ICS 35.040
L 80

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
中国国家标准化管理委员会　发布

目　次

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、王贯驷、李守鹏、江常青、彭勇、张利、钱伟明、邹琪、李娟、李静、王庆、斑晓芳、江典盛、陆丽、姚铁崭、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。

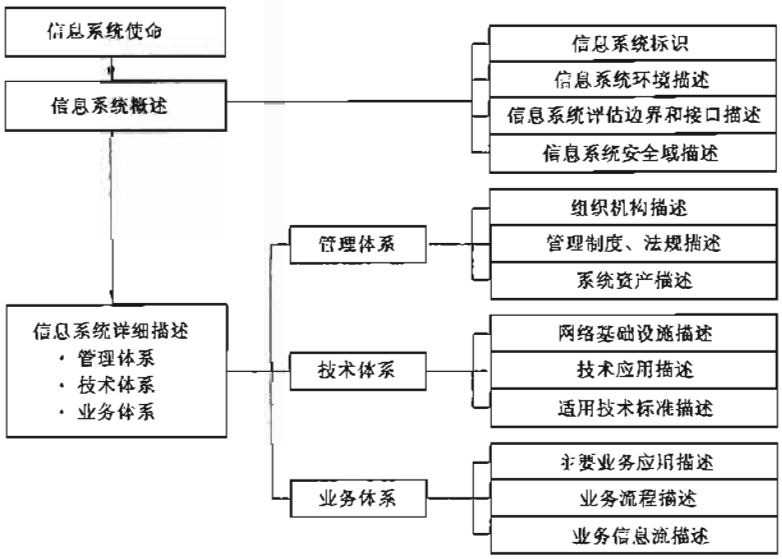

图 1　信息系统框架

整个信息系统描述主要包括三个大类：信息系统使命、信息系统概述和信息系统详细描述，相应的具体描述内容包括：

a) 信息系统使命：即从目的和意义方面对信息系统进行高层描述，它是信息系统根本和本质的要求。

b) 信息系统概述：对所要评估的信息系统进行概括性说明和描述。

1) 信息系统标识：应给出系统的正式名称和标识。系统标识包括其名称、所属的公司及其地点和包含最终用户及其地点等相关信息；

2) 信息系统环境描述：描述的运行环境以及系统开发、集成和维护的环境；

3) 信息系统评估边界和接口描述：描述所要评估系统的边界和相应的外部接口，此描述必须用图表或文字清晰地描述和界定所要评估的系统部件和边界；

4) 信息系统安全域描述：根据系统的关键性（描述系统的关键性以及系统可接受的风险级别）、数据的分类和密级（描述系统所处理的数据类型和机密级别）和系统用户（描述使用系统的用户描述）等方面划分系统的安全域。

c) 信息系统详细描述：此部分从管理体系、技术体系和业务体系三个方面分别对信息系统进行详细描述。

1) 管理体系：在管理体系中，需要对信息系统现有的管理组织结构、所使用的相应规章制度和所涉及的重要资产进行描述。

——组织机构描述：信息系统相关的管理、使用、开发、集成、支持组织机构的描述，特别是相关安全保障管理的组织机构的描述；

——管理制度、法规描述：列出同信息系统管理相关的目前使用的相应规章制度和相关法规；

——系统资产描述：信息系统的物理资产（指网上证券交易系统中的各种硬件、软件和物理设施）和信息资产（指在网上证券交易系统计划组织、开发采购、实施交付、运行维护和废弃这一网上证券交易系统生命周期过程中产生的同网上证券交易系统本身相关的有价值的信息以及网上证券交易系统所存储、处理和传输的各种相关的办公、管理和业务等信息）列表。

2) 技术体系：技术体系是信息系统描述的基础，需要对现有的各种应用、相应的网络基础设施和所使用的技术标准进行描述，这些描述将帮助了解用户的信息系统并为进一步描述业务系统提供基础和支持。

——网络基础设施描述：系统的网络层次等网络体系结构说明；

——技术应用描述：用户信息系统的各种应用说明；

——适用技术标准描述：列出相关技术应用等所适用的技术标准。

3) 业务体系：业务体系从业务角度和应用角度出发，基于技术体系，对组织机构的主要业务应用进行分类和描述，并通过业务流程和业务信息流来进一步解释。

——主要业务应用描述：列出组织机构的主要业务应用并进行描述；

——业务流程描述：基于组织机构的管理结构等，描述业务的流程；

——业务信息流描述：描述主要业务应用的接口和相应数据流，数据流描述应包括数据的类型以及数据传送的一般方式。

4.2 网上证券交易系统技术参考模型

为了更好地帮助理解和规范化网上证券交易系统描述，图2列出本规范所建议使用的信息系统技术参考模型。通过此技术参考模型的介绍，帮助用户能以一种更规范、结构化和标准化的方式描述信息技术系统。

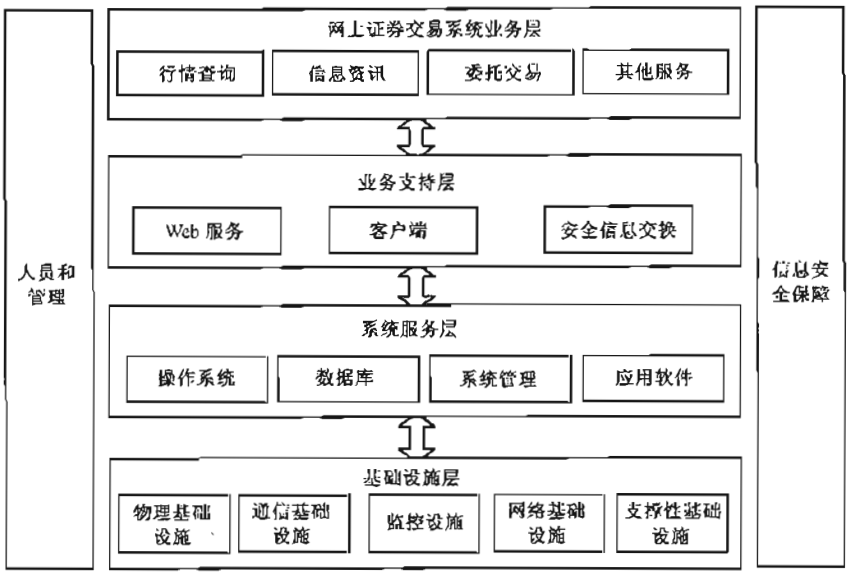

图 2　信息系统技术参考模型

信息系统技术参考模型提供了一个描述和理解信息技术系统的公共词汇表，并定义了信息技术系统通用的服务和接口集合。通过公共词汇表和服务、接口集合的定义，帮助用户以通用、标准化和提高互操作的方式建设、分析和描述信息技术系统。

信息系统技术参考模型主要涉及信息系统描述中的技术体系和业务体系。整个网上证券交易系统技术参考模型分为六个模块：基础设施层、系统服务层、业务支持层、业务应用层、信息安全保障、人员和管理，这六模块分别提供其特定的服务。

a) 基础设施层：向系统服务层提供所需的各种通用网络基础服务，如信息交换服务等；

b) 系统服务层：向业务支持层、业务应用层提供操作系统和数据库等支持；

c) 业务支持层：向业务应用层提供 Web 服务、客户端和安全交换等服务支持；

d) 业务应用层：提供行情查询、信息资讯、委托交易等应用服务技术；

e) 信息安全保障：在各个层面为网上证券交易提供机密性、完整性、可用性、鉴别、抗抵赖等安全服务。主要涉及安全管理、安全协议、加解密、签名与认证、密钥管理、安全测评、公钥基础设施等；

f) 人员和管理：为各个层面提供法律、法规、政策、标准、管理等支持。

4.3　网上证券交易系统描述

4.3.1　网上证券交易系统使命概述

证券公司建设网上证券交易系统，应依据国家相关标准，从具体情况出发，分析实际需求，确定系统所要实现的功能，明确系统与统一网络平台的接口，在保证安全的前提下促进系统的互联互通和系统资源的综合利用；分析系统运行中存在的威胁，从技术、管理、工程三方面实现安全保障。通过建立一个符合标准、功能完善、安全可靠的网上证券交易系统，安全、可靠、快捷的提供网上交易服务。

4.3.2　网上证券交易系统概述

网上证券交易系统概述，即对所要评估的信息系统进行概括性说明和描述。它主要包括：网上证券交易系统标识、网上证券交易系统环境描述、网上证券交易系统评估边界和接口描述以及网上证券交易系统安全域描述。

4.3.2.1　网上证券交易系统标识

网上证券交易系统应给出系统的正式名称和标识，在系统标识中应标明以下内容：

——名称：×××公司网上证券交易系统；

——所属公司；

——地点：×××公司。

4.3.2.2 网上证券交易系统环境描述

描述网上证券交易系统的运行环境以及系统开发、集成和维护的环境。在网上证券交易系统信息安全保障目的中网上证券交易系统的使用方应给出其所被评估的网上证券交易系统的详细环境描述。

4.3.2.3 信息系统评估边界和接口描述

信息系统评估边界和接口描述应根据所需评估的系统的实际情况，综合考虑安全域等原则进行边界划分，用图表和文字清晰地说明和界定所要评估的系统部件和边界。

图 3 中的例子用于概念化说明如何用图表对边界划分进行描述。此例为集中转发式网上交易系统实例，实际情况中可能主站点位于证券公司内部，仅作为参考。用户应在其信息安全保障目的文件中根据其所要评估信息系统的实际情况加以描述。

此例假设为某个网上证券交易系统的评估边界，其同外部系统的边界点和边界部件为：

——同公众网之间的逻辑隔离设备；

——评估边界为主站点、总部、下属营业部(可对营业部进行抽样)。主站点包括行情服务器、交易服务器等，总部包括转发前置机、安全隔离模块、转发后置机、营业部包括柜台前置机等；

——主站点是网上证券系统的对外联系"窗口"，主要负责实现接受用户的各类服务请求；接受、存储、发布行情信息；对用户的交易指令进行预处理，并转发给证券公司；

——位于总部的服务器通过广域网向营业部分发交易指令；接收交易所发送的卫星行情和资讯信息，并发送给托管机房服务器；监控、统计、分析各营业部的交易数据等；

——位于营业部的柜台前置机负责接收总部发送过来的交易数据；对交易数据进行加、解密；并将交易数据转换为柜台系统能够识别的格式发送给柜台系统处理。

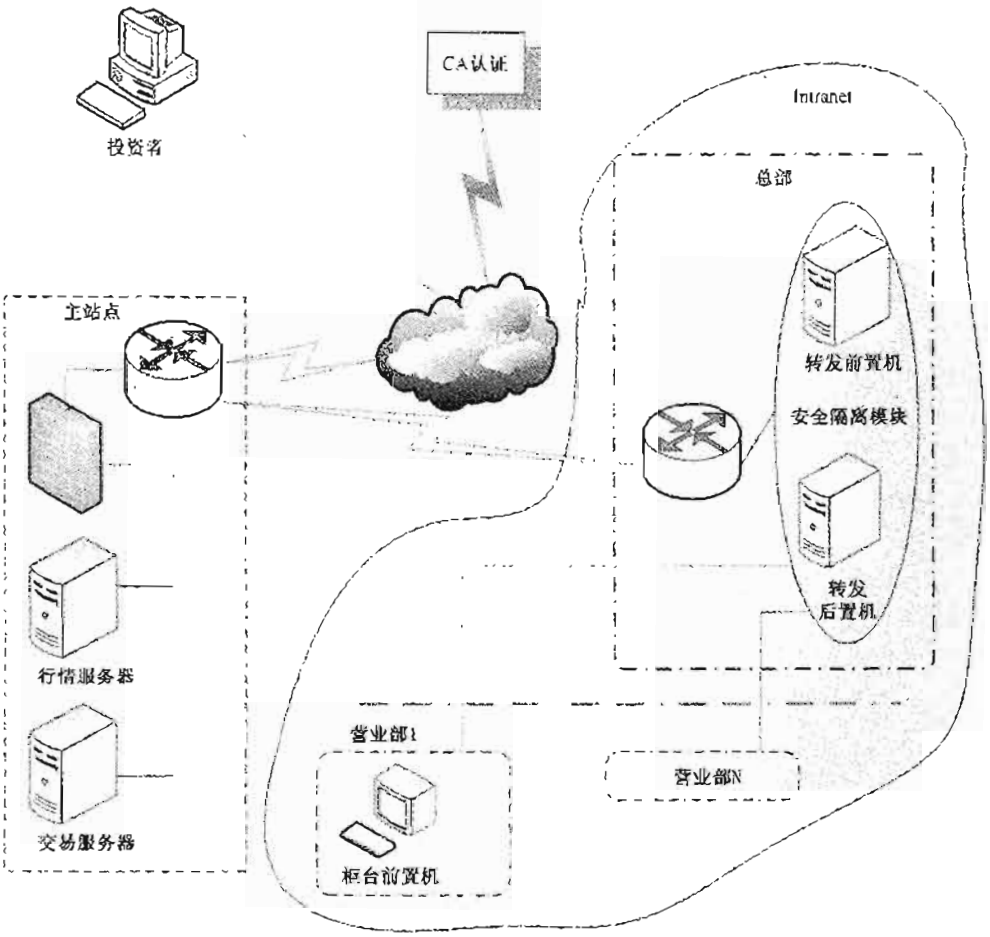

图 3 网上证券交易系统评估边界界定示意图

4.3.2.4 网上证券交易系统安全域描述

网上证券交易系统是一个涉及不同用户对象、数据敏感程度等的一个复杂网络。在网上证券交易系统的安全保障目的中，应根据用户对象、数据敏感程度等划分安全域。通过不同安全域的描述和界定，就能更好对网上证券交易系统进行描述。

网上证券交易系统的网络系统结构包括根据用户对象的不同以及所涉及的信息敏感程度的不同而进行的分类。如表1。

表1 网上证券交易系统用户和信息敏感程度描述

	网上证券交易系统		
用户对象	普通公众	投资者	证券公司人员
信息敏感程度	—	商业秘密	内部信息

4.3.3 网上证券交易系统详细描述

从管理体系、技术体系和业务体系三方面分别对网上证券交易系统进行描述。

4.3.3.1 网上证券交易系统管理体系

管理体系：在管理体系中，需要对网上证券交易系统现有的管理组织结构、所使用的相应规章制度和所涉及的重要资产进行描述。

4.3.3.1.1 组织机构

在网上证券交易系统组织机构概述中，应包括同网上证券交易系统相关的管理、使用、开发、集成、支持组织机构的描述，特别是相关安全保障管理的组织机构的描述。

4.3.3.1.2 管理制度和法规

管理制度、法规描述部分要求列出同网上证券交易系统管理相关的目前使用的相应规章制度和相关法规，在网上证券交易系统信息安全保障目标中用户应给出其所评估的网上证券交易系统管理中所使用的国家、部门、行业和内部的相关管理制度和法规。

4.3.3.1.3 系统资产

资产是网上证券交易系统所要保护的对象，所有威胁都必须针对资产才能产生影响，所有威胁只有通过资产这个载体才能影响网上证券交易系统的最终目标——网上证券交易系统的使命。

在网上证券交易系统中，资产分为物理资产和信息资产。

4.3.3.1.3.1 物理资产

物理资产是指网上证券交易系统中的各种硬件、软件和物理设施。例如：系统的各种网络设备和软件资产。在网上证券交易系统信息安全保障目标中，应详细列出所评估的特定网上证券交易系统中的所有重要资产。下面仅列出在网上证券交易系统中所包含的部分物理资产示例，作为参考：

a) 物理设施

物理设施包括场地、机房、电力供给(负荷量及冗余、备份、净化)、灾难应急(防水、火、地震、雷击等)、文档及介质存储。

b) 硬件资产

硬件资产包括：

1) 计算机：包括大、中、小型计算机、个人计算机；

2) 网络设备：包括交换机、集线器、网关设备或路由器、中继器、桥接设备、调制解调器/Modem池、配线架；

3) 中间件设备：作为交易中间件使用的后台转换机、柜台处理机、委托成交转换机、单向卫星接收机、双向卫星接收机、报盘机以及行情处理等专用微机或工作站；

4) 传输介质及转换器：包括同轴电缆(粗/细)、双绞线、光缆/光端机、卫星信道(收/发转换装置)、微波信道(收/发转换装置)；

5) 输入/输出设备：包括键盘、电话机、传真机、扫描仪、打印机(激光/针式/喷墨)、显示器、终端(数据/图像)；

6) 存储介质：包括纸介质、磁盘、磁光盘、光盘(只读/一次写入/多次擦写……)、磁带、录音/录像带；

7) 监控设备：包括摄像机、监视器、电视机、报警装置。

c) 软件资产

软件资产包括：

1) 计算机操作系统：包括 Unix、Windows NT/2000、HP-UX、其他计算机操作系统；

2) 网络操作系统：包括 IOS、Novell Netware、SNA、其他专用网络操作系统；

3) 通用应用软件：包括 Notes/MS Word、E-mail、Web 服务/发布与浏览软件、其他服务软件；

4) 网络管理软件：包括 SNMP、HP Openview、Netview、其他网络管理软件；

5) 数据库管理软件：包括 Oracle、Sybase、SQL Server、其他数据库管理软件；

6) 业务应用软件：包括网上交易客户端软件、交易主机应用服务软件、交易转发软件、行情服务、行情发送及行情接收软件、SSL 安全网关软件、物理隔离软件等。

4.3.3.1.3.2 信息资产

信息资产是指在网上证券交易系统计划组织、开发采购、实施交付、运行维护和废弃这一网上证券交易系统生命周期过程中产生的同网上证券交易系统本身相关的有价值的信息以及网上证券交易系统所存储、处理和传输的各种相关的办公、管理和业务等信息。例如：系统的网络配置信息、各种维护升级记录、各种业务应用信息等。下面仅列出在网上证券交易系统中所包含的部分信息资产示例，作为参考：

a) 客户信息：包括客户资料、资金数据和交易数据等，这些均属于商用加密信息类别；

b) 交易信息：是主要的业务数据，包括委托数据、成交回报数据等；

c) 行情信息：包括行情查询数据、行情分析数据、现行行情和历史行情信息数据等；

d) 信息资讯：主要是证券相关信息，如新闻、综合报道、专家观点、机构股评、资料、快讯新闻和股评等内容通过信息发布系统提供给投资者参考；

e) 密码信息：包括秘密密钥、私钥、公钥、证书等；

f) 系统维护管理信息：包括系统运行日志、系统审计日志、系统监督日志、入侵检测记录、系统口令、系统权限设置、数据存储分配、内部网络地址、系统配置数据、网络设备的配置信息、终端信息、IP 地址分配信息、设备采购信息、设备维护及升级记录、布线图纸、布线系统维护及升级记录、通信线路参数、以及其他信息等。

4.3.3.2 网上证券交易系统技术体系

技术体系是信息系统描述的基础，需要对现有的各种应用、相应的网络基础设施和所采用的技术标准进行描述，这些描述将帮助了解用户的信息系统并为进一步描述业务系统提供基础支持。技术体系描述包括网络基础设施描述、技术应用描述和适用技术标准描述。

4.3.3.2.1 网络基础设施描述

网络基础设施结构图将描述网上证券交易系统的网络层次等网络基础设施的构成图，是对网上证券交易系统的网络基础设施结构概念性说明。用户应基于此图，在信息系统专业设计文档中给出网上证券交易系统的详细网络结构图。

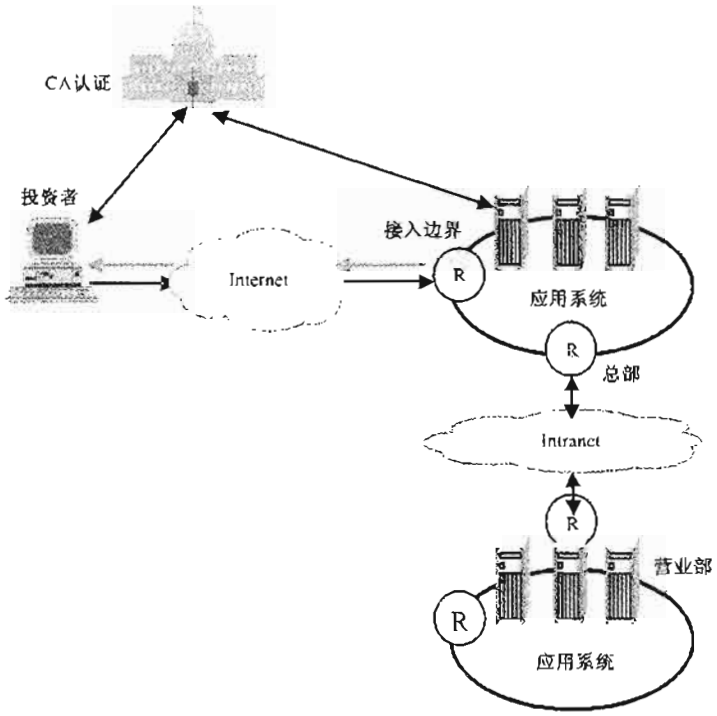

图 4　网上证券交易系统网络体系结构

本系统提供如下安全服务：

a）　确保投资者交易数据的机密性、完整性和准确性；

b）　正确识别网上投资者身份，防止假冒投资者或证券公司身份；

c）　防止交易双方事后否认该事情发生过；

d）　确保网上证券交易系统和其他业务在技术上隔离，禁止通过网上证券交易系统直接访问任何证券公司内部系统；

e）　保证本系统安全性和可用性。

4.3.3.2.2　技术应用描述

描述用户信息系统的各种应用说明。在网上证券交易系统信息安全保障目标中，应详细描述网上证券交易系统的各种应用系统，并进行详细描述。

4.3.3.2.3　适用技术标准描述

列出相关技术应用等所适用的技术标准。在网上证券交易系统信息安全保障目标中，应列出网上证券交易系统的各种应用系统所遵循的标准。

4.3.3.3　网上证券交易系统业务体系

业务体系描述即从业务角度和应用角度出发，基于技术体系，对组织机构的主要业务应用进行分类和描述，并通过业务流程和业务信息流来进一步解释。业务系统描述包括主要业务应用描述、业务流程描述和业务信息流描述。

