



中华人民共和国国家标准

GB/T 20987—2007

信息安全技术 网上证券交易系统 信息安全保障评估准则

Information security technology—
Evaluation criteria for online securities trading system
information security assurance

2007-06-14 发布

2007-11-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 系统描述	1
4.1 网上证券交易系统概述	1
4.2 网上证券交易系统技术参考模型	2
4.3 网上证券交易系统描述	3
5 安全环境	9
5.1 假设	9
5.2 威胁	10
5.3 组织安全策略	13
6 安全保障目的	15
6.1 安全保障技术目标	15
6.2 安全保障管理目标	16
6.3 安全保障工程目标	17
7 安全保障要求	18
7.1 安全保障技术要求	18
7.2 安全保障管理要求	51
7.3 安全保障工程要求	61
附录 A (规范性附录) 网上证券系统信息安全保障符合性	72
A.1 安全保障目的符合性声明	72
A.2 安全保障要求符合性声明	72
参考文献	80
图 1 信息系统框架	1
图 2 信息系统技术参考模型	3
图 3 网上证券交易系统评估边界界定示意图	4
图 4 网上证券交易系统网络体系结构	7
图 5 行情查看流程图	9
表 1 网上证券交易系统用户和信息敏感程度描述	5
表 2 网上证券交易系统威胁模型	12
表 3 端到端安全保障技术要求中主体对客体采取的操作对照表举例	18
表 4 端到端安全保障技术要求中的网上信息流控制策略举例	19
表 5 端到端安全保障技术要求的可审计安全事件类型	23
表 6 端到端安全保障技术要求的可查阅审计记录	24

表 7	端到端安全保障技术要求中安全角色对系统安全功能行为的管理权限	25
表 8	端到端安全保障技术要求中授权人员对系统安全属性的管理权限表举例	26
表 9	本地计算安全保障技术要求中主体对客体采取的操作对照表举例	27
表 10	本地计算安全保障技术要求中的网上信息流控制策略举例	29
表 11	本地计算安全保障技术要求的可审计安全事件类型	34
表 12	本地计算安全保障技术要求的可查阅审计记录	36
表 13	本地计算安全保障技术要求中安全角色对系统安全功能行为的管理权限	37
表 14	本地计算安全保障技术要求中授权人员对系统安全属性的管理权限表举例	38
表 15	本地计算安全保障技术要求中系统安全角色对系统安全数据的操作权限举例	38
表 16	系统边界安全保障技术要求中主体对客体采取的操作对照表举例	40
表 17	系统边界安全保障技术要求的网上信息流控制策略举例	41
表 18	系统边界安全保障技术要求的可审计安全事件类型	43
表 19	系统边界安全保障技术要求的可查阅审计记录	45
表 20	系统边界安全保障技术要求中安全角色对系统安全功能行为的管理权限	46
表 21	支撑性基础设施安全保障技术要求的可审计安全事件类型	49
表 22	支撑性基础设施安全保障技术要求的可查阅审计记录	51
表 A.1	安全保障技术目标与威胁、策略的对应表	73
表 A.2	安全保障管理目标、安全保障工程目标和威胁、策略的对应表	75
表 A.3	安全保障技术目标和安全保障技术要求映射	77
表 A.4	安全保障管理目标和安全保障管理要求映射	79
表 A.5	安全保障工程目标和安全保障工程要求映射	79

前 言

本标准的附录 A 为规范性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：中国信息安全产品测评认证中心。

本标准主要起草人：吴世忠、王海生、陈晓桦、王贵驹、李守鹏、江常青、彭勇、张利、钱伟明、邹琪、李娟、李静、王庆、班晓芳、江典盛、陆丽、姚轶崧、孙成昊、门雪松、杜宇鸽、杨再山。

引 言

0.1 网上证券交易系统信息安全保障的含义

随着互联网技术在证券行业的应用,网上证券交易系统日益成熟。以网络为媒介进行证券交易可满足随时、随地进行快捷交易的需求。信息技术的进步促进了证券市场的发展;证券市场不断发展的需求,也促进了信息技术应用的发展。网络通讯能力的增强、网络安全技术的应用,使得证券公司与其他金融机构之间的业务合作越来越紧密。网上交易的飞速发展一方面突破了证券行业依靠传统营业部“划地为营”的地域性限制,扩大了潜在的用户市场,降低了交易服务成本,提高了服务质量;同时网上交易的出现使得证券公司的经纪业务不再仅仅凭借营业部数量的多少取胜,从规模、地理位置、装修等硬件方面的竞争向价格、服务、品牌等软件方面转化。与传统交易方式相比,网上交易具有安全性高、速度快、财经信息丰富、操作便捷等优势。

信息安全保障问题是网上证券交易系统建设和运行中必须解决的基础和根本性问题,它关系到客户与证券公司的切身利益。网上证券交易系统是一种特定的信息系统(即用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和),它的信息安全保障工作必须结合证券行业的特点,以风险和策略为出发点和核心,即从网上证券交易系统所面临的风险和所处的环境出发制定网上证券交易系统的安全保障策略,在网上证券交易系统的整个生命周期中从技术、工程、管理和人员等方面提出安全保障要求,确保信息的保密性、完整性和可用性特征,实现和贯彻组织机构策略并将风险降低到可接受的程度,达到保护证券公司的信息和信息系统资产,从而保障证券公司业务安全、可靠开展的最终目的。

网上证券交易系统信息安全保障涵盖以下几个方面:

