、基金等各类型机构，具有广泛性和代表性。

（四）形成征求意见稿

起草工作组经过 8 个月的工作，期间在起草工作组成员单位内部广泛征求意见，并于 2025 年 4 月 22 日由中证技术行业信息安全联合实验召开标准草案讨论会，对标准草案提出了修订意见，起草工作组根据相关意见对标准草案进行了完善，形成标准草案征求意见稿并提交秘书处审核，后续将根据反馈意见继续完善标准草案。

三、编制主要内容

1. 证券期货业网络安全能力成熟度模型构建

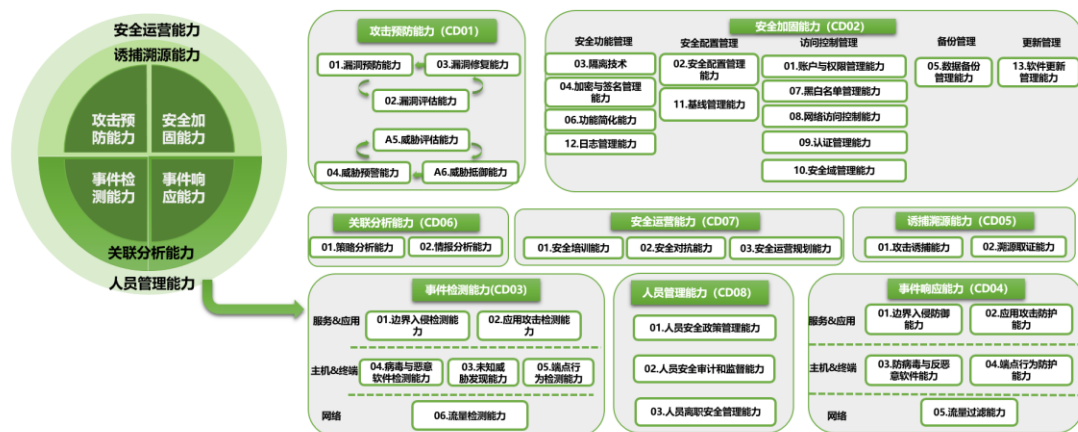


图 1：证券期货业网络安全能力成熟度模型

《证券期货业网络安全能力成熟度模型》（如图 1 所示）参考 CMM 的能力成

熟度设计，彻底从业务侧解耦合并进行接口化设计，使能力单元和流程的扩展、删除变得更加便利。该模型的主要部件由 8 个基本能力域和 40 个能力子域构成，明确行业机构网络安全生命周期安全管控的八个方面，具体包括攻击预防、安全加固、事件检测、事件响应、诱捕溯源、关联分析、安全运营、人员管理八个方面。

主要工作包括：

- 1) 能力成熟度等级划分指引，各能力成熟度等级特征说明；
- 2) 证券期货业网络安全能力成熟度模型架构说明；
- 3) 安全能力维度、安全过程维度的细则说明；
- 4) 标准相关能力项、标准编码规则、评分规则说明。

2. 核心保护对象安全评估细则

主要工作包括：详细阐述证券期货业网络安全能力成熟度模型相关的八个维度，即攻击预防能力、安全预防与加固能力、事件检测能力、事件响应能力、诱捕溯源能力、关联分析能力、安全运营能力、人员管理能力等 8 个能力域，并针对每个能力子域从人员配置、职责、技能意识层面和机制/流程、执行策略建设层面详细说明所需达到的具体目标。

四、主要试验（或验证）分析

证券期货业网络安全能力成熟度模型基于最新的防护理念，参考 WPDRRC、ATT&CK、自适应安全框架（ASA2.0）以及能力成熟度（CMM）等标准模型，引入并扩展最新的防御和安全保障技术，用于全面量化评估证券期货机构网络安全能力成熟度，提升组织应对各类新型威胁的能力，强化行业机构整体安全建设水平。

该模型在课题调研阶段已在郑商所、中信建投、国金证券等行业机构进行实验验证，并取得良好的业务反馈。主要验证过程包括开展深入的调研访谈，通过与机构信息安全负责人、漏洞安全运营人员、应急响应人员、基础 IT 运营人员、安全管理人员的调研访谈，了解机构的整体情况、组织架构、基础的安全工作情况、IT 信息化背景、日常漏洞扫描\测试\修复推送情况、各类防御类设备的监控\部署\策略\关联分析情况、机构网络安全域\访问控制规则\日志补丁情况、机构安全培训及体系相关人员制度落地情况，结合机构现状给出针对性的安全建设加固建议，为三家机构安全能力建设提供了有力支撑。

通过推广和落实证券期货业网络安全能力成熟度模型草案编写，预计可以显著提升行业机构在网络安全建设效果，避免重复投入，保障行业机构高质量推进数字化转型工作，实现网络安全防护能力的快速提升。

五、与有关的现行法律、法规和国家标准的关系

下列文件中的内容通过规范性引用，构成标准草案必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本标准；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 25069-2010 信息安全技术 术语

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

JR/T 0171-2020 个人金融信息保护技术规范

六、重大分歧意见的处理经过和依据

在遇到重大分歧意见时，我们建议通过起草工作组联合业界专家进行讨论交流，通过充分论证实现分歧消解，同时依据业界通常做法进行问题拆解，各个验证，形成可解释、可证明、可实施的能力评估方案。

七、贯彻标准的要求和建议措施

我们建议标准在早期实施阶段，尽可能多地走访证券期货业相关机构单位，推广和宣贯网络安全能力成熟度模型。组织形式可以是草案编制单位牵头，也可以是证标委的行业专家牵头。技术方面，依托牵头和参与单位现有系统进行技术展示和引导，展示标准的优势和效益，引导更多机构通过参与实验，进而过渡到正式采用的稳步推进步骤。

八、标准属性的建议

鉴于本标准的内容未涉及强制性标准或强制性条文的内容及要求，因此建议本标准作为推荐性行业标准。

九、废止有关现行标准的建议

本文件为首次编制，不存在对现行标准的废止问题。

十、其它说明事项

无。