4.3.3.3.1　主要业务应用描述

列出组织机构的主要业务应用并进行描述。在网上证券交易系统信息安全保障目标中，应对网上证券交易系统进行详细描述，此描述应包含系统的功能结构图、系统的输入数据、数据操作以及输出的产品。

网上交易系统从功能上主要划分为实时委托交易子系统、行情查询与分析子系统和资讯服务子系

统，分别包括如下业务：

a) 实时委托交易业务：A股委托交易、B股委托交易、新股申购、基金及债券业务、资金余额查询、股份余额查询、成交回报查询、历史成交记录查询、撤单、保证金对账单查询、个人信息查询、盈亏计算、总资产核算、修改交易密码、储蓄余额查询、从保证金转款到储蓄、从储蓄转款到保证金、计算市值、批量委托、交割单、对账单查询等；

b) 行情查询与分析业务：实时行情查询、大盘走势、个股行情、行情分析（支持分时走势，F5日线图，F8周线、月线、分钟线的查询）服务等；支持离线浏览和数据下载；支持各种画线功能图；支持自选股设置；支持板块定义及分析，综合排名功能，紧急公告功能；支持股票模糊查询、拼音查询等功能；

c) 资讯服务业务：提供深沪交易所信息、个股资料信息、提供部分研究报告服务及投资建议、特别报道、紧急公告功能、信息咨询服务、投资研究服务、投资建议等服务。

网上证券交易系统的应用业务是为证券公司现有客户和潜在客户提供安全、高效的网上证券交易，使客户方便快捷地查询个人信息资源，并能通过该系统接受行情分析、信息咨询等服务。

4.3.3.3.2 业务流程描述

基于组织机构的管理结构等，描述业务的流程。在网上证券交易系统信息安全保障目标中，根据业务应用结合组织机构的业务流程进行详细描述。

4.3.3.3.2.1 委托交易流程

委托交易子系统由客户端、物理隔离机、加解密安全网关、交易主机应用服务器、交易分发服务器和营业部交易前置机几部分组成。

首先，投资者亲自到开户营业部签署开通网上交易的协议同时获得数字身份证明文件（CA证书），以此通过客户端程序或Internet进入网上交易系统。

在正式开始交易前，客户端软件和服务器软件之间要先进行“握手”，在握手过程中通过数字身份证明文件（CA证书）互相鉴别身份。

其次为第二个阶段——数据传输过程，也就是实际的数据传输过程，这个过程发生在握手过程结束后。在正式交易过程中，客户的交易请求信息由客户端软件加密后把加密后的信息发给加解密安全网关服务器，继而发给交易主机应用服务器，然后转发给总部交易分发服务器，分发服务器根据客户不同的需求将交易信息发送到相对应的营业部交易前置机。再由前置机将加密后的交易请求信息经解密再提交给营业部柜台系统的中间件服务器，最后由营业部柜台系统做相应的处理，并将最终的交易结果按原路反馈给客户。

4.3.3.3.2.2 行情查看流程

行情分析子系统由行情客户端、行情服务器、行情接收系统及行情发送程序几部分组成。

投资者需要查看行情时，只需通过行情客户端输入想要查询的证券代码。客户端即将查询请求发送给行情服务器，在收到客户端的请求后，行情服务器从行情数据库中提取相应的证券信息反馈给行情客户端。

此外，在开市期间，行情接收程序会实时地从行情发送程序获取行情信息并将其转存到行情数据库中，以便用户得到最新的信息。

行情发送程序通过隔离机把读取的交易所的实时行情转发给行情采集接收程序，保存在行情数据库中供行情服务器调用。

行情查看流程如图5所示。

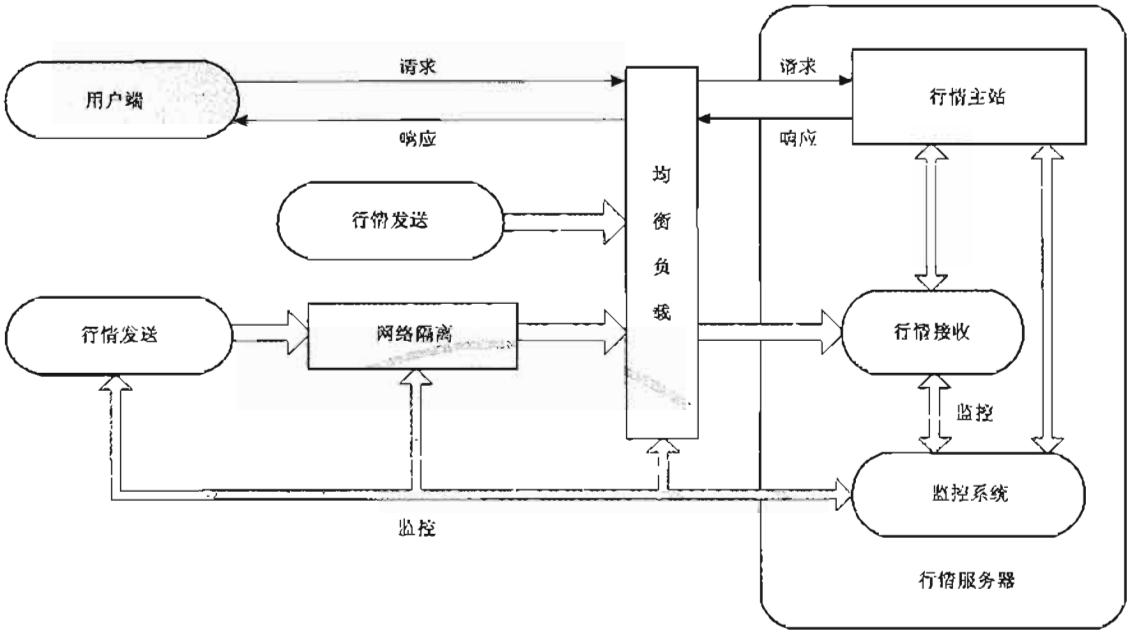

图 5　行情查看流程图

4.3.3.3.2.3　信息资讯流程

投资者可以通过浏览器访问证券网站或通过客户端程序直接查阅所需信息。信息资讯查看流程与行情查看流程完全相同。

4.3.3.3.3　业务信息流描述

描述主要业务应用的接口和相应数据流。数据流描述应包括数据的类型以及数据传送的一般方式。在网上证券交易系统中存在两种类型的信息流：投资者到券商的信息流、券商到投资者的信息流。在网上证券交易系统信息安全保障目标文档中应根据具体情况，并参考本准则中所提出的信息流分类方法进行详细描述。

5　安全环境

5.1　假设

假设是建立在对网上证券交易系统环境预期的应用环境和使用方式的基础上。假设按 A-1、A-2 ……A-N 编号，假设一般分两类：

a)　关于网上证券交易系统开发和运行环境的一般假设(包括与系统交互的人员、内部互连和物理控制的陈述)；

b)　网上证券交易系统中描述系统角色的假设。

5.1.1　网上证券交易系统环境安全假设

环境安全假设有：

A-1　可用性可能依赖于从通信线路提供商提供的通信质量和能力。自然或人为灾难对通信可用性产生的扰动是在系统之外的。通信线路是作为系统一部分的。系统必须提供足够的保护以降低拒绝服务攻击达到一个可接受的水平。

A-2　网上证券交易系统的开发应采用不断持续改进的方法。

A-3　网上证券交易系统能使用不可信任的通信网络来建设通信能力。

5.1.2　网上证券交易系统安全服务假设

网上证券交易系统安全服务假设有：

A-4　网上证券交易系统存在以下不同的安全域：

a) 每个安全域具有它的管理和策略；

b) 公众网是一个特殊的安全域，它有管理，没有安全策略，是敌对行为主要来源；

c) 安全域间的连接在建立互连之前要求上级主管单位授权。如果互连系统属于不同上级主管单位那么互连必须由两个上级主管单位批准；

d) 连接及使用公众网，应符合有关法令、规范和制度。

A-5 网上证券交易系统安全实行深度防御。在适合时，协调机构和系统管理者可以实现补充保护机制。

A-6 系统不能降低网上证券交易系统的全部安全状态。作为一个整体，必须考虑优于保护系统的对策能阻止系统引入对网上证券交易系统的额外安全风险。安全域外的连接必须针对潜在的风险进行检查。

a) 推动通用策略、过程和机制的发展；

b) 这些保护的运行可以分配给协调机构；

c) 符合网上证券交易系统特定的或唯一的脆弱性的策略和对策是系统的责任。

A-7 在检测到的涉及执法机构的安全事件里，协调机构为网上证券交易系统提供单方的意见。

5.2 威胁

在安全环境中的资产部分描述了网上证券交易系统所需保护的资产对象客体，在本条的威胁描述中将描述在网上证券交易系统安全环境中对这些资产的所有相关威胁，这些资产是在网上证券交易系统或其环境内需要特定保护的。值得注意的是，并非所有的在环境中可能遇到的威胁都必须列出，只有那些与网上证券交易系统的安全运行相关的威胁才需要列出。

威胁是一个具备一定攻击能力的特定攻击源利用特定脆弱性对特定资产进行某种方式攻击所产生某种程度影响的可能性。因此，威胁应通过已确定的攻击源、脆弱性、资产、攻击方式和可能影响的程度进行描述。

5.2.1 威胁的分类

威胁是由多个威胁要素组成的，因此从不同角度来看，威胁有不同的分类方式。

5.2.1.1 根据威胁源主体的威胁分类

从威胁源主体来分，威胁分为：

——人员威胁：由人产生或其激活的威胁，例如无意行动（偶然的数据访问、误操作等）或有意的行动（基于网络的攻击、恶意软件上传和机密数据的非授权访问等）；

——自然威胁：洪水、地震、龙卷风、山崩、雪崩、电力风暴以及其他此类事件；

——环境威胁：长期电力故障、污染、化学和液体泄漏。

5.2.1.2 根据攻击方式的威胁分类

从攻击方式来分，威胁分为：

——内部人员攻击；

——被动攻击；

——主动攻击；

——物理临近攻击；

——分发攻击。

各种攻击方式具体解释如下：

a) 内部人员攻击

内部人员攻击往往由内部合法人员造成，他们具有对网上证券交易系统的合法访问权限。内部人员攻击分为恶意和非恶意两种，即恶意攻击和非恶意攻击。

恶意攻击是内部人员出于各种目的，对所使用的信息系统实施的攻击。

非恶意攻击是由于内部合法人员的无意行为造成了对网上证券交易系统的攻击，他们并非故意要

破坏信息和系统，但由于误操作、经验不足、培训不足而导致一些特殊的行为，对系统造成了无意的破坏。

典型的内部人员攻击有：

1） 恶意修改数据和安全机制配置参数；

2） 恶意建立未授权的网络连接，如：拨号连接；

3） 恶意的物理损坏和破坏；

4） 无意的数据损坏和破坏，如：误删除。

b） 被动攻击

被动监视开放的通信信道（如：无线电、卫星、微波和公共通信网络）上的信息传送。被动攻击主要是了解所传送的信息，一般不易被发现。典型例子如下：

1） 监视通信数据；

2） 解密、加密不善的通信数据；

3） 口令截获；

4） 通信量分析。

c） 主动攻击

攻击者主动对信息系统实施攻击，包括企图避开安全保护，引入恶意代码，以及破坏数据和系统的完整性。典型的例子有：

1） 修改传输中的数据；

2） 重放所截获的数据；

3） 插入数据；

4） 盗取合法建立的会话；

5） 伪装；

6） 越权访问；

7） 利用缓存区溢出（BOF）漏洞执行代码；

8） 插入和利用恶意代码（如：特洛依木马、后门、病毒等）；

9） 利用协议、软件、系统故障和后门；

10） 拒绝服务攻击。

d） 物理临近攻击（接近攻击）

攻击者试图在地理上尽可能接近被攻击的网络、系统和设备，目的是修改、收集信息，或者破坏系统。这种接近可以是公开的和秘密进入的，也可以是两种都有，典型案例有：

1） 修改数据；

2） 收集信息；

3） 偷窃；

4） 物理破坏。

e） 分发攻击

分发攻击是指在网上证券交易系统软件和硬件的开发、生产、运输、安装阶段，攻击者恶意修改设计、配置等行为。例如：

1） 利用开发制造商的设备修改软硬件配置；

2） 在产品分发、安装时修改软硬件配置。

5.2.1.3 根据威胁造成的影响结果的威胁分类

从威胁造成的影响结果来分，威胁分为：

——可忽略的威胁；

——造成一定影响的威胁；

——造成严重影响的威胁；

——造成异常严重影响的威胁。

5.2.2 威胁模型

综合上述威胁分类和分析，网上证券交易系统的威胁模型将主要根据威胁源、攻击方式、资产、影响方式和影响结果进行分析，参照表2。

表2 网上证券交易系统威胁模型

威胁源			攻击方式	资产	影响方式	影响结果
人	客户和社会公众（外部用户）	普通公众	内部人员攻击 被动攻击 主动攻击 物理临近攻击 分发攻击	信息资产 物理资产	保密性 完整性 可用性 其他	影响结果可忽略 一定影响结果 严重影响结果 异常严重影响结果
		证券客户				
		商业和专业组织				
		政府				
	内部员工（内部用户）	普通员工				
		系统管理员				
自然						
环境						

从表2可以看出，网上证券交易系统的安全威胁是多级别的，因此，网上证券交易系统整体上必须具有应对这些攻击的能力，但具体到某一个应用系统则需要区别对待，认真分析。

5.2.3 具体的信息安全保障威胁

基于前面的威胁分类和威胁模型，结合网上证券交易系统的特点，列出网上证券交易系统的基于威胁源进行分类的主要威胁表，为方便参考、尤其是方便补充和描述，威胁按T-1、T-2……T-N编号。

a) 人员威胁

T-1 网上证券交易系统的体系结构、设计、实现和维护缺陷可能导致信息安全保障失效。

T-2 网上证券交易系统不正确的运行可能导致信息安全保障失效。

T-3 网上证券交易系统失效时不正确的重启和/或恢复可能导致信息安全保障失效。

T-4 网上证券交易系统环境的改变可能引入或恶化脆弱性。

T-5 未授权用户可能获得对网上证券交易系统的逻辑访问。

T-6 可信任角色的人（如网上证券交易系统的管理人员和维护人员）由于技术能力的不足，可能导致信息安全保障失效。

T-7 可信任角色的人（如网上证券交易系统的管理人员和维护人员），由于管理疏忽，可能导致信息安全保障失效。

T-8 某人可能物理的攻击网上证券交易系统从而危及它的信息安全保障。

T-9 某人可能引入未授权软件（包含恶意代码等）到网上证券交易系统中。

T-10 某人可能篡改网上证券交易系统的保护相关的机制。

T-11 授权用户（内部用户）或伪装成授权用户的未授权用户可能访问网上证券交易系统资源或执行未获准的访问权限的操作。

T-12 非授权用户的个人使用非技术手段可能获得处理资源或信息的访问。

T-13 用户输入错误可能导致错误数据，从而导致混乱的输出信息或拒绝服务。

T-14 用户对接收或发送信息行为的否认，以逃避接收或发送信息后所应负的责任和义务。

T-15 若干个人从事拒绝服务攻击，攻击可能导致网上证券交易系统资源不可用。

T-16 外部用户可能侵害网上证券交易系统的通信能力。

T-17 攻击者通过在通信线路上窃听的方式获取用户数据。

T-18 攻击者为了获得信息内容而对加密数据进行密码分析。

T-19 攻击者欺骗用户使其接受假冒系统的服务。

T-20 攻击者利用社会关系获得有关系统登录、使用、设计或操作的信息。

T-21 对策和策略的局限和缺陷可能被知识渊博的对手获取。

T-22 因为弱化或错误的执行访问控制，使攻击者未被检测即获得的对系统的访问，造成对系统完整性、保密性或可用性潜在的危害。

T-23 因为缺乏审计机制，造成安全相关的事件可能没有记录或不可追踪。

b) 自然威胁

T-24 自然灾害可能导致关键操作的暂停和/或网上证券交易系统服务的中断。

c) 环境威胁

T-25 电力系统故障可能导致关键操作的暂停和/或网上证券交易系统服务的中断。

T-26 通信线路出现意外中断，造成网上证券交易系统资源不可用。

T-27 关键系统组件技术故障导致网上证券交易系统关键功能丧失。

T-28 重要数据在传输过程中可能出现错误、导致信息完整性和可用性的破坏。

T-29 网上证券交易业务高峰时，由于网络流量过大造成故障。

5.3 组织安全策略

网上证券交易系统安全策略是一切信息安全保障活动的基础和出发点，指导如何对资产进行管理、保护和分配的规则和指示，指导整个网上证券交易系统安全体系的设计与实施。所有网上证券交易系统安全控制措施(包括技术控制措施和管理控制措施)的选择、运营和维护均依据安全策略进行。制定安全策略是每一个开展网上证券交易工作的公司都必须完成的工作，安全策略一定和相关的组织机构的业务相关，一份有效并设计良好的策略是安全目的能否实现的关键。

网上证券交易系统安全策略的制定必须建立在充分了解其策略需求的基础上、并符合国家的法令法规、国家的信息安全保障标准、上级业务主管部门颁布的信息安全保障规定、标准、规范的要求。安全策略的制定必须面面俱到，但是又不能太具体和注重细节。安全策略采用通俗易懂的语言解决网上证券交易系统信息安全保障应该做什么的问题，而不涉及怎么做的问题。

通常，安全策略通过规定一套规则来规范网上证券交易系统的建设及其运行、维护和管理。这些规则清晰的说明哪些行为是被允许的。

各种网上证券交易系统的其他各类文档，如网上证券交易系统的技术方案、管理制度及操作指导手册、工程实施过程文档和验收报告、应用软件开发过程等，必须满足信息安全保障策略的要求，所有的这些文本的陈述清晰地说明信息安全保障策略所规定的这些规则。通过使用管理控制措施、技术控制措施或者两者，这些规则可以被实现。规则覆盖了四个主要安全保障目的：

——可核查性；

——可用性；

——机密性；

——完整性。

信息安全保障策略要充分反映相应证券公司的运行和业务的安全保障要求，是组织、机构核心价值和任务的体现，因此，网上证券交易系统的安全策略的制定、签署、实施必须由相应公司的最高领导人负责。

证券系统的特点决定了网上证券交易系统的安全策略是一个多层次的结构，典型的网上证券交易系统信息安全保障策略具有三个层次：系统高层安全策略；系统及子系统级安全策略；安全产品级安全策略。策略按 P-1、P-2……P-N 编号。

5.3.1 网上证券交易系统高层安全策略

高层安全策略有：

P-1 建立网上证券交易系统高层策略：网上证券交易系统的高层安全策略是对信息安全保障问题的最高层次论述。表述证券公司最高领导层对信息安全保障的支持，定义网上证券交易系统所要实现的总体安全保障目标。网上证券交易系统高层安全策略要求用精炼的语言对网上证券交易系统的安全保障目标进行概括性论述，规定策略适用范围和应建立的安全保障管理组织及其相关职责。高级管理层将以身作则来支持信息安全保障的建设及其相关的规定，并且表明将对违反信息安全保障规范的行为做出惩戒。

5.3.2 系统及子系统级安全策略

系统及子系统级策略服从于高层安全策略所制定的网上证券交易系统的总体安全保障目标。它指导具体技术控制措施和管理控制措施的选用和实施。在网上证券交易系统，典型的系统及子系统级安全策略主要包括以下方面：

P-2 标识与鉴别策略：网上证券交易系统应能够对每个授权网络用户（包括人、设备和过程）进行唯一的标识；在允许任何用户执行任何操作（事先定义好的操作除外）之前，网上证券交易系统应能够鉴别每个用户（人或其他的信息系统）身份；如果采用口令进行鉴别，网上证券交易系统应该能够主动维护“强壮”口令设置，而不允许使用单词、代表日期的数字或其他弱的、易猜测的口令；如果口令还不能提供足够的鉴别强度，在允许任何用户执行任何操作（事先定义好的操作除外）之前，网上证券交易系统应能够提供更强的鉴别机制对用户身份进行鉴别；口令应该设置使用期限，过期的口令不能重复使用等。投资者发出委托买入、委托卖出、资金转出、资金转入、委托撤单请求时，需要提供口令进一步确认。