- a) 网上证券交易系统信息安全保障应贯穿网上证券交易系统的整个生命周期,包括规划组织、开发采购、实施交付、运行维护和废弃五个阶段,以获得网上证券交易系统信息安全保障能力的持续性。
- b) 网上证券交易系统信息安全保障不仅涉及安全技术,还应综合考虑安全管理、安全工程和人员安全等,以全面保障网上证券交易系统安全。在安全技术上,不仅要考虑具体的产品和技术,更要考虑网上证券交易系统的安全技术体系架构;在安全管理上,不仅要考虑基本安全管理实践,更要结合组织的特点建立相应的安全保障管理体系,形成长效和持续改进的安全管理机制;在安全工程上,不仅要考虑网上证券交易系统建设的最终结果,更要结合系统工程的方法,注重工程过程各个阶段的规范化实施;在人员安全上,要考虑与网上证券交易系统相关的所有人员包括规划者、设计者、管理者、运营维护者、评估者、使用者等的安全意识以及安全专业技能和能力等。
- c) 网上证券交易系统信息安全保障是基于工程的保障。通过风险识别、风险分析、风险评估、风险控制等风险管理活动,降低网上证券交易系统的风险,从而实现网上证券交易系统信息安全保障。
- d) 网上证券交易系统信息安全保障的目的不仅是保护信息和资产的安全,更重要的是通过保障网上证券交易系统的安全,保障网上证券交易系统所支持的业务,从而达到实现组织机构使命的目的。
- e) 网上证券交易系统信息安全保障是主观和客观的结合。通过在技术、管理、工程和人员方面客观地评估安全保障措施,向网上证券交易系统的所有者提供其现有安全保障工作是否满足其

安全保障目的的信心。因此,它是一种通过客观证据向网上证券交易系统所有者提供主观信心的活动,是主观和客观综合评估的结果。

- f) 保障网上证券交易系统安全不仅是系统所有者自身的职责,而且需要社会各方参与,包括电信、电力、国家信息安全基础设施等提供的支撑。保障网上证券交易系统安全不仅要满足系统所有者自身的安全需求,而且要满足国家相关法律、政策的要求,包括为其他机构或个人提供保密、公共安全和国家安全等社会职责。

0.2 网上证券交易系统信息安全保障评估准则的编制目的和意义

GB/T 20274《信息安全技术 信息系统安全保障评估框架》是建设、评估信息系统安全保障的基础性和框架性标准,给出了对信息系统安全保障体系的通用要求。本标准是在 GB/T 20274 的基础之上,结合网上证券交易系统的具体特点,给出了网上证券交易系统的信息系统安全保障要求。

制定本标准的意义在于:

- a) 为网上证券交易系统信息安全保障的设计、实施、建设、测评、审核提供规范的、通用的描述语言;
- b) 有利于网上证券交易系统所有者编制其信息系统的安全保障要求;
- c) 有利于网上证券交易系统安全集成商和安全服务提供商提供更为科学规范化的设计和服务,促进信息安全市场的发展;
- d) 有利于有关行政管理部门、执法机构、测评认证机构对网上证券交易系统进行安全检查、检测、审计、评估和认证。

信息安全技术 网上证券交易系统 信息安全保障评估准则

1 范围

本标准规定了网上证券交易系统的描述、安全环境、安全保障目的、安全保障要求及网上证券系统信息安全保障目的和安全保障要求的符合性声明。

本标准适用于规范网上证券系统在交易过程中涉及信息安全的评估工作。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 20274(所有部分) 信息安全技术 信息系统安全保障评估框架

3 术语和定义

GB/T 20274 确立的以及下列术语和定义适用于本标准。

网上委托 entrust through Internet

证券公司通过互联网,向在本机构开户的投资者提供用于下达证券交易指令、获取成交结果的一种服务方式。

4 系统描述

4.1 网上证券交易系统概述

网上证券交易系统是一种具有特定使命、技术系统和组织结构的信息系统。信息系统是用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和。在本标准中,所使用的信息系统概述框架见图 1。

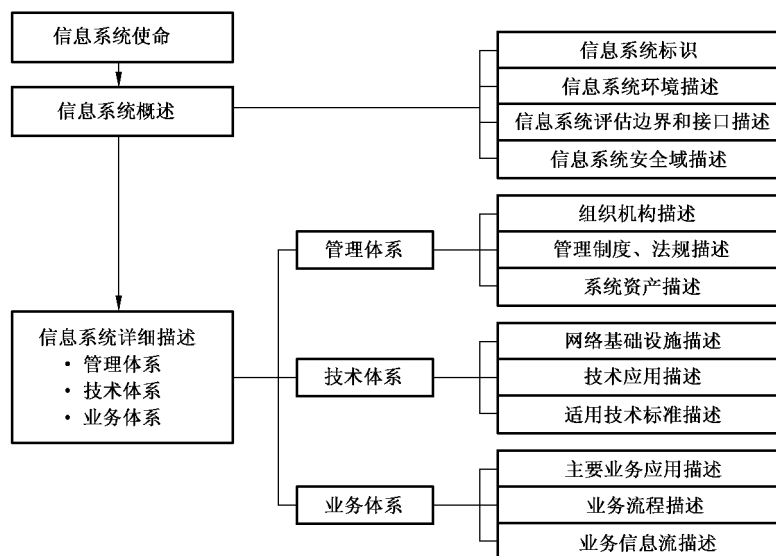


图 1 信息系统框架