团体标准《电子银行安全评估过程实施指南》编制说明

一、 工作简况

1.1 任务来源

《电子银行安全评估过程实施指南》由广东省网络空间安全协会归口管理。

1.2 主要起草单位和工作组成员

本标准由北京神州绿盟科技有限公司牵头，网安联认证中心有限公司、广州华南检验检测中心有限公司、广东新兴国家网络安全与信息化发展研究院、北京网络空间安全协会、广东关键信息基础设施保护中心、国源天顺科技产业集团有限公司、广东中证声像资料司法鉴定所、广州网络空间安全协会、揭阳网络空间安全协会等多家单位共同参与编制。

1.3 主要工作过程

（1）2024 年 3 月，标准正式立项，协会组织参与本标准编写的人员启动项目，成立规范编制小组，确立各自分工，对标准进行调研，听取各单位的相关意见；

（2）2024 年 4 月-7 月，编制组召开组内研讨会并结合充分的调研结果，参考各类国家标准和相关政策文件，形成标准草案第一稿；结合各参编单位的反馈意见，修改形成标准草案第二稿；

（3）2024 年 8-9 月，编制组召开组内研讨会，基于前期成果，

经多次内部讨论研究，组织完善草案内容，形成征求意见稿。

二、标准编制原则和标准编制详细说明及解决的主要问题

2.1 编制原则

本标准的研究与编制工作遵循以下原则：

（1）符合性原则

本标准使用时能够与法律法规和国家强制性标准的要求保持一致，符合国家相关主管部门的要求。

（2）最小影响原则

本标准规范涉及技术评估工作应尽可能小的影响系统和应用的正常运行，不会对正在的运行和业务的正常提供产生显著影响。

（3）全面性原则

风险等级评定应在全面收集银行相关信息的基础上，综合全部信息进行，范围应覆盖《电子银行安全评估指引》所要求的 8 个方面。

2.2 文档结构

《电子银行安全评估过程实施指南》标准文档分为前言、范围、规范性引用文件、术语和定义、电子银行安全评估原则、电子银行安全评估概述、电子银行安全评估方法和电子银行安全评价程序、附录 A 电子银行安全评估报告模版和附录 B 电子银行安全评估内容等部分。

2.3 整体格式

整体格式根据 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》的相关要求，对本标准的各要素进行编

写和排版。

在标准内容汇总及整个各方意见过程中，对各编写组成员提交部分，根据 GB/T 1.1-2020 的编写要求进行了必要的增删改，以确保符合一致性、协调性、易用性等文件的表述原则及相关规定。

2.4 标准名称英文翻译

标准的名称“电子银行安全评估过程实施指南” 翻译为 Guidelines for Implementing the Security Assessment Process for Electronic Banking。

2.5 术语和定义

术语和定义中所列的术语的英文翻译，如有类似术语的标准，参考了其翻译，没有类似术语标准翻译的，通过百度翻译和谷歌翻译后进行对比，并参考网络相关翻译后进行确定。

2.6 电子银行安全评估原则

电子银行安全评估原则包括全面性、系统性、公正性、重要性、保密性、最小影响原则。

2.7 电子银行安全评估概述

本章主要阐述了电子银行安全评估的定义和说明。是指金融机构在开展电子银行业务过程中，对电子银行的安全策略、内控制度、风险管理、系统安全、客户保护等方面进行的安全测试和管控能力的考察与评价。

2.8 电子银行安全评估方法

本章主要介绍了电子银行评估是针对电子银行业务，采用相关的评估手段，获取相关的证据数据，给出评估结论。主要通过安全策略评估、管理问卷评估、安全顾问访谈、网络架构分析、人工安全检查、安全漏洞扫描、渗透测试和安全配置核查的方法实现。

2.9 电子银行安全评估程序

本章主要介绍了电子银行安全评估风险等级、电子银行安全评估标准和电子银行安全评估评价程序。描述了风险等级的划分标准，电子银行8个检查方面与具体检查项细化的评价标准和评分的计算逻辑和评级等级划分。

2.10 附录 A 电子银行安全评估报告

本附录主要介绍了《电子银行安全评估报告》输出的模版格式要求和内容概述。

2.11 附录 B 电子银行安全评估内容详情

本附录主要介绍了所要求的8个检查方面与具体检查项，包括安全策略、内控制度建设、风险管理状况、系统安全性、电子银行业务连续性计划、电子银行业务运行应急计划、电子银行风险预警体系和其他重要安全环节和机制的管理的二级子类和指标项具体检查内容。

三、知识产权情况说明

本标准不涉及专利。

四、采用国际标准和国外先进标准情况

无采用国际标准和国外先进标准情况。

五、与现行相关法律、法规、规章及相关标准的协调性

建议本标准推荐性实施。本标准不触犯国家现行法律法规，不与其他强制性国标相冲突。

六、重大分歧意见的处理经过和依据

《电子银行安全评估过程实施指南》编制过程中未出现重大分歧。

七、标准性质的建议

建议《电子银行安全评估过程实施指南》作为推荐性团体标准发布实施。

八、贯彻标准的要求和措施建议

本标准是对商业银行电子银行业务作出评估规范要求标准。通过规范的评估，确保电子银行业务的安全性，提升整体信息安全水平。

九、替代或废止现行相关标准的建议

无替代或废止。

十、其他应予说明的事项

无。

《电子银行安全评估过程实施指南》
标准编制组
2024 年 9 月