P-3 访问控制策略：访问控制（登录安全、口令、用户界面、访问控制、远程办公和远程访问……），例如网上证券交易系统应该对网络用户实施强鉴别机制；网上证券交易系统应能够在达到管理员预设的失败登录尝试次数后自动锁定用户账号；网上证券交易系统应该在用户登录时依据上级机构的要求显示标准的“登录警告旗标”。

P-4 公众网安全策略：Internet 与网上交易的入口处建立访问控制策略，保证 Intranet 等各种通信信道的安全可信性。通信前使用数字证书验证和标识通信双方的身份。

P-5 备份和恢复策略：制定详细的备份策略，保护网上交易和行情系统的用户数据、安全功能数据、系统和应用程序、物理设备。对备份和恢复进行管理，制定备份和恢复权限，受备份的数据、程序和设备实施相应的访问控制策略。制定备份恢复计划，定期演练该计划。

P-6 恶意代码策略：应建立恶意代码（包括病毒、蠕虫、特洛伊木马……）的安全策略（例如：建立病毒防护类型、第三方软件的处理规则、与病毒责任相关的用户）。

P-7 加密策略：基于法律依据对加密管理，加密数据处理，密钥生成机密，密钥管理等建立相应的加密策略。

P-8 软件开发策略：软件开发策略包括对软件开发程序、测试文档、修改控制以及配置管理、第三方开发、知识产权等方面制定软件开发相关的策略。

P-9 安全审计策略。

P-10 风险评估策略。

P-11 外包服务策略。

P-12 人事策略：网上证券交易系统的授权的管理者和用户必须经过适当的培训，应建立定期的教育计划和开展培训活动以使他们能够：

——有效地遵守组织安全策略；

——正确执行组织安全策略所规定的安全控制措施。

P-13 事件响应策略。

P-14 业务持续性策略。

P-15 灾难恢复策略。

5.3.3 安全产品级安全策略

安全产品级安全策略需要满足系统安全策略。安全产品级策略直接指导制订安全产品的配置规则，关系到安全产品功能的实现，包括：

P-16 安全产品级安全策略。

典型的安全产品级安全策略有：

——防火墙使用策略；

——IDS 使用策略；

——VPN 产品使用策略；

——路由器使用策略；

——防病毒产品使用策略；

——CA 使用策略；

——隔离设备使用策略。

6 安全保障目的

6.1 安全保障技术目标

安全保障技术要求，即从信息技术系统安全角度达到信息系统的安全保障目标。同具体的信息技术产品和产品系统不同，信息技术系统是作为信息系统一部分的执行组织机构信息功能的用于采集、创建、通信、计算、分发、处理、存储和/或控制数据或信息的计算机硬件、软件和/或固件的任何组合所构成的一个复杂系统。要描述信息技术系统的具体目的，首先需要对信息技术系统建模并建立信息系统的分析框架，然后基于此建模和分析框架，进行具体技术措施和技术手段的安全保障要求。

在网上证券交易系统安全评估准则中，将基于通用的信息技术系统分析模型建立信息技术系统的分析模型。基于此分析模型，将安全保障技术目标分解为对网络基础设施的目标要求、对边界的要求、对计算环境的要求和对支撑性基础设施的要求，从而完成整个安全保障技术目的的描述。技术目标按 OT-1、OT-2……OT-N 编号。

6.1.1 端到端安全保障技术目标

为维护信息服务，应对端到端的信息进行保护，保护端到端的安全。符合该要求的目标如下：

OT-1 应通过加密功能来为远程系统提供安全会话。

OT-2 为用户从边界外发送和接收信息提供强认证和认证的访问控制。

OT-3 应充分定义密码的组成、功能和界限，为密码在整个生命期中提供保护。

OT-4 应能够限定单一用户并发会话数。

OT-5 必须能在指定的时间间隔到期后，自动终止用户对系统的访问权。

OT-6 应能提供接收方接收信息的证据，以避免接收方逃避接收信息的责任。

OT-7 应能提供发送方发送信息的证据，以避免发送方逃避发送信息的责任。

OT-8 应为用户提供服务和资源以阻止其他用户访问用户隐私。

OT-9 必须能够识别传送过程中信息的修改，包括插入伪造信息以及删除或替换合法信息。

6.1.2 本地计算安全保障目标

这包括在系统高端环境中的多种现有和新出现的应用中充分利用标识和鉴别、访问控制、机密性、完整性和抗抵赖性安全服务。为满足上述要求应实现下列安全保障目标：

OT-10 确保服务器和应用得到充分保护以避免拒绝服务、数据非授权泄漏和数据的更改。

OT-11 无论服务器或应用位置，都必须确保由其处理的数据的机密性和完整性。

OT-12 对于内部和外部的受信任人员与系统从事的违规和攻击活动具有充分的防范能力，对行为进行审计。

OT-13 必须为管理员规定存取权限（访问控制策略），防止管理员滥用职权使用信息。

OT-14 对系统实体参数的变化进行审计，以便于防止管理员允许未授权的用户访问对其本应禁止访问的资产。

OT-15 必须定义审计管理员职责，以防止审计数据的修改和破坏。

OT-16 为所有服务器进行配置管理维护以跟踪补丁和系统配置变更。

OT-17 当某一安全功能没有成功执行时，信息系统能自动恢复到一个安全状态。

OT-18 必须为关键组件提供运行错误容限，当一个或多个系统组件失效时系统能继续运行。

OT-19 应提供充分的备份存储和有效恢复机制确保系统能够被重构。

6.1.3 系统的边界安全保障目标

为了从专用或公共网络上获得信息和服务，许多机构通过其信息基础设施与这些网络连接。因此，这些机构必须对其信息基础设施实施保护，例如：保护其本地计算机环境不受入侵。一次成功的入侵可能会导致对于可用性、完整性或机密性的损坏。符合该要求的目标如下：

OT-20 确保在边界间或通过远程访问进行交换的数据得到保护并免受泄漏。

OT-21 确保物理和逻辑边界得到充分的保护。

OT-22 确保受保护边界内的系统和网络维持可接受的可用性并得到充分保障以避免拒绝服务。

OT-23 为那些在边界内的由于技术或配置问题而不能保护自己的系统提供边界防御。

OT-24 对系统边界发生的安全行为进行检测、审计及响应。

6.1.4 网络和基础设施的安全保障目标

为维护信息服务，并对各种信息进行保护，避免无意中泄露或更改这些信息，组织机构必须保护其网络和基础设施。符合该要求的安全保障目标如下：

OT-25 保护局域网和广域网通信网络(例如：免受拒绝服务攻击)。

OT-26 为这些网络上传送的数据提供机密性和完整性的保护(例如：使用加密和流量流安全措施以抵抗被动监控)。

OT-27 确保广域网上所交换的所有数据得到保护，不会泄漏给任何未授权的网络访问者。

OT-28 确保支持使命关键和使命支持数据的广域网提供合适的保护，免受拒绝服务的攻击。

OT-29 保护受保护信息免受延时、误传或未传送的破坏。

OT-30 保护下列信息免受流量分析：用户流量，网络基础设施控制信息。

OT-31 确保保护机制不会干扰同其他授权骨干网络和封闭网络间的无缝操作。

6.1.5 支撑性基础设施安全保障目标

支撑性基础设施为信息技术系统安全提供了支撑性的平台，它为信息技术系统提供了密钥管理、监测和响应功能。所需要的能够进行检测与响应的支撑性基础设施组件包括：入侵监测系统、审计、配置系统，以及调查所需信息的收集，符合该要求的安全保障目标如下：

OT-32 提供用以支持密钥、优先权与证书管理的密码基础设施；并能够积极识别使用网络服务的实体。

OT-33 提供一种能够对入侵和其他违规事件快速进行检测与响应并能够支持操作环境的入侵检测、报告、分析、评估和响应基础设施。

6.2 安全保障管理目标

网上证券交易系统信息安全保障管理的目标就是根据通过覆盖信息系统生命周期的各阶段的管理域来标准化建立完善的信息安全保障管理体系，从而在实现信息能够充分共享的基础上，同时保障信息和其他资产，保证业务的持续性并使业务的损失最小化。信息系统安全保障管理的各管理域的目标要求如下，管理目标按 OM-1、OM-2……OM-N 编号。

OM-1 安全组织机构：应当建立健全的信息安全保障管理的组织机构，并在组织机构内部进行恰当的信息安全保障管理的权责分配。

OM-2 信息安全保障策略制度：为网上证券交易系统提供信息安全保障活动的管理方向及支持。

安全策略通过规定一套规则来规范网上证券交易系统的建设及其运行、维护和管理。这些规则清晰的说明哪些行为是被允许的。安全策略应能够指导整个网上证券交易系统安全体系的设计与实施，所有网上证券交易系统安全控制措施（包括技术控制措施和管理控制措施）的选择、运营和维护均依据安全策略进行。

OM-3 人员安全：确保网上证券交易系统的合法用户（特别是关键的系统安全保障管理人员）素质可信、能力可靠。并通过有效的培训教育，确保网上证券交易系统的有效运行，减少有意和无意的人为威胁。

OM-4 信息安全保障战略规划：开发信息技术长期和短期规划，确保网上证券交易系统的信息技术同证券公司的使命和业务战略相一致。并指导进行年度预算，监控费用、投资和收益，确保网上证券交易系统的建设能够有序、持续的进行，并保持运行的高效性。

OM-5 投资和预算管理：通过建年度预算，监控费用、投资和收益，确保网上证券交易系统的建设能够保持合理的成本一效益比。

OM-6 应用系统开发与维护：对应用系统的开发过程进行规范性管理，并对应用系统的运行过程进行维护，预防恶意代码对业务造成的威胁。

OM-7 资产管理：建立网上证券交易系统的资产清单和责任人，对关键资产建立管理规范，对信息资产进行分级和标注。从而保证网上证券交易系统可核查性的安全保障目标，避免破坏关键信息资产的机密性。

OM-8 物理安全：根据运行环境的不同进行物理区域隔离，并进行区域访问控制，同时采取防火、防水、温度控制等措施保障网上证券交易系统基础设施的安全，有效防范自然威胁和物理临近攻击的风险。

OM-9 通信与运行管理：通过对计算机设备与主机系统的配置进行管理、制定严格的操作规范、提供不间断电源和关键设备备份、网络管理、采取防病毒措施等手段保障网上证券交易系统运行的安全。采用加密、身份认证和抗抵赖措施保障网上证券交易系统通信的安全。

OM-10 访问控制：采取有效的访问控制机制和管理措施来预防非授权物理访问和逻辑访问的风险。

OM-11 变更控制管理：在业务、使命、技术等发生变更时，将业务中断、非授权的更改和故障等的可能性减至最小。

OM-12 业务持续性管理：防止业务停顿，以及保护重要业务进程不受重大失效或灾难的影响。

OM-13 遵循性：遵循法律，避免触犯任何刑事及民事法律以及其他法定的、条例的、合同的义务和安全需求。通过核对安全策略及技术合格性，保证系统按机构的安全策略及标准进行。确保系统审计处理发挥最大效用，并把干扰降到最低。

6.3 安全保障工程目标

网上证券交易系统的安全保障工程目标是通过对信息系统建设工程过程进行标准化。信息系统的安全工程过程生命周期主要包括：挖掘安全需求、定义安全保障要求、设计体系结构、详细安全设计、实现系统安全和有效性评估。安全保障工程目标按 OP-1、OP-2……OP-N 编号。

OP-1 挖掘安全需求：目的是帮助用户理解网上证券交易系统的任务需求，确定安全策略。

OP-2 定义安全保障要求：目的是为信息系统的规划者、设计者、实施者或用户提供他们所需的安全信息。

OP-3 设计体系结构：目的是识别并设计出信息系统的体系结构。

OP-4 详细安全设计：目的是详细说明信息系统的设计方案。

OP-5 实现系统安全：目的是构造、购买、集成、验证组成信息保护子系统的配置项集合并使之生效。

OP-6 有效性评估：目的是保证信息系统能够满足用户的安全保障要求。

7 安全保障要求

7.1 安全保障技术要求

7.1.1 端到端安全保障技术要求

7.1.1.1 用户数据保护(FDP)

7.1.1.1.1 访问控制策略(FDP_ACC)

####### 7.1.1.1.1.1 子集访问控制(FDP_ACC.1)

FDP_ACC.1.1 网上证券交易系统安全功能(以下简称系统安全功能)将对安全功能策略所覆盖的主体、客体和它们之间的操作执行网上证券交易访问控制策略(以下简称网上访问控制策略)。

7.1.1.1.2 访问控制功能(FDP_ACF)

####### 7.1.1.1.2.1 基于安全属性的访问控制(FDP_ACF.1)

FDP_ACF.1.1 系统安全功能将基于安全属性和确定的安全属性组,对已明确的客体执行网上访问控制策略。

FDP_ACF.1.2 系统安全功能将执行网上访问控制策略,决定受控的主体与客体间的操作是否被允许。

FDP_ACF.1.3 系统安全功能将执行网上访问控制策略,拒绝主体对客体的访问。

应用注释:当用户账号被锁定时,系统所指定的特定实体之外的所有实体(包括用户)都不能使用该账号。只有授权管理员(如安全管理员)才能解锁该账号(如表3)。

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

客体	主体				
	投资者	安全管理员	网上委托系统操作人员	柜台操作人员	……
投资者姓名	R,E				
投资者投资账号	R,E,De				
投资者投资账号密码					
投资者通信密码					
投资者股票持有信息					
投资者股票交易信息					
投资者公开密钥					
投资者私有密钥					
……	……	……	……	……	……

注:R——读;W——写;D——删;E——加密;De——解密。

####### 7.1.1.1.3 数据鉴别(FDP_DAU)

######## 7.1.1.1.3.1 伴有保证者身份的数据鉴别(FDP_DAU.2)

系统安全功能应具有相应的能力,保证主体的真实身份,并承担信息真实性的责任(如,通过数字签名),用来保证指定的数据单元的有效性,进而验证静态的信息没有被伪造或篡改。

FDP_DAU.2.1 系统安全功能将提供产生保证客体(详见FDP_ACF.1)的有效性证据的能力。

FDP_DAU.2.2 系统安全功能将为投资者和券商提供验证网上证券交易有关数据和指令真实有效的证据和产生该证据的真实身份的能力。

7.1.1.1.4 信息流控制策略(FDP_IFC)

7.1.1.1.4.1 完全信息流控制(FDP_IFC.2)

FDP_IFC.2.1 对已确定的主体、信息流及所有导致信息流入流出安全功能策略覆盖的主体的操作,系统安全功能应执行网上信息流控制策略。

FDP_IFC.2.2 系统安全功能应确保所有导致安全控制范围内的任何信息流入流出安全控制范围内的任何主体的操作被网上信息流控制策略所覆盖(如表4)。

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

	允许	不允许
投资者到券商	合法的交易指令 未加密的行情查询指令	未经数字签名的交易指令 不符合格式要求的数据包
券商到投资者	经过加密和完整性保护的合法交易结果	未经加密和完整性保护的历史成交记录查询结果
……		

7.1.1.1.5 信息流控制功能(FDP_IFF)

7.1.1.1.5.1 简单安全属性(FDP_IFF.1)

FDP_IFF.1.1 系统安全功能应在主体和最小数目和类型的信息安全属性的基础上执行网上信息流控制策略。

FDP_IFF.1.2 对每一个操作,如果在主体和信息之间必须有基于安全属性的关系,系统安全功能应允许受控主体和受控信息之间存在经由受控操作的信息流。

FDP_IFF.1.5 系统安全功能应根据基于安全属性的规则,明确授权信息流。

FDP_IFF.1.6 系统安全功能应根据基于安全属性的规则,明确拒绝信息流。

7.1.1.1.5.2 无非法信息流(FDP_IFF.5)

FDP_IFF.5.1 系统安全功能应确保没有规避网上信息流控制策略的非法信息流存在。

7.1.1.1.6 从安全功能控制之外输入(FDP_ITC)

7.1.1.1.6.1 有安全属性的用户数据输入(FDP_ITC.2)

此功能要求安全属性能正确反映用户数据,并与从系统安全控制范围之外输入的数据正确无歧义地联系在一起。

FDP_ITC.2.1 在系统安全功能策略控制下,从系统安全控制范围之外输入用户数据时,应执行网上信息流控制策略。

FDP_ITC.2.2 系统安全功能应使用与输入的数据相关联的安全属性。

FDP_ITC.2.3 系统安全功能应确保使用的协议在安全属性和接收的用户数据之间提供明确的联系。

FDP_ITC.2.4 系统安全功能应确保对输入的用户数据的安全属性的解释与用户数据源的解释是一致的。

7.1.1.1.7 残余信息保护(FDP_RIP)

7.1.1.1.7.1 子集残余信息保护(FDP_RIP.1)

要求系统安全功能有能力确保:对于安全控制范围内的某个已定义的客体子集进行资源的配给或回收时,任何资源的任何剩余信息是不可用的,确保已经被删除的信息不再是可访问的。

FDP_RIP.1.1 系统安全功能应确保对客体(详见FDP_ACC.1)分配或回收资源时,使指定资源的任何以前的信息不再是可用的。

7.1.1.1.8 安全功能间用户数据传送保密性保护(FDP_UCT)

7.1.1.1.8.1 基本数据交换保密性(FDP_UCT.1)

FDP_UCT.1.1 系统安全功能应执行网上访问控制策略和网上信息流控制策略,能以防止未授

权泄露的方式传送和接收客体。

7.1.1.1.9 安全功能间用户数据传送完整性保护(FDP_UIT)

7.1.1.1.9.1 数据交换完整性(FDP_UIT.1)

此功能主要解决对被传输的用户数据的篡改、删除、插入和重用等的检测。

FDP_UIT.1.1 系统安全功能应执行网上信息流控制策略,能以避免出现篡改、删除、插入或重用等的方式传送和接收用户数据。

FDP_UIT.1.2 系统安全功能应能根据收到的用户数据判断,是否出现了篡改、删除、插入和重用。

7.1.1.2 标识和鉴别(FIA)

7.1.1.2.1 用户标识(FIA_UID)

7.1.1.2.1.1 用户标识(FIA_UID.1)

FIA_UID.1.1 系统应在用户被识别之前,允许代表用户实施关闭用户标识。

FIA_UID.1.2 系统允许任何代表用户启动安全功能之前,要求每个用户都被成功识别。

7.1.1.2.2 用户属性定义(FIA_ATD)

7.1.1.2.2.1 用户属性定义(FIA_ATD.1)

FIA_ATD.1.1 系统应为每一个用户保存属于他的安全属性表:用户权限及属性。

7.1.1.2.3 秘密的规范(FIA_SOS)

7.1.1.2.3.1 秘密的验证(FIA_SOS.1)

FIA_SOS.1.1 系统应提供一种机制以证明秘密(如口令字长度及字符集)满足规定的强度。

7.1.1.2.3.2 秘密的 TSF 生成(FIA_SOS.2)

FIA_SOS.2.1 系统应提供一种机制以产生满足规定的强度。

FIA_SOS.2.2 系统应能够为用户身份鉴别使用系统产生的秘密。

7.1.1.2.4 用户鉴别(FIA_UAU)

7.1.1.2.4.1 用户标识(FIA_UAU.1)

FIA_UAU.1.1 系统应在用户被鉴别之前允许代表用户请求系统证书。

FIA_UAU.1.2 系统在允许任何代表用户启动安全功能之前,要求每个用户都被成功鉴别。

7.1.1.2.4.2 不可伪造的鉴别(FIA_UAU.3)

FIA_UAU.3.1 系统应检测任何用户伪造的和正在系统中使用的鉴别数据。

FIA_UAU.3.2 系统应检测从任何其他用户复制的和正在系统中使用的鉴别数据。

7.1.1.2.4.3 多重鉴别机制(FIA_UAU.5)

FIA_UAU.5.1 系统应提供口令、证书机制以支持用户鉴别。

FIA_UAU.5.2 系统应根据口令、证书鉴别任何用户所声称的身份。

7.1.1.2.4.4 重鉴别(FIA_UAU.6)

FIA_UAU.6.1 系统应在下列条件下重新鉴别用户:交易请求失败后、及其他重鉴别条件。

7.1.1.2.4.5 受保护的鉴别反馈(FIA_UAU.7)

FIA_UAU.7.1 当鉴别在进行时,系统应仅仅将鉴别是否成功反馈给用户。

7.1.1.2.5 鉴别失败(FIA_AFL)

7.1.1.2.5.1 鉴别失败处理(FIA_AFL.1)

FIA_AFL.1.1 系统应检测何时与交易申请鉴别相关的不成功鉴别尝试达到门限值。

FIA_AFL.1.2 当达到或超过定义了的不成功鉴别尝试的次数时,系统将拒绝交易并记录。

7.1.1.2.6 用户—主体绑定(FIA_USB)

7.1.1.2.6.1 用户—主体绑定(FIA_USB.1)

FIA_USB.1.1 系统将把合适的用户安全属性关联到代表用户活动的主体上。

7.1.1.3 抗抵赖(FCO)

7.1.1.3.1 原发抗抵赖(FCO_NRO)

7.1.1.3.1.1 强制原发证明(FCO_NRO.2)

FCO_NRO.2.1 系统在任何时候都将对交易数据强制产生原发证据。

FCO_NRO.2.2 系统应能将信息原发者的身份与适用于证据的信息数字签名和证书相关联。

FCO_NRO.2.3 系统应能为给定证书、数字签名的接收者、相关检查部门提供验证信息原发证据的能力。

7.1.1.3.2 接收抗抵赖(FCO_NRR)

7.1.1.3.2.1 强制接收证明(FCO_NRR.2)

FCO_NRR.2.1 系统对收到的交易数据强制产生接收证据。

FCO_NRR.2.2 系统应能将信息收信者的身份与适用于证据的信息数字签名和证书相关联。

FCO_NRR.2.3 系统应能为给定数字签名、证书接收者、相关检查部门提供验证接收证据的能力。

7.1.1.4 安全功能保护(FPT)

7.1.1.4.1 安全功能数据输出的保密性(FPT_ITC)

7.1.1.4.1.1 传输过程中安全功能间的保密性(FPT_ITC.1)

要求系统安全功能确保安全功能数据在系统与远程可信 IT 产品间的传输不被泄露。

FPT_ITC.1.1 网上证券交易系统应保护所有的安全功能数据从系统到远程可信 IT 产品的传输过程中不被未经授权的泄密。

7.1.1.4.2 安全功能数据输出的完整性(FPT_ITI)

7.1.1.4.2.1 安全功能间的修改检测(FPT_ITI.1)

提供在远程可信 IT 被产品知道所使用的机制的假设下,检测安全功能数据在系统与远程可信 IT 产品传输过程中修改的能力。

FPT_ITI.1.1 网上证券交易系统应能够检测系统与远程可信 IT 产品间传输的所有安全功能数据的修改。

FPT_ITI.1.2 应验证在系统与远程可信 IT 产品间传输的所有安全功能数据的完整性,如果检测到数据修改时应及时通知数据的拥有者。

7.1.1.4.3 重放检测(FPT_RPL)

7.1.1.4.3.1 重放检测(FPT_RPL.1)

要求网上证券交易系统能够检测出鉴别数据和交易委托数据的重放。

FPT_RPL.1.1 网上证券交易系统应能检测鉴别数据和交易委托数据的重放。

FPT_RPL.1.2 检测到重放时,系统应及时通知系统管理员。

7.1.1.4.4 安全功能域分离(FPT_SEP)

7.1.1.4.4.1 安全功能域分离(FPT_SEP.1)

为安全功能提供不同的保护域,并在安全功能控制范围内客体分离之间提供。

FPT_SEP.1.1 安全功能应为自身的执行维护一个安全域,防止不可信主体的干扰和篡改。

FPT_SEP.1.2 安全功能应在其控制范围内主体的安全域之间强行分离。

7.1.1.4.5 状态同步协议(FPT_SSP)

7.1.1.4.5.1 相互的可信回执(FPT_SSP.2)

本组件要求对交换安全功能数据相互回执。

FPT_SSP.2.1 当网上证券交易系统的一部分发出需要回执请求时,与其通信的另一部分应在接收到未经修改的安全功能数据时给予回执。

FPT_SSP.2.2 系统安全功能应通过使用回执,来确保系统管理部分知道在各部分间所传输的安

全功能数据都处于正确状态。

7.1.1.4.6 **时间戳**(FPT_STM)

7.1.1.4.6.1 **可靠的时间戳**(FPT_STM.1)

本组件要求系统安全功能为自身提供可靠的时间戳。

FPT_STM.1.1 网上证券交易系统的安全功能应能为自身的应用提供可靠的时间戳。

7.1.1.4.7 **系统安全功能间安全功能数据的一致性**(FPT_TDC)

7.1.1.4.7.1 **系统安全功能间基本安全功能数据的一致性**(FPT_TDC.1)

本组件要求网上证券交易系统提供确保安全功能间属性的一致性的能力。

FPT_TDC.1.1 当网上证券交易系统与别的可信IT产品共享安全功能数据时，系统应能够判断所有安全功能数据的一致性。

FPT_TDC.1.2 当判断来自别的可信IT产品的安全功能数据时，系统应使用预先大家所协定的一组规则。

7.1.1.5 **系统访问**(FTA)

7.1.1.5.1 **多重并发会话限定**(FTA_MCS)

7.1.1.5.1.1 **多重并发会话的基本限定**(FTA_MCS.1)

提供适用于系统内所有用户的限制。

FTA_MCS.1.1 系统应限定并发会话的最大数目。

FTA_MCS.1.2 系统应利用缺省值执行最高并发会话次数的限定。

系统开发者应提供最大会话次数的具体数值。

7.1.1.5.2 **系统访问历史**(FTA_TAH)

7.1.1.5.2.1 **系统访问历史**(FTA_TAH.1)

提供系统显示与先前建立的会话相关的信息的要求。

FTA_TAH.1.1 在会话成功建立的基础上，系统应显示用户上一次成功的会话建立的日期、时间、方法。

FTA_TAH.1.2 在会话成功建立的基础上，系统应显示用户的上一次不成功的会话建立的尝试的日期、时间、方法、位置和从上一次成功的会话建立以来的不成功的尝试的次数。

FTA_TAH.1.3 系统在没有给用户回顾访问历史信息的机会的情况下是不能从用户界面上抹去该信息的。

7.1.1.6 **安全审计**(FAU)

安全审计包括产生、记录、存储和分析那些与安全相关活动有关的信息。审计记录结果可用来检测、判断发生了哪些安全相关活动以及这些活动是由哪个用户负责的。

7.1.1.6.1 **安全审计自动响应**(FAU_ARP)

7.1.1.6.1.1 **安全警告**(FAU_ARP.1)

安全警告功能描述了当检测到可能的安全侵害时，系统将采取的行动，包括报警或系统自动响应。

FAU_ARP.1.1 当检测到潜在的安全侵害时，系统将通知授权管理员，使产生潜在安全侵害的主体失效，或采取其他由授权管理员确定的行动。

例如，系统安全功能能够生成实时报警、终止违例进程、取消服务、或断开用户账号以及使用户账号失效等。

7.1.1.6.2 **安全审计数据产生**(FAU_GEN)

本条要求发生安全相关事件时应记录其出现，列举出网上证券系统可审计的事件类型，以及应在各审计记录内提供的审计相关信息的最小集合。

7.1.1.6.2.1 **审计数据产生(FAU_GEN.1)**

网上证券系统的审计数据产生功能只产生最小级审计事件记录，并规定进行每项记录的数据表。

FAU_GEN.1.1 系统应能为下述可审计事件产生审计记录：

a) 审计功能的启动和关闭；

b) 所有最小级的可审计事件；

c) 其他专门定义的可审计事件由证券公司自行定义。

FAU_GEN.1.2 系统将在每个审计记录中至少记录如下信息：

a) 事件的日期和时间、事件类型，主体身份，事件的结果(成功或失败)；

b) 最小级可审计事件类型见表5；

c) 专门定义的可审计事件清单由开发者列于表5的第四栏。

表5 端到端安全保障技术要求的可审计安全事件类型

组件标识	审计级别	可审计事件	专门定义的审计事件
FAU_ARP.1	最小级	当即将发生安全侵害时采取的行动。	
FAU_SAA.1	最小级	开启和关闭任何分析机制； 由工具完成的自动响应。	
FCO_NRO.2	最小级	调用抗抵赖服务。	
FCO_NRR.2	最小级	调用抗抵赖服务。	
FDP_ACF.1	最小级	成功的请求对某个被安全功能策略覆盖的客体上执行某操作。	
FDP_DAU.2	最小级	成功的产生有效证据。	
FDP_ETC.1	最小级	成功的信息输出。	
FDP_ETC.2	最小级	成功的信息输出。	
FDP_IFF.1	最小级	判定允许请求的信息流。	
FDP_IFF.5	最小级	判定允许请求的信息流。	
FDP_ITC.2	最小级	成功输入用户数据，包括任何安全属性。	
FDP_SDI.2	最小级	成功尝试检测用户数据的完整性，包括指示检测结果。	
FDP_UCT.1	最小级	使用数据交换机制的任何用户或主体的身份。	
FDP_UIT.1	最小级	使用数据交换机制的任何用户或主体的身份。	
FIA_AFL.1	最小级	获取失败鉴别的阈值和采取的动作(如，使终端无效)，及随后还原到正常状态(如，重新使终端有效)。	
FIA_SOS.1	最小级	安全功能拒绝任何测试的秘密。	
FIA_SOS.2	最小级	安全功能拒绝任何测试的秘密。	
FIA_UAU.1	最小级	使用鉴别机制失败。	
FIA_UAU.3	最小级	检测欺骗性的鉴别数据。	
FIA_UAU.5	最小级	鉴别的最后判定。	
FIA_UAU.6	最小级	重鉴别失败。	
FIA_UID.1	最小级	使用用户标识机制失败，包括提供的用户身份。	

表 5(续)

组件标识	审计级别	可审计事件	专门定义的审计事件
FIA_USB.1	最小级	绑定用户安全属性到一个主体失败(如,产生一个主体)。	
FMT_MOF.1	最小级	系统安全功能的所有改动。	
FMT_MSA.2	最小级	对某安全属性,所有提供的和被拒绝的值。	
FMT_SMR.1	最小级	对角色一部分的用户组的改动。	
FMT_SMR.3	最小级	明确请求担任某角色。	
FPT_ITI.1	最小级	检测传输的安全功能数据的修改。	
FPT_RCV.1	最小级	出现失败或服务中断。 恢复正常运行。	
FPT_SSP.2	最小级	接收期待的回执时,发生失败。	
FPT_STM.1	最小级	时间的变动。	
FPT_TDC.1	最小级	成功使用安全功能数据一致性机制。	
FRU_FLT.1	最小级	安全功能检测出的任何故障。	
FRU_RSA.1	最小级	因资源的限制对分配操作的拒绝。	
FTA_MCS.1	最小级	基于多重并发会话限定对新会话的拒绝。	
FTP_ITC.1	最小级	可信信道功能故障。 失败的可信信道功能的原发者及目标的标识。	

7.1.1.6.2.2 用户身份关联(FAU_GEN.2)

该功能解决可审计事件追溯到单个用户身份上的要求。

FAU_GEN.2.1 系统能将每个可审计事件与引起该事件的用户身份相关联。

7.1.1.6.3 安全审计分析(FAU_SAA)

7.1.1.6.3.1 潜在侵害分析(FAU_SAA.1)

本功能为寻找可能的或真正的安全侵害,用来分析系统活动和审计数据的自动化措施的要求。这种分析可用于支持入侵检测。潜在侵害分析需要基于一个固定规则集的基本门限检测。

FAU_SAA.1.1 系统应有能力用一系列规则去监测审计事件,并依据这些规则指出对安全策略的潜在侵害。

FAU_SAA.1.2 系统用下列规则来监视审计事件:

根据已知的由可审计安全事件积累或组合对应的安全攻击模式。

7.1.1.6.4 安全审计查阅(FAU_SAR)

7.1.1.6.4.1 审计查阅(FAU_SAR.1)

审计查阅功能提供从审计记录中读取信息的能力。

FAU_SAR.1.1 系统将提供具有查阅审计数据功能的工具,以读取审计记录。

FAU_SAR.1.2 系统将规定准许指定用户按表 6 的形式建立规则查阅某些审计记录。

表 6 端到端安全保障技术要求的可查阅审计记录

用户	可查阅的审计记录
系统审计员	所有对于安全功能的审计记录
系统安全员	所有对于安全功能的审计记录
系统管理员	所有对于系统功能的审计记录

7.1.1.6.4.2 **有限审计查阅**(FAU_SAR.2)

有限审计查阅功能要求除在 FAU_SAR.1 中确定的用户外，其他用户不能读取信息。

FAU_SAR.2.1 除具有明确读访问权限的用户外，系统将禁止所有用户对审计记录的读访问。

7.1.1.6.5 **安全审计事件存储**(FAU_STG)

本条提出创建并维护安全的审计踪迹的要求。

7.1.1.6.5.1 **确保审计数据可用性**(FAU_STG.2)

确保审计数据可用性功能要求审计踪迹应避免未授权的删除或修改，并确保在意外情况出现时审计数据的可用性。

FAU_STG.2.1 系统将保护已储存的审计记录，以避免未授权的删除。

FAU_STG.2.2 系统应能防止对审计记录的修改。

FAU_STG.2.3 当发生审计存储已满、失败或攻击情况时，系统应确保审计记录在一定记录数之内或确定的维护时间范围内不被破坏，这一度量准则由国家行政管理机构统一确定或由证券公司根据需要自行决定。

7.1.1.6.5.2 **防止审计数据丢失**(FAU_STG.4)

防止审计数据丢失功能要求规定当审计踪迹溢满时所采取的行动。

FAU_STG.4.1 如果审计踪迹已满，系统将阻止除由系统审计员产生的以外的所有可审计事件。

7.1.1.7 **安全管理**(FMT)

7.1.1.7.1 **系统中功能的管理**(FMT_MOF)

7.1.1.7.1.1 **安全功能行为的管理**(FMT_MOF.1)

允许授权用户管理系统安全功能。

FMT_MOF.1.1 系统应限定授权用户对是否使用、修改下列安全功能进行决定的能力(如表 7)。

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

类型	安全功能	系统管理员	系统安全员	系统审计员	系统操作员	投资者
审计	审计参数	无	无	配置	备份	无
	审计失败时进行相应操作	维护	无	管理	无	无
	审计项目的更改	无	无	管理	无	无
识别和鉴别	用户账号、角色、属性	无	管理	无	维护	无
	鉴别数据的管理	无	管理	无	无	管理关联数据
	鉴别机制和规则	无	管理	无	无	无
	用户被鉴别前可采取的动作表	无	管理	无	无	无
	对失败的鉴别尝试的阈值及所要采取的动作的管理	无	管理	无	无	无
密码支持	密钥属性的管理	无	管理	无	无	无
	对用于验证及产生秘密的量度的管理	无	管理	无	无	无
安全管理	维护系统中的角色组	维护	管理	无	无	无
	对改变信息类型、域、原发者属性和证据接收者的管理	维护	管理	无	无	无
	定义默认的主体安全属性	无	管理	无	无	无
	为用户组、用户和主体规定某资源的最大使用限度	管理	无	无	无	无

表 7(续)

类型	安全功能	系统管理员	系统安全员	系统审计员	系统操作员	投资者
安全功能的保护	管理数据备份参数	管理	无	无	启动	无
	管理需要可信信道的活动	无	管理	无	无	无
	时间戳	无	管理	无	无	无
	管理支持有效期的安全属性表及过期将采取的动作	无	管理	无	无	无
	多重并发会话的基本限定	无	管理	无	无	无
	管理用于作出访问或拒绝访问决策的属性	无	管理	无	无	无
	选择何时执行剩余信息保护即配给或索回	无	管理	无	无	无
	配置检测到完整性错误时所要采取的动作	无	管理	无	无	无
安全功能的保护	抽象机测试产生的条件及时间间隔的管理	无	管理	无	无	无
	要防止的修改类型的管理	无	管理	无	无	无
	用于输入的附加控制规则	无	管理	无	无	无
	不同部分间数据传输保护机制的管理	无	管理	无	无	无
	可检测出其重放的确定实体列表及须采取的行动列表的管理	无	管理	无	无	无

7.1.1.7.2 **安全属性的管理**(FMT_MSA)

7.1.1.7.2.1 **安全属性的管理**(FMT_MSA.1)

允许授权用户(角色)管理规定的安全属性。

FMT_MSA.1.1 系统安全功能应执行网上访问控制策略及网上信息流控制策略,以限定系统管理员对安全属性进行修改默认值、查询、修改、删除操作的能力。

应用注释:系统的开发者应在与国家行政管理机构协商的基础上提供针对特定系统的详细的授权人员对系统安全属性的管理权限表。举例如表 8。

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

安全属性	系统管理员	系统安全员	系统审计员	系统操作员	投资者
投资者信息及账户	无	管理	无	维护	修改相关数据
审计参数	无	无	配置	无	无
连接属性	管理、配置	无	无	无	无
系统安全角色组	维护	管理	无	无	无
服务优先级	管理	无	无	无	无
访问控制列表	维护	管理	无	无	无

7.1.1.7.2.2 **安全属性确保系统安全**(FMT_MSA.2)

确保赋给安全属性的值使系统处于安全状态。

FMT_MSA.2.1 安全属性的值必须确保系统保密。

7.1.1.7.2.3 **静态属性初始化**(FMT_MSA.3)

确保安全属性中关于允许或限制规定的默认值是适当的。

FMT_MSA.3.1 系统应执行网上访问控制策略及网上信息流控制策略,以便为系统的安全属性

提供限制的默认值。

FMT_MSA.3.2 系统应允许系统管理员为生成的客体或信息规定新的初始值以代替原来的默认值。

7.1.1.7.3 **安全属性的到期**(FMT_SAE)

7.1.1.7.3.1 **时限授权**(FMT_SAE.1)

支持授权用户安全属性的有效期。

FMT_SAE.1.1 系统应提供使系统管理员可规定系统安全属性有效期的能力。

FMT_SAE.1.2 对每个这样的安全属性,系统应能够在指定的安全属性过了有效期后采取规定的行动。

7.1.1.8 **可信路径/通道**(FTP)

7.1.1.8.1 **系统间可信信道**(FTP_ITC)

7.1.1.8.1.1 **系统间可信信道**(FTP_ITC.1)

FTP_ITC.1.1 系统应在它和一远程可信 IT 产品之间提供一条通信信道,它在逻辑上明显不同于其他通信信道,并提供其末点的标识及信道数据保护免遭被修改和泄露。

FTP_ITC.1.2 系统应允许系统内部各组件原发经可信信道的通信。

FTP_ITC.1.3 系统对交易数据原发经可信信道的通信。

FTP_ITC.1.4 整个信道应有同样的可信(如保密)等级,不得中途降低其可信(如保密)等级。

7.1.2 **本地计算安全保障技术要求**

7.1.2.1 **用户数据保护**(FDP)

为保护投资者的资金账户、股票账户、身份、交易指令等敏感信息,网上证券交易系统应具备以下功能。

7.1.2.1.1 **访问控制策略**(FDP_ACC)

7.1.2.1.1.1 **子集访问控制**(FDP_ACC.1)

FDP_ACC.1.1 网上证券交易系统安全功能(以下简称系统安全功能)将对安全功能策略所覆盖的主体、客体和他们之间的操作执行网上证券交易访问控制策略(以下简称网上访问控制策略)。

7.1.2.1.2 **访问控制功能**(FDP_ACF)

7.1.2.1.2.1 **基于安全属性的访问控制**(FDP_ACF.1)

FDP_ACF.1.1 系统安全功能将基于安全属性和确定的安全属性组,对已明确的客体执行网上访问控制策略。

FDP_ACF.1.2 系统安全功能将执行网上访问控制策略,决定受控的主体与客体间的操作是否被允许。

FDP_ACF.1.3 系统安全功能将执行网上访问控制策略,拒绝主体对客体的访问。

应用注释:当用户账号被锁定时,系统所指定的特定实体之外的所有实体(包括用户)都不能使用该账号。只有授权管理员才能解锁该账号(如表 9)。

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

客体	主体				
	投资者	安全管理员	网上委托系统操作人员	柜台操作人员	……
投资者姓名	R,E				
投资者投资账号	R,E,De				
投资者投资账号密码					

表 9(续)

客体	主体				
	投资者	安全管理员	网上委托系统操作人员	柜台操作人员	……
投资者通信密码					
投资者股票持有信息					
投资者股票交易信息					
投资者公开密钥					
投资者私有密钥					
……	……	……	……	……	……
注：R——读；W——写；D——删；E——加密；De——解密。					

7.1.2.1.3 数据鉴别(FDP_DAU)

7.1.2.1.3.1 伴有保证者身份的数据鉴别(FDP_DAU.2)

系统安全功能应具有相应的能力，保证主体的真实身份，并承担信息真实性的责任(如，通过数字签名)，用来保证指定的数据单元的有效性，进而验证静态的信息没有被伪造或篡改。

FDP_DAU.2.1 系统安全功能将提供产生保证客体(详见 FDP_ACF.1)的有效性证据的能力。

FDP_DAU.2.2 系统安全功能将为投资者和券商提供验证网上证券交易有关数据和指令真实有效的证据和产生该证据的真实身份的能力。

7.1.2.1.4 输出到安全功能控制之外(FDP_ETC)

7.1.2.1.4.1 没有安全属性的用户数据输出(FDP_ETC.1)

FDP_ETC.1.1 在安全功能策略控制下输出用户数据到系统安全控制范围之外时，系统安全功能将执行网上访问控制策略和网上证券交易信息流控制策略(以下简称网上信息流控制策略，详见 FDP_IFC.2)

FDP_ETC.1.2 系统应输出不带有相关安全属性的用户数据。

7.1.2.1.4.2 有安全属性的用户数据输出(FDP_ETC.2)

FDP_ETC.2.1 在安全功能策略控制下输出用户数据到系统安全控制范围之外时，系统安全功能将执行网上访问控制策略和网上信息流控制策略。

FDP_ETC.2.2 系统安全功能输出用户数据到系统安全控制范围之外时，应带有与数据相关联的安全属性。

FDP_ETC.2.3 在安全属性输出到系统安全控制范围之外时，系统安全功能应确保其与输出的数据密切关联。

7.1.2.1.5 信息流控制策略(FDP_IFC)

7.1.2.1.5.1 完全信息流控制(FDP_IFC.2)

FDP_IFC.2.1 对已确定的主体、信息流及所有导致信息流入流出安全功能策略覆盖的主体的操作，系统安全功能应执行网上信息流控制策略。

FDP_IFC.2.2 系统安全功能应确保所有导致安全控制范围内的任何信息流入流出安全控制范围内的任何主体的操作被网上信息流控制策略所覆盖(如表 10)。

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

	允许	不允许
投资者到券商	合法的交易指令 未加密的行情查询指令	未经数字签名的交易指令 不符合格式要求的数据包
券商到投资者	经过加密和完整性保护的合法交易结果	未经加密和完整性保护的历史成交记录查询结果
……		

7.1.2.1.6　信息流控制功能(FDP_IFF)

7.1.2.1.6.1　简单安全属性(FDP_IFF.1)

FDP_IFF.1.1　系统安全功能应在主体和最小数目和类型的信息安全属性的基础上执行网上信息流控制策略。

FDP_IFF.1.2　对每一个操作，如果在主体和信息之间必须有基于安全属性的关系，系统安全功能应允许受控主体和受控信息之间存在经由受控操作的信息流。

FDP_IFF.1.5　系统安全功能应根据基于安全属性的规则，明确授权信息流。

FDP_IFF.1.6　系统安全功能应根据基于安全属性的规则，明确拒绝信息流。

7.1.2.1.6.2　无非法信息流(FDP_IFF.5)

FDP_IFF.5.1　系统安全功能应确保没有规避网上信息流控制策略的非法信息流存在。

7.1.2.1.7　从安全功能控制之外输入(FDP_ITC)

7.1.2.1.7.1　有安全属性的用户数据输入(FDP_ITC.2)

此功能要求安全属性能正确反映用户数据，并与从系统安全控制范围之外输入的数据正确无歧义地联系在一起。

FDP_ITC.2.1　在系统安全功能策略控制下，从系统安全控制范围之外输入用户数据时，应执行网上信息流控制策略。

FDP_ITC.2.2　系统安全功能应使用与输入的数据相关联的安全属性。

FDP_ITC.2.3　系统安全功能应确保使用的协议在安全属性和接收的用户数据之间提供明确的联系。

FDP_ITC.2.4　系统安全功能应确保对输入的用户数据的安全属性的解释与用户数据源的解释是一致的。

7.1.2.1.8　残余信息保护(FDP_RIP)

7.1.2.1.8.1　子集残余信息保护(FDP_RIP.1)

要求系统安全功能有能力确保，对于安全控制范围内的某个已定义的客体子集进行资源的配给或回收时，任何资源的任何剩余信息是不可用的，确保已经被删除的信息不再是可访问的。

FDP_RIP.1.1　系统安全功能应确保对客体(详见 FDP_ACC.1)分配或回收资源时，使指定资源的任何以前的信息不再是可用的。

7.1.2.1.9　存储数据的完整性(FDP_SDI)

7.1.2.1.9.1　存储数据完整性监视和行动(FDP_SDI.2)

FDP_SDI.2.1　系统安全功能应基于用户数据属性，监视存储在系统内部的用户数据是否出现完整性错误。

FDP_SDI.2.2　检测到完整性错误时，系统安全功能要采取相应的行动。

7.1.2.1.10　安全功能间用户数据传送保密性保护(FDP_UCT)

7.1.2.1.10.1　基本数据交换保密性(FDP_UCT.1)

FDP_UCT.1.1　系统安全功能应执行网上访问控制策略和网上信息流控制策略，能以防止未授

权泄露的方式传送和接收客体。

7.1.2.1.11 安全功能间用户数据传送完整性保护(FDP_UIT)

7.1.2.1.11.1 数据交换完整性(FDP_UIT.1)

此功能主要解决对被传输的用户数据的篡改、删除、插入和重用等的检测。

FDP_UIT.1.1 系统安全功能应执行网上信息流控制策略,能以避免出现篡改、删除、插入或重用等的方式传送和接收用户数据。

FDP_UIT.1.2 系统安全功能应能根据收到的用户数据判断,是否出现了篡改、删除、插入和重用。

7.1.2.2 标识和鉴别(FIA)

7.1.2.2.1 用户标识(FIA_UID)

7.1.2.2.1.1 用户标识(FIA_UID.1)

FIA_UID.1.1 系统应在用户被识别之前,允许代表用户实施关闭用户标识。

FIA_UID.1.2 系统允许任何代表用户启动安全功能之前,要求每个用户都被成功识别。

7.1.2.2.2 用户属性定义(FIA_ATD)

7.1.2.2.2.1 用户属性定义(FIA_ATD.1)

FIA_ATD.1.1 系统应为每一个用户保存属于他的安全属性表:用户权限及属性。

7.1.2.2.3 秘密的规范(FIA_SOS)

7.1.2.2.3.1 秘密的验证(FIA_SOS.1)

FIA_SOS.1.1 系统应提供一种机制以证明秘密(如口令字长度及字符集)满足规定的强度。

7.1.2.2.3.2 秘密的 TSF 生成(FIA_SOS.2)

FIA_SOS.2.1 系统应提供一种机制以产生满足规定的强度。

FIA_SOS.2.2 系统应能够为用户身份鉴别使用系统产生的秘密。

7.1.2.2.4 用户鉴别(FIA_UAU)

7.1.2.2.4.1 用户标识(FIA_UAU.1)

FIA_UAU.1.1 系统应在用户被鉴别之前允许代表用户请求系统证书。

FIA_UAU.1.2 系统在允许任何代表用户启动安全功能之前,要求每个用户都被成功鉴别。

7.1.2.2.4.2 不可伪造的鉴别(FIA_UAU.3)

FIA_UAU.3.1 系统应检测任何用户伪造的和正在系统中使用的鉴别数据。

FIA_UAU.3.2 系统应检测从任何其他用户复制的和正在系统中使用的鉴别数据。

7.1.2.2.4.3 多重鉴别机制(FIA_UAU.5)

FIA_UAU.5.1 系统应提供口令、证书机制以支持用户鉴别。

FIA_UAU.5.2 系统应根据口令、证书鉴别任何用户所声称的身份。

7.1.2.2.4.4 重鉴别(FIA_UAU.6)

FIA_UAU.6.1 系统应在下列条件下重新鉴别用户:交易请求失败后,及其他重鉴别条件。

7.1.2.2.4.5 受保护的鉴别反馈(FIA_UAU.7)

FIA_UAU.7.1 当鉴别在进行时,系统应仅仅将鉴别是否成功反馈给用户。

7.1.2.2.5 鉴别失败(FIA_AFL)

7.1.2.2.5.1 鉴别失败处理(FIA_AFL.1)

FIA_AFL.1.1 系统应检测何时与交易申请鉴别相关的不成功鉴别尝试达到门限值。

FIA_AFL.1.2 当达到或超过定义了的不成功鉴别尝试的次数时,系统将拒绝交易并记录。

7.1.2.2.6 用户—主体绑定(FIA_USB)

7.1.2.2.6.1 用户—主体绑定(FIA_USB.1)

FIA_USB.1.1 系统将把合适的用户安全属性关联到代表用户活动的主体上。

7.1.2.3 抗抵赖(FCO)

7.1.2.3.1 原发抗抵赖(FCO_NRO)

7.1.2.3.1.1 强制原发证明(FCO_NRO.2)

FCO_NRO.2.1 系统在任何时候都将对交易数据强制产生原发证据。

FCO_NRO.2.2 系统应能将信息原发者的身份与适用于证据的信息数字签名和证书相关联。

FCO_NRO.2.3 系统应能为给定证书、数字签名的接收者、相关检查部门提供验证信息原发证据的能力。

7.1.2.3.2 接收抗抵赖(FCO_NRR)

7.1.2.3.2.1 强制接收证明(FCO_NRR.2)

FCO_NRR.2.1 系统对收到的交易数据强制产生接收证据。

FCO_NRR.2.2 系统应能将信息收信者的身份与适用于证据的信息数字签名和证书相关联。

FCO_NRR.2.3 系统应能为给定数字签名、证书接收者、相关检查部门提供验证接收证据的能力。

7.1.2.4 密码支持(FCS)

系统可以利用密码功能来满足一些高级安全目的。这些功能包括:标识与鉴别、抗抵赖,可信信道和数据分离等。可用硬件、固件和/或软件来实现,在系统执行密码功能时使用。密码支持要求包括对密钥管理和密码运算方面的要求。

7.1.2.4.1 密钥管理(FCS_CKM)

密钥在其整个生存期内都必须进行管理。本条定义了以下几种管理功能:密钥产生、密钥分配、密钥访问和密钥销毁。如使用PKI体系,用于加密的密钥对和加密证书与用于签名的密钥对和签名证书应分开,不得使用同一密钥对和证书进行签名和加密。

7.1.2.4.1.1 密钥产生(FCS_CKM.1)

密钥产生功能要求以基于某个指定标准的特定的算法和密钥长度来产生密钥。

FCS_CKM.1.1 系统将以符合标准要求的特定密钥产生算法和密钥长度来产生密钥。

应用注释:对称密钥产生器所产生的密钥应使每个密钥产生的概率独立等概,并通过最长连长、"0""1"概率分布、扑克检验和连长检验等随机性检验。公开密钥产生器应证明产生的素数确为素数,且每个素数独立等概。

7.1.2.4.1.2 密钥分配(FCS_CKM.2)

密钥分配功能要求以基于某个指定标准的特定的分配方法来分配密钥。

FCS_CKM.2.1 系统可采用公钥体制的密钥分配方法来分配密钥。

7.1.2.4.1.3 密钥访问(FCS_CKM.3)

密钥访问功能要求根据基于某个指定标准的特定的访问方法来访问密钥。

FCS_CKM.3.1 系统应规定密钥访问规则,并依此来控制对密钥的访问。

7.1.2.4.1.4 密钥销毁(FCS_CKM.4)

密钥销毁功能要求以基于某个指定标准的特定的销毁方法来销毁密钥。

FCS_CKM.4.1 系统应根据符合标准的密钥管理规范中特定的密钥销毁方法来销毁密钥。

7.1.2.4.2 密码运算(FCS_COP)

7.1.2.4.2.1 密码运算(FCS_COP.1)

为了保证密码运算的功能正确,必须按照特定的算法和一定长度的密钥来运算。密码运算包括:数据加密和/或解密、数字签名产生和/或验证、针对完整性的密码校验和产生和/或检验、保密散列(信息摘要)、密钥加密和/或解密,以及密钥协商等。

FCS_COP.1.1 系统将以符合规定标准要求的特定密钥产生算法和密钥长度来执行特定密码运算。

7.1.2.5 安全功能保护(FPT)

7.1.2.5.1 抽象机测试(FPT_AMT)

7.1.2.5.1.1 抽象机测试(FPT_AMT.1)

抽象机测试提供了对根本的抽象机的测试。

FPT_AMT.1.1 网上证券交易系统应在初始化启动期间或定期运行一套测试,来验证由安全功能基于的抽象机所提供的安全假设都正确执行了。

7.1.2.5.2 失败保护(FPT_FLS)

7.1.2.5.2.1 带维持安全状态的失败(FPT_FLS.1)

当确定的失败出现时,要求网上证券交易系统维持一种安全状态。

FPT_FLS.1.1 网上证券交易系统在发生鉴别和通信失败时应维持一种安全状态。

7.1.2.5.3 安全功能数据输出的保密性(FPT_ITC)

7.1.2.5.3.1 传输过程中安全功能间的保密性(FPT_ITC.1)

要求系统安全功能确保安全功能数据在系统与远程可信 IT 产品间的传输不被泄露。

FPT_ITC.1.1 网上证券交易系统应保护所有的安全功能数据从系统到远程可信 IT 产品的传输过程中不被未经授权的泄密。

7.1.2.5.4 安全功能数据输出的完整性(FPT_ITI)

7.1.2.5.4.1 安全功能间的修改检测(FPT_ITI.1)

提供在远程可信 IT 被产品知道所使用的机制的假设下,检测安全功能数据在系统与远程可信 IT 产品传输过程中修改的能力。

FPT_ITI.1.1 网上证券交易系统应能够检测系统与远程可信 IT 产品间传输的所有安全功能数据的修改。

FPT_ITI.1.2 应验证在系统与远程可信 IT 产品间传输的所有安全功能数据的完整性,如果检测到数据修改时应及时通知数据的拥有者。

7.1.2.5.5 系统内部安全功能数据传输(FPT_ITT)

7.1.2.5.5.1 系统内部安全功能数据传输的基本保护(FPT_ITT.1)

要求对网上证券交易系统的分离部分间传输的安全功能数据进行保护。

FPT_ITT.1.1 在网上证券交易系统的各个部分间传输安全功能数据时,应保护其不被泄漏。

7.1.2.5.6 可信恢复(FPT_RCV)

7.1.2.5.6.1 手工恢复(FPT_RCV.1)

容许网上证券交易系统只提供人工干预以返回安全状态的机制。

FPT_RCV.1.1 发生故障或服务中断后,系统安全功能应进入维护方式,该方式提供将系统返回到一个安全状态的能力。

7.1.2.5.7 重放检测(FPT_RPL)

7.1.2.5.7.1 重放检测(FPT_RPL.1)

要求网上证券交易系统能够检测出鉴别数据和交易委托数据的重放。

FPT_RPL.1.1 网上证券交易系统应能检测鉴别数据和交易委托数据的重放;

FPT_RPL.1.2 检测到重放时,系统应及时通知系统管理员。

7.1.2.5.8 参照仲裁(FPT_RVM)

7.1.2.5.8.1 安全策略的不可旁路性(FPT_RVM.1)

要求安全功能控制范围内的每一项功能都不可旁路。

FPT_RVM.1.1 应确保继续执行在安全功能控制范围内的每一项功能前,安全策略的强制执行功能都已成功激活。

7.1.2.5.9 安全功能域分离(FPT_SEP)

7.1.2.5.9.1 安全功能域分离(FPT_SEP.1)

为安全功能提供不同的保护域,并在安全功能控制范围内客体分离之间提供。

FPT_SEP.1.1 安全功能应为自身的执行维护一个安全域,防止不可信主体的干扰和篡改。

FPT_SEP.1.2 安全功能应在其控制范围内主体的安全域之间强行分离。

7.1.2.5.10 状态同步协议(FPT_SSP)

7.1.2.5.10.1 相互的可信回执(FPT_SSP.2)

本组件要求对交换安全功能数据相互回执。

FPT_SSP.2.1 当网上证券交易系统的一部分发出需要回执请求时,与其通信的另一部分应在接收到未经修改的安全功能数据时给予回执。

FPT_SSP.2.2 系统安全功能应通过使用回执,来确保系统管理部分知道在各部分间所传输的安全功能数据都处于正确状态。

7.1.2.5.11 时间戳(FPT_STM)

7.1.2.5.11.1 可靠的时间戳(FPT_STM.1)

本组件要求系统安全功能为自身提供可靠的时间戳。

FPT_STM.1.1 网上证券交易系统的安全功能应能为自身的应用提供可靠的时间戳。

7.1.2.5.12 系统安全功能间安全功能数据的一致性(FPT_TDC)

7.1.2.5.12.1 系统安全功能间基本安全功能数据的一致性(FPT_TDC.1)

本组件要求网上证券交易系统提供确保安全功能间属性的一致性的能力。

FPT_TDC.1.1 当网上证券交易系统与别的可信IT产品共享安全功能数据时,系统应能够判断所有安全功能数据的一致性。

FPT_TDC.1.2 当判断来自别的可信IT产品的安全功能数据时,系统应使用预先大家所协定的一组规则。

7.1.2.5.13 安全功能自检(FPT_TST)

7.1.2.5.13.1 安全功能测试(FPT_TST.1)

本组件提供对系统安全功能正确操作的测试能力。这些测试可在启动时进行,或周期性地进行,或当授权用户要求时或满足别的条件时进行。同时也提供对安全功能数据及可执行码的完整性的验证能力。

FPT_TST.1.1 系统安全功能在每次启动时或定期运行一套自检以验证安全功能的正确操作。

FPT_TST.1.2 系统安全功能为授权用户提供了验证安全功能数据完整性的能力。

FPT_TST.1.3 系统安全功能为授权用户提供了验证所存储的安全功能可执行码完整性的能力。

7.1.2.6 系统访问(FTA)

7.1.2.6.1 多重并发会话限定(FTA_MCS)

7.1.2.6.1.1 多重并发会话的基本限定(FTA_MCS.1)

提供适用于系统内所有用户的限制。

FTA_MCS.1.1 系统应限定并发会话的最大数目。

FTA_MCS.1.2 系统应利用缺省值执行最高并发会话次数的限定。

系统开发者应提供最大会话次数的具体数值。

7.1.2.6.2 系统访问历史(FTA_TAH)

7.1.2.6.2.1 系统访问历史(FTA_TAH.1)

提供系统显示与先前建立的会话相关的信息的要求。

FTA_TAH.1.1 在会话成功建立的基础上,系统应显示用户上一次成功的会话建立的日期、时间、方法。

FTA_TAH.1.2 在会话成功建立的基础上，系统应显示用户的上一次不成功的会话建立的尝试的日期、时间、方法、位置和从上一次成功的会话建立以来的不成功的尝试的次数。

FTA_TAH.1.3 系统在没有给用户回顾访问历史信息的机会的情况下是不能从用户界面上抹去该信息的。

7.1.2.7 **安全审计**(FAU)

安全审计包括产生、记录、存储和分析那些与安全相关活动有关的信息。审计记录结果可用来检测、判断发生了哪些安全相关活动以及这些活动是由哪个用户负责的。

7.1.2.7.1 **安全审计自动响应**(FAU_ARP)

7.1.2.7.1.1 **安全警告**(FAU_ARP.1)

安全警告功能描述了当检测到可能的安全侵害时，系统将采取的行动，包括报警或系统自动响应。

FAU_ARP.1.1 当检测到潜在的安全侵害时，系统将通知授权管理员，使产生潜在安全侵害的主体失效，或采取其他由授权管理员确定的行动。

例如，系统安全功能能够生成实时报警、终止违例进程、取消服务、或断开用户账号以及使用户账号失效等。

应用注释：如果一个审计事件由 FAU_SAA 组件指出，那么这个事件将被定义为是“潜在的安全侵害事件”。

7.1.2.7.2 **安全审计数据产生**(FAU_GEN)

本节要求发生安全相关事件时应记录其出现，列举出网上证券系统可审计的事件类型，以及应在各审计记录内提供的审计相关信息的最小集合。

7.1.2.7.2.1 **审计数据产生**(FAU_GEN.1)

网上证券系统的审计数据产生功能只产生最小级审计事件记录，并规定进行每项记录的数据表。

FAU_GEN.1.1 系统应能为下述可审计事件产生审计记录：

a) 审计功能的启动和关闭；

b) 所有最小级的可审计事件；

c) 其他专门定义的可审计事件由证券公司自行定义。

FAU_GEN.1.2 系统将在每个审计记录中至少记录如下信息：

a) 事件的日期和时间，事件类型，主体身份，事件的结果(成功或失败)；

b) 最小级可审计事件类型见表 11；

c) 专门定义的可审计事件清单由开发者列于表 11 的第四栏。

表 11 本地计算安全保障技术要求的可审计安全事件类型

组件标识	审计级别	可审计事件	专门定义的审计事件
FAU_ARP.1	最小级	当即将发生安全侵害时采取的行动。	
FAU_SAA.1	最小级	开启和关闭任何分析机制。 由工具完成的自动响应。	
FCO_NRO.2	最小级	调用抗抵赖服务。	
FCO_NRR.2	最小级	调用抗抵赖服务。	
FDP_ACF.1	最小级	成功的请求对某个被安全功能策略覆盖的客体上执行某操作。	
FDP_DAU.2	最小级	成功的产生有效证据。	
FDP_ETC.1	最小级	成功的信息输出。	

表 11(续)

组件标识	审计级别	可审计事件	专门定义的审计事件
FDP_ETC. 2	最小级	成功的信息输出。	
FDP_IFF. 1	最小级	判定允许请求的信息流。	
FDP_IFF. 5	最小级	判定允许请求的信息流。	
FDP_ITC. 2	最小级	成功输入用户数据,包括任何安全属性。	
FDP_SDI. 2	最小级	成功尝试检测用户数据的完整性,包括指示检测结果。	
FDP_UCT. 1	最小级	使用数据交换机制的任何用户或主体的身份。	
FDP_UIT. 1	最小级	使用数据交换机制的任何用户或主体的身份。	
FIA_AFL. 1	最小级	获取失败鉴别的阈值和采取的动作(如,使终端无效),及随后,还原到正常状态(如,重新使终端有效)。	
FIA_SOS. 1	最小级	安全功能拒绝任何测试的秘密。	
FIA_SOS. 2	最小级	安全功能拒绝任何测试的秘密。	
FIA_UAU. 1	最小级	使用鉴别机制失败。	
FIA_UAU. 3	最小级	检测欺骗性的鉴别数据。	
FIA_UAU. 5	最小级	鉴别的最后判定。	
FIA_UAU. 6	最小级	重鉴别失败。	
FIA_UID. 1	最小级	使用用户标识机制失败,包括提供的用户身份。	
FIA_USB. 1	最小级	绑定用户安全属性到一个主体失败(如,产生一个主体)。	
FMT_MOF. 1	最小级	系统安全功能的所有改动。	
FMT_MSA. 2	最小级	对某安全属性,所有提供的和被拒绝的值。	
FMT_SMR. 1	最小级	对角色一部分的用户组的改动。	
FMT_SMR. 3	最小级	明确请求担任某角色。	
FPT_ITI. 1	最小级	检测传输的安全功能数据的修改。	
FPT_RCV. 1	最小级	出现失败或服务中断。 恢复正常运行。	
FPT_SSP. 2	最小级	接收期待的回执时,发生失败。	
FPT_STM. 1	最小级	时间的变动。	
FPT_TDC. 1	最小级	成功使用安全功能数据一致性机制。	
FRU_FLT. 1	最小级	安全功能检测出的任何故障。	
FRU_RSA. 1	最小级	因资源的限制对分配操作的拒绝。	
FTA_MCS. 1	最小级	基于多重并发会话限定对新会话的拒绝。	
FTP_ITC. 1	最小级	可信信道功能故障。 失败的可信信道功能的原发者及目标的标识。	

7.1.2.7.2.2 **用户身份关联**(FAU_GEN.2)

该功能解决可审计事件追溯到单个用户身份上的要求。

FAU_GEN.2.1 系统能将每个可审计事件与引起该事件的用户身份相关联。

7.1.2.7.3 **安全审计分析**(FAU_SAA)

7.1.2.7.3.1 **潜在侵害分析**(FAU_SAA.1)

本功能提出为寻找可能的或真正的安全侵害,用来分析系统活动和审计数据的自动化措施的要求,这种分析可用于支持入侵检测。潜在侵害分析需要基于一个固定规则集的基本门限检测。

FAU_SAA.1.1 系统应有能力用一系列规则去监测审计事件,并依据这些规则指出对安全策略的潜在侵害。

FAU_SAA.1.2 系统用下列规则来监视审计事件:

a) 根据已知的由可审计安全事件积累或组合对应的安全攻击模式。

注:由于系统使用商用操作系统,建议使用入侵检测安全产品。

7.1.2.7.4 **安全审计查阅**(FAU_SAR)

7.1.2.7.4.1 **审计查阅**(FAU_SAR.1)

审计查阅功能提供从审计记录中读取信息的能力。

FAU_SAR.1.1 系统将提供具有查阅审计数据功能的工具,以读取审计记录。

FAU_SAR.1.2 系统将规定准许指定用户按表12的形式建立规则查阅某些审计记录。

表12 本地计算安全保障技术要求的可查阅审计记录

用户	可查阅的审计记录
系统审计员	所有对于安全功能的审计记录
系统安全员	所有对于安全功能的审计记录
系统管理员	所有对于系统功能的审计记录

7.1.2.7.4.2 **有限审计查阅**(FAU_SAR.2)

有限审计查阅功能要求除在FAU_SAR.1中确定的用户外,其他用户不能读取信息。

FAU_SAR.2.1 除具有明确读访问权限的用户外,系统将禁止所有用户对审计记录的读访问。

7.1.2.7.5 **安全审计事件存储**(FAU_STG)

本条提出创建并维护安全的审计踪迹的要求。

7.1.2.7.5.1 **确保审计数据可用性**(FAU_STG.2)

确保审计数据可用性功能要求审计踪迹应避免未授权的删除和/或修改,并确保在意外情况出现时审计数据的可用性。

FAU_STG.2.1 系统将保护已储存的审计记录,以避免未授权的删除。

FAU_STG.2.2 系统应能防止对审计记录的修改。

FAU_STG.2.3 当发生审计存储已满、失败或攻击情况时,系统应确保审计记录在一定记录数之内或确定的维护时间范围内不被破坏,这一度量准则由国家行政管理机构统一确定或由证券公司根据需要自行决定。

7.1.2.7.5.2 **防止审计数据丢失**(FAU_STG.4)

防止审计数据丢失功能要求规定当审计踪迹溢满时所采取的行动。

FAU_STG.4.1 如果审计踪迹已满,系统将阻止除由系统审计员产生的以外的所有可审计事件。

7.1.2.8 **安全管理**(FMT)

7.1.2.8.1 **系统中功能的管理**(FMT_MOF)

7.1.2.8.1.1 **安全功能行为的管理**(FMT_MOF.1)

允许授权用户管理系统安全功能。

FMT_MOF.1.1 系统应限定授权用户对是否使用、修改下列安全功能进行决定的能力(见表13)。

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

类型	安全功能	系统管理员	系统安全员	系统审计员	系统操作员	投资者
审计	审计参数	无	无	配置	备份	无
	审计失败时进行相应操作	维护	无	管理	无	无
	审计项目的更改	无	无	管理	无	无
识别和鉴别	用户账号、角色、属性	无	管理	无	维护	无
	鉴别数据的管理	无	管理	无	无	管理关联数据
	鉴别机制和规则	无	管理	无	无	无
	用户被鉴别前可采取的动作表	无	管理	无	无	无
	对失败的鉴别尝试的阈值及所要采取的动作的管理	无	管理	无	无	无
密码支持	密钥属性的管理	无	管理	无	无	无
	对用于验证及产生秘密的量度的管理	无	管理	无	无	无
安全管理	维护系统中的角色组	维护	管理	无	无	无
	对改变信息类型、域、原发者属性和证据接收者的管理	维护	管理	无	无	无
	定义默认的主体安全属性	无	管理	无	无	无
	为用户组、用户和主体规定某资源的最大使用限度	管理	无	无	无	无
安全功能的保护	管理数据备份参数	管理	无	无	启动	无
	管理需要可信信道的活动	无	管理	无	无	无
	时间戳	无	管理	无	无	无
	管理支持有效期的安全属性表及过期将采取的动作	无	管理	无	无	无
	多重并发会话的基本限定	无	管理	无	无	无
	管理用于作出访问或拒绝访问决策的属性	无	管理	无	无	无
	选择何时执行剩余信息保护即配给或索回	无	管理	无	无	无
	配置检测到完整性错误时所要采取的动作	无	管理	无	无	无
	抽象机测试产生的条件及时间间隔的管理	无	管理	无	无	无
	要防止的修改类型的管理	无	管理	无	无	无
	用于输入的附加控制规则	无	管理	无	无	无
	不同部分间数据传输保护机制的管理	无	管理	无	无	无
	可检测出其重放的确定实体列表及须采取的行动列表的管理	无	管理	无	无	无

7.1.2.8.2　安全属性的管理(FMT_MSA)

7.1.2.8.2.1　安全属性的管理(FMT_MSA.1)

允许授权用户(角色)管理规定的安全属性。

FMT_MSA.1.1　系统安全功能应执行网上访问控制策略及网上信息流控制策略，以限定系统管

理员对安全属性进行修改默认值、查询、修改、删除操作的能力。

应用注释：系统的开发者应在与国家行政管理机构协商的基础上提供针对特定系统的详细的授权人员对系统安全属性的管理权限表。举例如表14。

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

安全属性	系统管理员	系统安全员	系统审计员	系统操作员	投资者
投资者信息及账户	无	管理	无	维护	修改相关数据
审计参数	无	无	配置	无	无
连接属性	管理、配置	无	无	无	无
系统安全角色组	维护	管理	无	无	无
服务优先级	管理	无	无	无	无
访问控制列表	维护	管理	无	无	无

7.1.2.8.2.2 **安全属性确保系统安全**(FMT_MSA.2)

确保赋给安全属性的值使系统处于安全状态。

FMT_MSA.2.1 安全属性的值必须确保系统保密。

7.1.2.8.2.3 **静态属性初始化**(FMT_MSA.3)

确保安全属性中关于允许或限制规定的默认值是适当的。

FMT_MSA.3.1 系统应执行网上访问控制策略及网上信息流控制策略，以便为系统的安全属性提供限制的默认值。

FMT_MSA.3.2 系统应允许系统管理员为生成的客体或信息规定新的初始值以代替原来的默认值。

7.1.2.8.3 **系统数据的管理**(FMT_MTD)

7.1.2.8.3.1 **安全功能数据的管理**(FMT_MTD.1)

允许授权用户管理系统安全数据。

FMT_MTD.1.1 安全功能应限定授权用户对下列系统数据进行改变默认值、查询、修改、删除、清空等操作的权力。

应用注释：系统开发者应在与国家行政管理机构协商的基础上给出系统安全角色对系统安全数据的操作权限表。举例如表15。

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

	系统管理员	系统安全员	系统审计员	系统操作员	投资者
系统配置	改变默认值、修改	无	无	备份、恢复	无
审计数据	无	无	配置、查看、删除	备份、恢复	无
系统参数	创建、修改	无	无	备份、恢复	无
控制审计存储能力的参数	参数设置、维护	无	无	无	无
鉴别数据及其参数	无	管理	无	维护	本账户关联数据的修改
用户信息及账号	创建	管理	无	维护	本账户关联数据的修改

7.1.2.8.4 安全属性的到期(FMT_SAE)

7.1.2.8.4.1 时限授权(FMT_SAE.1)

支持授权用户安全属性的有效期。

FMT_SAE.1.1 系统应提供使系统管理员可规定系统安全属性有效期的能力。

FMT_SAE.1.2 对每个这样的安全属性,系统应能够在指定的安全属性过了有效期后采取规定的行动。

7.1.2.8.5 安全管理角色(FMT_SMR)

7.1.2.8.5.1 安全角色(FMT_SMR.1)

规定系统认可的安全功能相关的角色。为了保证网上证券交易系统的安全,将系统的安全功能分配给不同的角色执行。下面给出了本标准中安全管理所使用角色的定义。实际系统中,不一定使用所有这些角色,但必须实现对安全角色的区分。为保证网上证券交易系统的安全,不可将系统管理员、系统审计员和系统维护员的职责分配给同一人担任。

系统角色定义如下:

系统管理员:授权对系统进行建立、配置、维护;对用户账号进行创建、维护的人员。

系统安全员:管理系统安全相关功能的人员。

系统审计员:授权进行审计日志查看与维护的人员。

系统操作员:系统日常操作工作的人员,负责授权进行系统日常维护及备份与恢复的人员。

投资者:网上交易的使用者。

FMT_SMR.1.1 系统应维护系统管理员和系统审计员。

FMT_SMR.1.2 系统应能够把用户和角色关联起来。

7.1.2.8.5.2 担任角色(FMT_SMR.3)

要求向系统明确请求担任某个角色。

FMT_SMR.3.1 系统应要求担任系统管理员和系统审计员的人员须正式明确请求。

7.1.2.9 可信路径/通道(FTP)

7.1.2.9.1 系统间可信信道(FTP_ITC)

7.1.2.9.1.1 系统间可信信道(FTP_ITC.1)

FTP_ITC.1.1 系统应在它和一远程可信 IT 产品之间提供一条通信信道,它在逻辑上明显不同于其他通信信道,并提供其末点的标识及信道数据保护免遭被修改和泄露。

FTP_ITC.1.2 系统应允许系统内部各组件原发经可信信道的通信。

FTP_ITC.1.3 系统对交易数据原发经可信信道的通信。

FTP_ITC.1.4 整个信道应有同样的可信(如保密)等级,不得中途降低其可信(如保密)等级。

7.1.2.10 资源利用(FRU)

7.1.2.10.1 容错(FRU_FLT)

7.1.2.10.1.1 降低容错(FRU_FLT.1)

FRU_FLT.1.1 系统应确保当互联网故障发生时,不会导致错误交易。

FRU_FLT.1.1 当系统采用多台服务器作热备份时,服务器的身份应采用较高的识别和鉴别机制互相鉴别身份。

7.1.2.10.2 资源分配(FRU_RSA)

7.1.2.10.2.1 最高配额(FRU_RSA.1)

FRU_RSA.1.1 系统应定义以下资源:交易和行情系统的用户数量的最高配额,这些资源是定义的用户能同时使用的。

7.1.3 系统的边界安全保障技术要求

7.1.3.1 用户数据保护(FDP)

7.1.3.1.1 访问控制策略(FDP_ACC)

7.1.3.1.1.1 子集访问控制(FDP_ACC.1)

FDP_ACC.1.1 网上证券交易系统安全功能(以下简称系统安全功能)将对安全功能策略所覆盖的主体、客体和它们之间的操作执行网上证券交易访问控制策略(以下简称网上访问控制策略)。

7.1.3.1.2 访问控制功能(FDP_ACF)

7.1.3.1.2.1 基于安全属性的访问控制(FDP_ACF.1)

FDP_ACF.1.1 系统安全功能将基于安全属性和确定的安全属性组,对已明确的客体执行网上访问控制策略。

FDP_ACF.1.2 系统安全功能将执行网上访问控制策略,决定受控的主体与客体间的操作是否被允许。

FDP_ACF.1.3 系统安全功能将执行网上访问控制策略,拒绝主体对客体的访问。

应用注释:当用户账号被锁定时,系统所指定的特定实体之外的所有实体(包括用户)都不能使用该账号。只有授权管理员才能解锁该账号(如表16)。

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

客体	主体				
	投资者	安全管理员	网上委托系统操作人员	柜台操作人员	……
投资者姓名	R,E				
投资者投资账号	R,E,De				
投资者投资账号密码					
投资者通信密码					
投资者股票持有信息					
投资者股票交易信息					
投资者公开密钥					
投资者私有密钥					
……	……	……	……	……	……
注:R——读;W——写;D——删;E——加密;De——解密。					

7.1.3.1.3 输出到安全功能控制之外(FDP_ETC)

7.1.3.1.3.1 没有安全属性的用户数据输出(FDP_ETC.1)

FDP_ETC.1.1 在安全功能策略控制下输出用户数据到系统安全控制范围之外时,系统安全功能将执行网上访问控制策略和网上证券交易信息流控制策略(以下简称网上信息流控制策略,详见FDP_IFC.2)。

FDP_ETC.1.2 系统应输出不带有相关安全属性的用户数据。

7.1.3.1.3.2 有安全属性的用户数据输出(FDP_ETC.2)

FDP_ETC.2.1 在安全功能策略控制下输出用户数据到系统安全控制范围之外时,系统安全功能将执行网上访问控制策略和网上信息流控制策略。

FDP_ETC.2.2 系统安全功能输出用户数据到系统安全控制范围之外时,应带有与数据相关联的安全属性。

FDP_ETC.2.3 在安全属性输出到系统安全控制范围之外时,系统安全功能应确保其与输出的数据密切关联。

7.1.3.1.4 信息流控制策略(FDP_IFC)

7.1.3.1.4.1 完全信息流控制(FDP_IFC.2)

FDP_IFC.2.1 对已确定的主体、信息流及所有导致信息流入流出安全功能策略覆盖的主体的操作,系统安全功能应执行网上信息流控制策略。

FDP_IFC.2.2 系统安全功能应确保所有导致安全控制范围内的任何信息流入流出安全控制范围内的任何主体的操作被网上信息流控制策略所覆盖(如表17)。

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

	允许	不允许
投资者到券商	合法的交易指令 未加密的行情查询指令	未经数字签名的交易指令 不符合格式要求的数据包
券商到投资者	经过加密和完整性保护的合法交易结果	未经加密和完整性保护的历史成交记录查询结果
……		

7.1.3.1.5 信息流控制功能(FDP_IFF)

7.1.3.1.5.1 简单安全属性(FDP_IFF.1)

FDP_IFF.1.1 系统安全功能应在主体和最小数目和类型的信息安全属性的基础上执行网上信息流控制策略。

FDP_IFF.1.2 对每一个操作,如果在主体和信息之间必须有基于安全属性的关系,系统安全功能应允许受控主体和受控信息之间存在经由受控操作的信息流。

FDP_IFF.1.5 系统安全功能应根据基于安全属性的规则,明确授权信息流。

FDP_IFF.1.6 系统安全功能应根据基于安全属性的规则,明确拒绝信息流。

7.1.3.1.5.2 无非法信息流(FDP_IFF.5)

FDP_IFF.5.1 系统安全功能应确保没有规避网上信息流控制策略的非法信息流存在。

7.1.3.1.6 从安全功能控制之外输入(FDP_ITC)

7.1.3.1.6.1 有安全属性的用户数据输入(FDP_ITC.2)

此功能要求安全属性能正确反映用户数据,并与从系统安全控制范围之外输入的数据正确无歧义地联系在一起。

FDP_ITC.2.1 在系统安全功能策略控制下,从系统安全控制范围之外输入用户数据时,应执行网上信息流控制策略。

FDP_ITC.2.2 系统安全功能应使用与输入的数据相关联的安全属性。

FDP_ITC.2.3 系统安全功能应确保使用的协议在安全属性和接收的用户数据之间提供明确的联系。

FDP_ITC.2.4 系统安全功能应确保对输入的用户数据的安全属性的解释与用户数据源的解释是一致的。

7.1.3.1.7 存储数据的完整性(FDP_SDI)

7.1.3.1.7.1 存储数据完整性监视和行动(FDP_SDI.2)

FDP_SDI.2.1 系统安全功能应基于用户数据属性,监视存储在系统内部的用户数据是否出现完整性错误。

FDP_SDI.2.1 检测到完整性错误时,系统安全功能应要采取相应的行动。

7.1.3.1.8 安全功能间用户数据传送保密性保护(FDP_UCT)

7.1.3.1.8.1 基本数据交换保密性(FDP_UCT.1)

FDP_UCT.1.1 系统安全功能应执行网上访问控制策略和网上信息流控制策略,能以防止未授

权泄露的方式传送和接收客体。

7.1.3.1.9 安全功能间用户数据传送完整性保护(FDP_UIT)

7.1.3.1.9.1 数据交换完整性(FDP_UIT.1)

此功能主要解决对被传输的用户数据的篡改、删除、插入和重用等的检测。

FDP_UIT.1.1 系统安全功能应执行网上信息流控制策略,能以避免出现篡改、删除、插入或重用等的方式传送和接收用户数据。

FDP_UIT.1.2 系统安全功能应能根据收到的用户数据判断,是否出现了篡改、删除、插入和重用。

7.1.3.2 安全功能保护(FPT)

7.1.3.2.1 安全功能数据输出的保密性(FPT_ITC)

7.1.3.2.1.1 传输过程中安全功能间的保密性(FPT_ITC.1)

要求系统安全功能确保安全功能数据在系统与远程可信 IT 产品间的传输不被泄露。

FPT_ITC.1.1 网上证券交易系统应保护所有的安全功能数据从系统到远程可信 IT 产品的传输过程中不被未经授权的泄密。

7.1.3.2.2 安全功能数据输出的完整性(FPT_ITI)

7.1.3.2.2.1 安全功能间的修改检测(FPT_ITI.1)

提供在远程可信 IT 被产品知道所使用的机制的假设下,检测安全功能数据在系统与远程可信 IT 产品传输过程中修改的能力。

FPT_ITI.1.1 网上证券交易系统应能够检测系统与远程可信 IT 产品间传输的所有安全功能数据的修改。

FPT_ITI.1.2 应验证在系统与远程可信 IT 产品间传输的所有安全功能数据的完整性,如果检测到数据修改时应及时通知数据的拥有者。

7.1.3.2.3 系统内部安全功能数据传输(FPT_ITT)

7.1.3.2.3.1 系统内部安全功能数据传输的基本保护(FPT_ITT.1)

要求对网上证券交易系统的分离部分间传输的安全功能数据进行保护。

FPT_ITT.1.1 在网上证券交易系统的各个部分间传输安全功能数据时,应保护其不被泄漏。

7.1.3.2.4 重放检测(FPT_RPL)

7.1.3.2.4.1 重放检测(FPT_RPL.1)

要求网上证券交易系统能够检测出鉴别数据和交易委托数据的重放。

FPT_RPL.1.1 网上证券交易系统应能检测鉴别数据和交易委托数据的重放。

FPT_RPL.1.2 检测到重放时,系统应及时通知系统管理员。

7.1.3.2.5 参照仲裁(FPT_RVM)

7.1.3.2.5.1 安全策略的不可旁路性(FPT_RVM.1)

要求安全功能控制范围内的每一项功能都不可旁路。

FPT_RVM.1.1 应确保继续执行在安全功能控制范围内的每一项功能前,安全策略的强制执行功能都已成功激活。

7.1.3.2.6 安全功能域分离(FPT_SEP)

7.1.3.2.6.1 安全功能域分离(FPT_SEP.1)

为安全功能提供不同的保护域,并在安全功能控制范围内客体分离之间提供。

FPT_SEP.1.1 安全功能应为自身的执行维护一个安全域,防止不可信主体的干扰和篡改。

FPT_SEP.1.2 安全功能应在其控制范围内主体的安全域之间强行分离。

7.1.3.2.7 系统安全功能间安全功能数据的一致性(FPT_TDC)

7.1.3.2.7.1 系统安全功能间基本安全功能数据的一致性(FPT_TDC.1)

本组件要求网上证券交易系统提供确保安全功能间属性的一致性的能力。

FPT_TDC.1.1 当网上证券交易系统与别的可信IT产品共享安全功能数据时，系统应能够判断所有安全功能数据的一致性。

FPT_TDC.1.2 当判断来自别的可信IT产品的安全功能数据时，系统应使用预先大家所协定的一组规则。

7.1.3.3 安全审计(FAU)

安全审计包括产生、记录、存储和分析那些与安全相关活动有关的信息。审计记录结果可用来检测、判断发生了哪些安全相关活动以及这些活动是由哪个用户负责的。

7.1.3.3.1 安全审计自动响应(FAU_ARP)

7.1.3.3.1.1 安全警告(FAU_ARP.1)

安全警告功能描述了当检测到可能的安全侵害时，系统将采取的行动，包括报警或系统自动响应。

FAU_ARP.1.1 当检测到潜在的安全侵害时，系统将通知授权管理员，使产生潜在安全侵害的主体失效，或采取其他由授权管理员确定的行动。

例如，系统安全功能能够生成实时报警、终止违例进程、取消服务、或断开用户账号以及使用户账号失效等。

应用注释：如果一个审计事件由FAU_SAA组件指出，那么这个事件将被定义为是"潜在的安全侵害事件"。

7.1.3.3.2 安全审计数据产生(FAU_GEN)

本节要求发生安全相关事件时应记录其出现，列举出网上证券系统可审计的事件类型，以及应在各审计记录内提供的审计相关信息的最小集合。

7.1.3.3.2.1 审计数据产生(FAU_GEN.1)

网上证券系统的审计数据产生功能只产生最小级审计事件记录，并规定进行每项记录的数据装。

FAU_GEN.1.1 系统应能为下述可审计事件产生审计记录：

a) 审计功能的启动和关闭；

b) 所有最小级的可审计事件；

c) 其他专门定义的可审计事件由证券公司自行定义。

FAU_GEN.1.2 系统将在每个审计记录中至少记录如下信息：

a) 事件的日期和时间，事件类型，主体身份，事件的结果(成功或失败)；

b) 最小级可审计事件类型见表18；

c) 专门定义的可审计事件清单由开发者列于表18的第四栏。

表18 系统边界安全保障技术要求的可审计安全事件类型

组件标识	审计级别	可审计事件	专门定义的审计事件
FAU_ARP.1	最小级	当即将发生安全侵害时采取的行动。	
FAU_SAA.1	最小级	开启和关闭任何分析机制。 由工具完成的自动响应。	
FCO_NRO.2	最小级	调用抗抵赖服务。	
FCO_NRR.2	最小级	调用抗抵赖服务。	
FDP_ACF.1	最小级	成功的请求对某个被安全功能策略覆盖的客体上执行某操作。	
FDP_DAU.2	最小级	成功的产生有效证据。	

表 18(续)

组件标识	审计级别	可审计事件	专门定义的审计事件
FDP_ETC. 1	最小级	成功的信息输出。	
FDP_ETC. 2	最小级	成功的信息输出。	
FDP_IFF. 1	最小级	判定允许请求的信息流。	
FDP_IFF. 5	最小级	判定允许请求的信息流。	
FDP_ITC. 2	最小级	成功输入用户数据,包括任何安全属性。	
FDP_SDI. 2	最小级	成功尝试检测用户数据的完整性,包括指示检测结果。	
FDP_UCT. 1	最小级	使用数据交换机制的任何用户或主体的身份。	
FDP_UIT. 1	最小级	使用数据交换机制的任何用户或主体的身份。	
FIA_AFL. 1	最小级	获取失败鉴别的阈值和采取的动作(如,使终端无效),及随后还原到正常状态(如,重新使终端有效)。	
FIA_SOS. 1	最小级	安全功能拒绝任何测试的秘密。	
FIA_SOS. 2	最小级	安全功能拒绝任何测试的秘密。	
FIA_UAU. 1	最小级	使用鉴别机制失败。	
FIA_UAU. 3	最小级	检测欺骗性的鉴别数据。	
FIA_UAU. 5	最小级	鉴别的最后判定。	
FIA_UAU. 6	最小级	重鉴别失败。	
FIA_UID. 1	最小级	使用用户标识机制失败,包括提供的用户身份。	
FIA_USB. 1	最小级	绑定用户安全属性到一个主体失败(如,产生一个主体)。	
FMT_MOF. 1	最小级	系统安全功能的所有改动。	
FMT_MSA. 2	最小级	对某安全属性,所有提供的和被拒绝的值。	
FMT_SMR. 1	最小级	对角色一部分的用户组的改动。	
FMT_SMR. 3	最小级	明确请求担任某角色。	
FPT_ITI. 1	最小级	检测传输的安全功能数据的修改。	
FPT_RCV. 1	最小级	出现失败或服务中断。 恢复正常运行。	
FPT_SSP. 2	最小级	接收期待的回执时,发生失败。	
FPT_STM. 1	最小级	时间的变动。	
FPT_TDC. 1	最小级	成功使用安全功能数据一致性机制。	
FRU_FLT. 1	最小级	安全功能检测出的任何故障。	
FRU_RSA. 1	最小级	因资源的限制对分配操作的拒绝。	
FTA_MCS. 1	最小级	基于多重并发会话限定对新会话的拒绝。	
FTP_ITC. 1	最小级	可信信道功能故障。 失败的可信信道功能的原发者及目标的标识。	

7.1.3.3.2.2 用户身份关联(FAU_GEN.2)

该功能解决可审计事件追溯到单个用户身份上的要求。

FAU_GEN.2.1 系统能将每个可审计事件与引起该事件的用户身份相关联。

7.1.3.3.3 安全审计分析(FAU_SAA)

7.1.3.3.3.1 潜在侵害分析(FAU_SAA.1)

本功能提出为寻找可能的或真正的安全侵害,用来分析系统活动和审计数据的自动化措施的要求,这种分析可用于支持入侵检测。潜在侵害分析需要基于一个固定规则集的基本门限检测。

FAU_SAA.1.1 系统应有能力用一系列规则去监测审计事件,并依据这些规则指出对安全策略的潜在侵害。

FAU_SAA.1.2 系统用下列规则来监视审计事件:

根据已知的由可审计安全事件积累或组合对应的安全攻击模式。

注:由于系统使用外国操作系统,建议使用入侵检测安全产品。

7.1.3.3.4 安全审计查阅(FAU_SAR)

7.1.3.3.4.1 审计查阅(FAU_SAR.1)

审计查阅功能提供从审计记录中读取信息的能力。

FAU_SAR.1.1 系统将提供具有查阅审计数据功能的工具,以读取审计记录。

FAU_SAR.1.2 系统将规定准许指定用户按表19中的规则查阅某些审计记录。

表19 系统边界安全保障技术要求的可查阅审计记录

用户	可查阅的审计记录
系统审计员	所有对于安全功能的审计记录
系统安全员	所有对于安全功能的审计记录
系统管理员	所有对于系统功能的审计记录

7.1.3.3.4.2 有限审计查阅(FAU_SAR.2)

有限审计查阅功能要求除在FAU_SAR.1中确定的用户外,其他用户不能读取信息。

FAU_SAR.2.1 除具有明确读访问权限的用户外,系统将禁止所有用户对审计记录的读访问。

7.1.3.3.5 安全审计事件存储(FAU_STG)

本节提出创建并维护安全的审计踪迹的要求。

7.1.3.3.5.1 确保审计数据可用性(FAU_STG.2)

确保审计数据可用性功能要求审计踪迹应避免未授权的删除和/或修改,并确保在意外情况出现时审计数据的可用性。

FAU_STG.2.1 系统将保护已储存的审计记录,以避免未授权的删除。

FAU_STG.2.2 系统应能防止对审计记录的修改。

FAU_STG.2.3 当发生审计存储已满、失败或攻击情况时,系统应确保审计记录在一定记录数之内或确定的维护时间范围内不被破坏,这一度量准则由国家行政管理机构统一确定或由证券公司根据需要自行决定。

7.1.3.3.5.2 防止审计数据丢失(FAU_STG.4)

防止审计数据丢失功能要求规定了当审计踪迹溢满时所采取的行动。

FAU_STG.4.1 如果审计踪迹已满,系统将阻止除由系统审计员产生的以外的所有可审计事件。

7.1.3.4 安全管理(FMT)

7.1.3.4.1 系统中功能的管理(FMT_MOF)

7.1.3.4.1.1 安全功能行为的管理(FMT_MOF.1)

允许授权用户管理系统安全功能。

FMT_MOF.1.1 系统应限定授权用户对是否使用、修改下列安全功能进行决定的能力(如表20)。

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

类型	安全功能	系统管理员	系统安全员	系统审计员	系统操作员	投资者
审计	审计参数	无	无	配置	备份	无
	审计失败时进行相应操作	维护	无	管理	无	无
	审计项目的更改	无	无	管理	无	无
识别和鉴别	用户账号、角色、属性	无	管理	无	维护	无
	鉴别数据的管理	无	管理	无	无	管理关联数据
	鉴别机制和规则	无	管理	无	无	无
	用户被鉴别前可采取的动作表	无	管理	无	无	无
	对失败的鉴别尝试的阈值及所要采取的动作的管理	无	管理	无	无	无
密码支持	密钥属性的管理	无	管理	无	无	无
	对用于验证及产生秘密的量度的管理	无	管理	无	无	无
安全管理	维护系统中的角色组	维护	管理	无	无	无
	对改变信息类型、域、原发者属性和证据接收者的管理	维护	管理	无	无	无
	定义默认的主体安全属性	无	管理	无	无	无
	为用户组、用户和主体规定某资源的最大使用限度	管理	无	无	无	无
安全功能的保护	管理数据备份参数	管理	无	无	启动	无
	管理需要可信信道的活动	无	管理	无	无	无
	时间戳	无	管理	无	无	无
	管理支持有效期的安全属性表及过期将采取的动作	无	管理	无	无	无
	多重并发会话的基本限定	无	管理	无	无	无
	管理用于作出访问或拒绝访问决策的属性	无	管理	无	无	无
	选择何时执行剩余信息保护即配给或索回	无	管理	无	无	无
	配置检测到完整性错误时所要采取的动作	无	管理	无	无	无
	抽象机测试产生的条件及时间间隔的管理	无	管理	无	无	无
	要防止的修改类型的管理	无	管理	无	无	无
	用于输入的附加控制规则	无	管理	无	无	无
	不同部分间数据传输保护机制的管理	无	管理	无	无	无
	可检测出其重放的确定实体列表及须采取的行动列表的管理	无	管理	无	无	无

7.1.4 网络和基础设施安全保障技术要求

7.1.4.1 用户数据保护(FDP)

7.1.4.1.1 数据鉴别(FDP_DAU)

7.1.4.1.1.1 伴有保证者身份的数据鉴别(FDP_DAU.2)

系统安全功能应具有相应的能力，保证主体的真实身份，并承担信息真实性的责任(如，通过数字签名)，用来保证指定的数据单元的有效性，进而验证静态的信息没有被伪造或篡改。

FDP_DAU.2.1 系统安全功能将提供产生保证客体(详见 FDP_ACF.1)的有效性证据的能力。

FDP_DAU.2.2 系统安全功能将为投资者和券商提供验证网上证券交易有关数据和指令真实有效的证据和产生该证据的真实身份的能力。

7.1.4.1.2 存储数据的完整性(FDP_SDI)

7.1.4.1.2.1 存储数据完整性监视和行动(FDP_SDI.2)

FDP_SDI.2.1 系统安全功能应基于用户数据属性，监视存储在系统内部的用户数据是否出现完整性错误。

FDP_SDI.2.1 检测到完整性错误时，系统安全功能应要采取相应的行动。

7.1.4.1.3 安全功能间用户数据传送保密性保护(FDP_UCT)

7.1.4.1.3.1 基本数据交换保密性(FDP_UCT.1)

FDP_UCT.1.1 系统安全功能应执行网上访问控制策略和网上信息流控制策略，能以防止未授权泄露的方式传送和接收客体。

7.1.4.1.4 安全功能间用户数据传送完整性保护(FDP_UIT)

7.1.4.1.4.1 数据交换完整性(FDP_UIT.1)

此功能主要解决对被传输的用户数据的篡改、删除、插入和重用等的检测。

FDP_UIT.1.1 系统安全功能应执行网上信息流控制策略，能以避免出现篡改、删除、插入或重用等的方式传送和接收用户数据。

FDP_UIT.1.2 系统安全功能应能根据收到的用户数据判断，是否出现了篡改、删除、插入和重用。

7.1.4.2 安全功能保护(FPT)

7.1.4.2.1 安全功能数据输出的保密性(FPT_ITC)

7.1.4.2.1.1 传输过程中安全功能间的保密性(FPT_ITC.1)

要求系统安全功能确保安全功能数据在系统与远程可信 IT 产品间的传输不被泄露。

FPT_ITC.1.1 网上证券交易系统应保护所有的安全功能数据从系统到远程可信 IT 产品的传输过程中不被未经授权的泄密。

7.1.4.2.2 安全功能数据输出的完整性(FPT_ITI)

7.1.4.2.2.1 安全功能间的修改检测(FPT_ITI.1)

提供在远程可信 IT 被产品知道所使用的机制的假设下，检测安全功能数据在系统与远程可信 IT 产品传输过程中修改的能力。

FPT_ITI.1.1 网上证券交易系统应能够检测系统与远程可信 IT 产品间传输的所有安全功能数据的修改。

FPT_ITI.1.2 应验证在系统与远程可信 IT 产品间传输的所有安全功能数据的完整性，如果检测到数据修改时应及时通知数据的拥有者。

7.1.4.2.3 系统内部安全功能数据传输(FPT_ITT)

7.1.4.2.3.1 系统内部安全功能数据传输的基本保护(FPT_ITT.1)

要求对网上证券交易系统的分离部分间传输的安全功能数据进行保护。

FPT_ITT.1.1 在网上证券交易系统的各个部分间传输安全功能数据时，应保护其不被泄漏。

7.1.4.2.4 时间戳(FPT_STM)

7.1.4.2.4.1 可靠的时间戳(FPT_STM.1)

本组件要求系统安全功能为自身提供可靠的时间戳。

FPT_STM.1.1 网上证券交易系统的安全功能应能为自身的应用提供可靠的时间戳。

7.1.4.2.5 系统安全功能间安全功能数据的一致性(FPT_TDC)

7.1.4.2.5.1 系统安全功能间基本安全功能数据的一致性(FPT_TDC.1)

本组件要求网上证券交易系统提供确保安全功能间属性的一致性的能力。

FPT_TDC.1.1 当网上证券交易系统与别的可信 IT 产品共享安全功能数据时,系统应能够判断所有安全功能数据的一致性。

FPT_TDC.1.2 当判断来自别的可信 IT 产品的安全功能数据时,系统应使用预先大家所协定的一组规则。

7.1.5 支撑性基础设施安全保障技术要求

7.1.5.1 密码支持(FCS)

系统可以利用密码功能来满足一些高级安全目的。这些功能包括:标识与鉴别,抗抵赖,可信信道和数据分离等。可用硬件、固件和/或软件来实现,在系统执行密码功能时使用。密码支持要求包括对密钥管理和密码运算方面的要求。

7.1.5.1.1 密钥管理(FCS_CKM)

密钥在其整个生存期内都必须进行管理。本条定义了以下几种管理功能:密钥产生、密钥分配、密钥访问和密钥销毁。如使用 PKI 体系,用于加密的密钥对和加密证书与用于签名的密钥对和签名证书应分开,不得使用同一密钥对和证书进行签名和加密。

7.1.5.1.1.1 密钥产生(FCS_CKM.1)

密钥产生功能要求以基于某个指定标准的特定的算法和密钥长度来产生密钥。

FCS_CKM.1.1 系统将以符合标准要求的特定密钥产生算法和密钥长度来产生密钥。

应用注释:对称密钥产生器所产生的密钥应使每个密钥产生的概率独立等概,并通过最长连长、"0""1"概率分布、扑克检验和连长检验等随机性检验。公开密钥产生器应证明产生的素数确为素数,且每个素数独立等概。

7.1.5.1.1.2 密钥分配(FCS_CKM.2)

密钥分配功能要求以基于某个指定标准的特定的分配方法来分配密钥。

FCS_CKM.2.1 系统可采用公钥体制的密钥分配方法来分配密钥。

7.1.5.1.1.3 密钥访问(FCS_CKM.3)

密钥访问功能要求根据基于某个指定标准的特定的访问方法来访问密钥。

FCS_CKM.3.1 系统应规定密钥访问规则,并依此来控制对密钥的访问。

7.1.5.1.1.4 密钥销毁(FCS_CKM.4)

密钥销毁功能要求以基于某个指定标准的特定的销毁方法来销毁密钥。

FCS_CKM.4.1 系统应根据符合标准的密钥管理规范中特定的密钥销毁方法来销毁密钥。

7.1.5.1.2 密码运算(FCS_COP)

7.1.5.1.2.1 密码运算(FCS_COP.1)

为了保证密码运算的功能正确,必须按照特定的算法和一定长度的密钥来运算。密码运算包括:数据加密和/或解密、数字签名产生和/或验证、针对完整性的密码校验和产生和/或检验、保密散列(信息摘要)、密钥加密和/或解密,以及密钥协商等。

FCS_COP.1.1 系统将以符合规定标准要求的特定密钥产生算法和密钥长度来执行特定密码运算。

7.1.5.2 安全审计(FAU)

安全审计包括产生、记录、存储和分析那些与安全相关活动有关的信息。审计记录结果可用来检测、判断发生了哪些安全相关活动以及这些活动是由哪个用户负责的。

7.1.5.2.1 安全审计自动响应(FAU_ARP)

7.1.5.2.1.1 安全警告(FAU_ARP.1)

安全警告功能描述了当检测到可能的安全侵害时,系统将采取的行动,包括报警或系统自动响应。

FAU_ARP.1.1 当检测到潜在的安全侵害时,系统将通知授权管理员,使产生潜在安全侵害的主体失效,或采取其他由授权管理员确定的行动。

例如,系统安全功能能够生成实时报警、终止违例进程、取消服务、或断开用户账号以及使用户账号失效等。

应用注释:如果一个审计事件由 FAU_SAA 组件指出,那么这个事件将被定义为是"潜在的安全侵害事件"。

7.1.5.2.2 安全审计数据产生(FAU_GEN)

本节要求发生安全相关事件时应记录其出现,列举出网上证券系统可审计的事件类型,以及应在各审计记录内提供的审计相关信息的最小集合。

7.1.5.2.2.1 审计数据产生(FAU_GEN.1)

网上证券系统的审计数据产生功能只产生最小级审计事件记录,并规定进行每项记录的数据表。

FAU_GEN.1.1 系统应能为下述可审计事件产生审计记录:

a) 审计功能的启动和关闭;

b) 所有最小级的可审计事件;

c) 其他专门定义的可审计事件由证券公司自行定义。

FAU_GEN.1.2 系统将在每个审计记录中至少记录如下信息:

a) 事件的日期和时间,事件类型,主体身份,事件的结果(成功或失败);

b) 最小级可审计事件类型见表 21;

c) 专门定义的可审计事件清单由开发者列于表 21 的第四栏。

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

组件标识	审计级别	可审计事件	专门定义的审计事件
FAU_ARP.1	最小级	当即将发生安全侵害时采取的行动。	
FAU_SAA.1	最小级	开启和关闭任何分析机制。 由工具完成的自动响应。	
FCO_NRO.2	最小级	调用抗抵赖服务。	
FCO_NRR.2	最小级	调用抗抵赖服务。	
FDP_ACF.1	最小级	成功的请求对某个被安全功能策略覆盖的客体上执行某操作。	
FDP_DAU.2	最小级	成功的产生有效证据。	
FDP_ETC.1	最小级	成功的信息输出。	
FDP_ETC.2	最小级	成功的信息输出。	
FDP_IFF.1	最小级	判定允许请求的信息流。	
FDP_IFF.5	最小级	判定允许请求的信息流。	
FDP_ITC.2	最小级	成功输入用户数据,包括任何安全属性。	

表 21(续)

组件标识	审计级别	可审计事件	专门定义的审计事件
FDP_SDI. 2	最小级	成功尝试检测用户数据的完整性,包括指示检测结果。	
FDP_UCT. 1	最小级	使用数据交换机制的任何用户或主体的身份。	
FDP_UIT. 1	最小级	使用数据交换机制的任何用户或主体的身份。	
FIA_AFL. 1	最小级	获取失败鉴别的阈值和采取的动作(如,使终端无效),及随后还原到正常状态(如,重新使终端有效)。	
FIA_SOS. 1	最小级	安全功能拒绝任何测试的秘密。	
FIA_SOS. 2	最小级	安全功能拒绝任何测试的秘密。	
组件标识	审计级别	可审计事件。	专门定义的审计事件
FIA_UAU. 1	最小级	使用鉴别机制失败。	
FIA_UAU. 3	最小级	检测欺骗性的鉴别数据。	
FIA_UAU. 5	最小级	鉴别的最后判定。	
FIA_UAU. 6	最小级	重鉴别失败。	
FIA_UID. 1	最小级	使用用户标识机制失败,包括提供的用户身份。	
FIA_USB. 1	最小级	绑定用户安全属性到一个主体失败(如,产生一个主体)。	
FMT_MOF. 1	最小级	系统安全功能的所有改动。	
FMT_MSA. 2	最小级	对某安全属性,所有提供的和被拒绝的值。	
FMT_SMR. 1	最小级	对角色一部分的用户组的改动。	
FMT_SMR. 3	最小级	明确请求担任某角色。	
FPT_ITI. 1	最小级	检测传输的安全功能数据的修改。	
FPT_RCV. 1	最小级	出现失败或服务中断。 恢复正常运行。	
FPT_SSP. 2	最小级	接收期待的回执时,发生失败。	
FPT_STM. 1	最小级	时间的变动。	
FPT_TDC. 1	最小级	成功使用安全功能数据一致性机制。	
FRU_FLT. 1	最小级	安全功能检测出的任何故障。	
FRU_RSA. 1	最小级	因资源的限制对分配操作的拒绝。	
FTA_MCS. 1	最小级	基于多重并发会话限定对新会话的拒绝。	
FTP_ITC. 1	最小级	可信信道功能故障。 失败的可信信道功能的原发者及目标的标识。	

7.1.5.2.2.2 **用户身份关联**(FAU_GEN. 2)

该功能解决可审计事件追溯到单个用户身份上的要求。

FAU_GEN. 2. 1 系统能将每个可审计事件与引起该事件的用户身份相关联。

7.1.5.2.3 安全审计分析(FAU_SAA)

7.1.5.2.3.1 潜在侵害分析(FAU_SAA.1)

本功能提出为寻找可能的或真正的安全侵害,用来分析系统活动和审计数据的自动化措施的要求,这种分析可用于支持入侵检测。潜在侵害分析需要基于一个固定规则集的基本门限检测。

FAU_SAA.1.1 系统应有能力用一系列规则去监测审计事件,并依据这些规则指出对安全策略的潜在侵害。

FAU_SAA.1.2 系统用下列规则来监视审计事件:

a) 根据已知的由可审计安全事件积累或组合对应的安全攻击模式。

注:由于系统使用外国操作系统,建议使用入侵检测安全产品。

7.1.5.2.4 安全审计查阅(FAU_SAR)

7.1.5.2.4.1 审计查阅(FAU_SAR.1)

审计查阅功能提供从审计记录中读取信息的能力。

FAU_SAR.1.1 系统将提供具有查阅审计数据功能的工具,以读取审计记录。

FAU_SAR.1.2 系统将规定准许指定用户按表22形式建立规则查阅某些审计记录。

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

用户	可查阅的审计记录
系统审计员	所有对于安全功能的审计记录
系统安全员	所有对于安全功能的审计记录
系统管理员	所有对于系统功能的审计记录

7.1.5.2.4.2 有限审计查阅(FAU_SAR.2)

有限审计查阅功能要求除在FAU_SAR.1中确定的用户外,其他用户不能读取信息。

FAU_SAR.2.1 除具有明确读访问权限的用户外,系统将禁止所有用户对审计记录的读访问。

7.1.5.2.5 安全审计事件存储(FAU_STG)

本条提出创建并维护安全的审计踪迹的要求。

7.1.5.2.5.1 确保审计数据可用性(FAU_STG.2)

确保审计数据可用性功能要求审计踪迹应避免未授权的删除和/或修改,并确保在意外情况出现时审计数据的可用性。

FAU_STG.2.1 系统将保护已储存的审计记录,以避免未授权的删除。

FAU_STG.2.2 系统应能防止对审计记录的修改。

FAU_STG.2.3 当发生审计存储已满、失败或攻击情况时,系统应确保审计记录在一定记录数之内或确定的维护时间范围内不被破坏,这一度量准则由国家行政管理机构统一确定或由证券公司根据需要自行决定。

7.1.5.2.5.2 防止审计数据丢失(FAU_STG.4)

防止审计数据丢失功能要求规定了规定当审计踪迹溢满时所采取的行动。

FAU_STG.4.1 如果审计踪迹已满,系统将阻止除由系统审计员产生的以外的所有可审计事件。

7.2 安全保障管理要求

7.2.1 管理保障控制类:风险管理(MRM)

7.2.1.1 管理保障控制类风险管理(MRM)介绍

信息安全管理保障是以风险和策略为核心。本类的目的是建立一套风险管理体系,通过对象确立、风险评估、风险控制三个基本步骤,并将沟通与监控贯穿于这三个步骤中,进行信息安全风险管理与防范,将系统风险降低到可接受的水平。

7.2.1.2 对象确立(MRM_TEM)

7.2.1.2.1 对象确立子类介绍

根据网上证券系统的业务目标和特性，确定风险管理对象；识别信息系统资产，并评价资产价值；根据信息系统安全需求，确定风险评价准则。

7.2.1.2.2 确定风险管理对象(MRM_TEM.1)

应综合考虑组织机构的使命、业务、组织结构、管理制度和技术平台，以及国家、地区或行业的相关政策、法律、法规和标准，确定信息安全风险管理的范围和对象；并对对象的业务目标、业务特性、管理特性、技术特性、体系架构和安全要求等进行分析调查。

7.2.1.2.3 识别和评价资产(MRM_TEM.2)

组织机构应识别与风险管理对象相关的系统资产，并根据资产安全价值进行估值。

7.2.1.2.4 MRM_TEM.3 制定安全基线(MRM_TEM.3)

组织机构应在风险评估前制定系统安全基线，即满足信息系统的基本安全要求，使系统达到一定安全水平的一组安全控制措施。

7.2.1.3 风险评估(MRM_RAM)

7.2.1.3.1 风险评估子类介绍

识别、分析和评价网上证券交易系统所面临的风险。

7.2.1.3.2 识别风险(MRM_RAM.1)

组织机构应识别网上证券交易系统面临的威胁和存在的脆弱性。

7.2.1.3.3 分析风险(MRM_RAM.2)

组织机构应分析威胁源动机、威胁行为的能力、脆弱点被利用的可能性以及脆弱点被利用后对系统造成的影响。

7.2.1.3.4 评价风险(MRM_RAM.3)

组织机构应评价威胁源动机的等级、威胁行为能力的等级、脆弱性被利用的等级、资产价值等级和影响程度等级，并综合评价风险等级。

7.2.1.4 风险控制(MRM_RCT)

7.2.1.4.1 风险控制子类介绍

依据风险评估结果，选择并实施恰当的安全措施，将风险控制在可接受的范围内。

7.2.1.4.2 确立控制目标(MRM_RCT.1)

组织机构应确定可接受风险等级，判断现存风险是否可接受，确立风险控制目标。

7.2.1.4.3 选择控制措施(MRM_RCT.2)

组织机构应选择风险控制方式和风险控制措施。

7.2.1.4.4 实施控制措施(MRM_RCT.3)

制定风险控制实施计划，实施风险控制措施。

7.2.1.4.5 验证控制措施(MRM_RCT.4)

验证风险控制的结果是否满足信息系统的安全要求。

7.2.2 管理保障控制类：信息安全策略(MSP)

7.2.2.1 管理保障控制类信息安全策略(MSP)介绍

信息安全管理保障是以风险和策略为核心。信息安全策略体系规范和指导了整个组织机构的信息安全保障工作。信息安全策略管理保障控制类提供了信息安全策略在制定和维护方面的管理，为信息安全提供符合业务要求和相关法律法规的管理指导和支持。

7.2.2.2 信息安全策略(MSP_SPL)

7.2.2.2.1 信息安全策略子类介绍

通过定义一套规则来规范信息安全体系的建设、运行和管理，为信息安全建设提供方向，为信息安

全工作符合业务要求和相关的法律法规要求。

管理层应建立清晰的安全策略，安全策略应符合组织机构的业务目标。通过在整个组织机构中发布和维护信息安全策略可以表明管理层对信息安全的支持力度和信息安全承诺。

7.2.2.2.2 制定安全策略(MSP_SPL.1)

组织机构应制定安全策略文件，系统的安全策略应覆盖系统的整个生命周期和系统安全管理的所有方面。

7.2.2.2.3 审核批准安全策略(MSP_SPL.2)

安全策略文件应由组织机构决策层审核批准，确保安全策略的完整性和有效性。

7.2.2.2.4 发布与落实安全策略(MSP_SPL.3)

安全策略文件应向组织机构全体员工发布，各级员工应以安全策略为指导进行日常工作。

7.2.2.2.5 维护更新安全策略(MSP_SPL.4)

应定期或当系统发生重大变更时审核安全策略以保持策略的适用性、充分性和有效性。

7.2.3 管理保障控制类：信息安全组织机构(MSO)

7.2.3.1 管理保障控制类信息安全组织机构(MSO)介绍

信息安全组织机构是信息安全管理的基础，需要得到组织机构最高管理层的承诺和支持，建立完善的信息安全组织结构。建立相应的岗位、职责和职权，建立完善的内部和外部沟通协作组织和机制，同组织机构内部和外部信息安全保障的所有相关方进行充分沟通、学习、交流和合作等。进一步将信息安全融至组织机构的整个环境和文化中，使信息安全真正满足安全策略和风险管理的要求，实现保障组织机构资产和使命的最终目的。

7.2.3.2 信息安全的管理支持(MSO_SOM)

7.2.3.2.1 信息安全的管理支持子类介绍

管理层应提供保障和支持，提供清晰的指导，明确安全职责，协调和审核组织机构内安全。

7.2.3.2.2 管理层的支持(MSO_SOM.1)

管理层应对网上证券系统的安全有足够的认知能力和水平，并在组织机构内通过清晰的指导，明确信息安全职责的分配和确认，提供对系统安全建设和维护的主动支持。

7.2.3.3 信息安全组织架构(MSO_ORG)

7.2.3.3.1 信息安全组织架构子类介绍

组织机构应建立完善的信息安全组织体系，以启动和控制组织机构内的信息安全。

7.2.3.3.2 组织架构的建立和维护(MSO_ORG.1)

形成架构清晰的信息安全保障组织机构，保持整体组织结构的稳定性。

7.2.3.4 信息安全职责(MSO_RES)

7.2.3.4.1 信息安全职责子类的介绍

组织机构应有清晰的和恰当的安全职责划分和职责到人，保证信息安全措施的落实。

7.2.3.4.2 信息安全职责分配(MSO_RES.1)

应清晰地定义组织机构的所有的信息安全职责，并保证各项职责明确到人。

7.2.3.4.3 职责分离要求(MSO_RES.2)

组织机构应分离某些任务的管理、执行和职责范围，加强监督力度，以降低非法修改或误用职权带来的风险。

7.2.3.4.4 独立审计要求(MSO_RES.3)

应在计划的时间间隔或在对安全实施有重要变更时，对组织机构信息系统安全及其控制策略(如，信息安全的控制目标、策略、过程、流程等)进行独立审核。

7.2.3.5 沟通协作(MSO_CAC)

7.2.3.5.1 沟通协作子类介绍

组织机构应该根据业务持续性和风险评估的需要，建立和维护内部与外部组织机构的有效沟通和协作机制。

7.2.3.5.2 信息安全活动的内部协调(MSO_CAC.1)

在组织机构内，应建立一个内部协调机制以保证信息安全活动的有效沟通和实施。

7.2.3.5.3 维护与外部机构的协作(MSO_CAC.2)

应建立同组织机构系统和业务相关的各有关职能机构、运营商、服务方等的沟通和协作，维护与外部机构协作的及时性和有效性。

7.2.4 管理保障控制类：人员安全(MPS)

7.2.4.1 管理保障控制类人员安全(MPS)介绍

人员安全是信息安全管理的基础。应建立规范的人员安全管理，对组织机构的聘用人员进行严格的审查，明确人员的安全职责和保密要求。加强人员的安全意识培训和教育，并建立考核和奖惩机制，使信息安全融至组织机构的整个环境和文化中，减少有意、无意的内、外部威胁，确保组织机构顺利完成系统使命。

7.2.4.2 安全意识和培训(MPS_SAT)

7.2.4.2.1 安全意识和培训子类介绍

确保员工、合约方和用户了解信息安全威胁的存在，以及他们的安全责任，并获取必要的安全技能。

7.2.4.2.2 安全意识(MPS_SAT.1)

应对用户进行安全意识的教育和培训，确保信息系统的所有合法用户了解信息安全的基本要求。必要性以及他们所担负的安全责任。

7.2.4.2.3 安全培训(MPS_SAT.2)

组织机构应确定每个工作人员在信息系统中的安全角色和职责，在工作人员访问系统之前给他们提供恰当的信息系统安全培训，之后应以组织规定的时间继续培训。

7.2.5 管理保障控制类：资产管理(MAM)

7.2.5.1 管理保障控制类资产管理(MAM)介绍

资产管理是信息安全管理的基础，同时也是信息安全保证的重要内容，组织机构应通过规范资产的管理和使用来保障资产的安全，来保证系统的安全，最终保障组织机构使命。

7.2.5.2 资产登记管理(MAM_ARM)

7.2.5.2.1 资产登记管理子类介绍

清晰了解组织机构所有的有形和无形资产。

7.2.5.2.2 资产清单(MAM_ARM.1)

应清晰地识别和确认所有资产，应制定并维护一份重要资产清单。

7.2.5.3 资产管理职责(MAM_AMR)

7.2.5.3.1 资产管理职责子类介绍

维持并实施适当的保护措施保护组织机构的资产。所有重要的信息资产应有负责人，并有选定的所有者，制定适当控制责任。

7.2.5.3.2 资产管理职责(MAM_AMR.1)

同信息处理设施相关的所有信息和资产都应指定到机构中的部门，对所拥有的资产负责。对同信息处理设施相关的信息和资产的登记、使用都应实施适当控制。

7.2.5.4 资产分类管理(MAM_ACM)

7.2.5.4.1 资产分类管理子类介绍

确保系统的资产依据不同程度的敏感度及重要性得到相应级别的保护。

7.2.5.4.2 资产分类(MAM_ACM.1)

组织机构的资产包括有形的物理资产和无形的信息资产,组织机构不仅需要对有形的物理资产进行分类,还应根据信息对组织机构的价值、法律要求、敏感性和关键性等对信息资产进行分类。

7.2.5.4.3 信息的标记和处理(MAM_ACM.2)

应该制定并实施一组恰当的标注及处理信息流程,流程应符合组织机构所采用的分类方法。

7.2.6 管理保障控制类:物理和环境安全(MPE)

7.2.6.1 管理保障控制类物理和环境安全(MPE)介绍

物理和环境安全是保障基础设施安全的基础。组织机构应保证物理安全区域安全,建立严格的物理访问控制措施,以防止非法访问、危害及干扰系统运行。基础设施是系统的重要资产,应在防火、防水、温湿度、防雷等方面做到安全防护,保证基础设施安全,保证系统持续运行。

7.2.6.2 物理安全区域管理(MPE_PSA)

7.2.6.2.1 物理安全区域子类介绍

应有物理的保护防止对基础设施和信息的非法访问、危害和干扰。对重要或敏感的业务信息处理设备应放在安全的地方,并在规定的安全边界处用恰当的安全障碍和控制措施进行保护。

7.2.6.2.2 物理安全区域和边界(MPE_PSA.2)

应根据不同的安全保护需求,划分不同的安全区域,实施不同等级的安全管理。

7.2.6.2.3 物理安全保护(MPE_PSA.3)

应设计和应用安全区域和设施的物理安全防护。

7.2.6.2.4 人员出入控制(MPE_PSA.4)

应通过合适的入口控制保护安全区域,确保只有授权人员才允许访问。

7.2.6.2.5 设备出入控制(MPE_PSA.5)

应对带离安全区域的设备、信息或软件进行控制。

7.2.6.2.6 在安全区域中工作的控制(MPE_PSA.6)

应制定安全区域工作的物理保护的管理规定,对在安全区域内工作的人员及被授权进入安全区域的其他人员加强管理。

7.2.6.3 支撑基础设施安全(MPE_SIS)

7.2.6.3.1 支撑基础设施安全子类介绍

所有的支撑设施,如电力、水、加热、通风和空调都应满足系统的需要。应定期对支撑设施进行检查,并进行适当的测试来确保其正常的功能,减少发生故障和失败的风险。

7.2.6.3.2 电力设施管理(MPE_SIS.1)

应防止由于电力故障导致对设备的损害。

7.2.6.3.3 线缆安全(MPE_SIS.2)

电力和通信电缆由于携带数据或是信息设备支撑,应该予以保护防止被侦听和破坏。

7.2.6.3.4 运行环境安全(MPE_SIS.3)

应采取相应的防火、防水、防尘、防雷、温湿度控制等控制措施为设备与介质提供适宜的环境,并提供相应的环境监控,以避免由于环境因素造成对设备和介质的损害。

7.2.6.3.5 紧急处理设施(MPE_SIS.4)

对于一些具体的位置,集中包含信息系统资源(例如:数据中心、服务器房间、大型机房间),组织机构提供关掉电源的能力,信息技术组件可能产生故障(例如:由于电火)或威胁(例如:由于水渗漏),要求远离设备,从而不会危及到人的生命安全。

组织机构实施和维持自动化紧急照明系统,在电源损耗或破坏时能指示紧急出口和撤退路线。

7.2.6.4 设备安全（MPE_EMS）

7.2.6.4.1 设备安全子类介绍

应防止由于资产的丢失、损害、被盗或老化等造成对组织活动的中断。

应防止设备受到物理和环境的威胁；考虑放置安全，防止受到未授权的破坏。

7.2.6.4.2 设备放置和保护（MPE_EMS.1）

为避免环境威胁和未经授权访问的影响，应将设备与介质安全放置并保护。

设备或介质如因工作需要带离安全区域，更要注意对其进行保护。

一些固定在部门安全区域外的设备，同样要注意物理防护。

7.2.7 管理保障控制类：符合性管理（MCM）

7.2.7.1 管理保障控制类符合性管理（MCM）介绍

符合性管理是信息安全保障的基础。组织机构应建立有效的监督体系以监督验证信息系统安全保障工作对相关法律法规、政策标准等要求以及组织机构所制定的信息安全策略体系的符合性以及执行的效果。

7.2.7.2 法律法规和政策符合性（MCM_LCP）

7.2.7.2.1 法律法规和政策符合性子类介绍

确保网上证券系统与信息安全相关的国家政策、法律法规、行政法规和相关合同等要求的符合性。

7.2.7.2.2 确定适用的法律法规和政策（MCM_LCP.1）

组织机构应明确标识信息安全保障相关的所有国家、信息安全主管机构、上级部门的法律、法规、政策等的要求，并确保信息系统的设计、操作、使用及管理应符合相关法律、法规或合同中同信息安全相关的要求。

7.2.7.2.3 符合适用的法律、法规、政策（MCM_LCP.2）

应确保信息系统的设计、操作、使用及管理应符合相关法律、法规或合同的安全要求。

应该在信息系统的建设和运行中明确定义和说明所有有关法定的、条例规定的或合同的要求，并明确满足这些要求的特定控制措施和相关责任。

7.2.7.3 标准的符合性（MCM_STP）

7.2.7.3.1 标准的符合性子类介绍

确保信息安全管理工作与国际、国内、行业的相关标准的符合性，以便于同测评机构、开发商和用户之间的有效沟通和结果的互认。

7.2.7.3.2 确定适用的标准（MCM_STP.1）

组织机构应明确、收集和整理信息安全管理工作遵循的国际、国内、行业的相关标准，并保持相关文件的更新。

7.2.7.3.3 符合适用的标准（MCM_STP.2）

组织机构应在系统的建设和运行中遵循适用的国际、国内、行业的相关标准要求。

7.2.7.4 安全策略符合性（MCM_PSP）

7.2.7.4.1 安全策略符合性介绍

组织机构应确保系统符合组织机构的安全策略和安全技术要求。

7.2.7.4.2 安全策略符合性核查（MCM_PSP.1）

管理层应确定在自己负责范围之内正确执行所有安全程序，还要定期检查机构内所有部门，以保证机构的安全策略及标准正确实施。信息系统的拥有者应积极配合接受定期检查。

7.2.7.4.3 技术符合性的检查（MCM_PSP.2）

组织机构应定期检查信息系统安全实施与标准的符合性。

7.2.8 管理保障控制类:信息安全规划管理(MSP)

7.2.8.1 管理保障控制类信息安全规划管理(MSP)介绍

信息安全建设是信息化的有机组成部分,必须与信息化同步规划、同步建设。应在信息系统生命周期的第一个阶段——计划组织阶段,综合考虑信息安全的规划并将其作为信息系统规划的有机组成部分。

7.2.8.2 信息安全规划(MSP_ISP)

7.2.8.2.1 安全保障管理目的介绍

组织机构应建立完善的信息安全规划管理体系,以规划和指导组织机构的信息安全保障工作。

信息安全规划应基于组织机构的业务要求和风险管理的要求,它包括组织机构对信息安全所建立的长期规划和短期规划,这些规划是组织机构整体规划的综合组成部分。

7.2.8.2.2 信息安全长期规划(MSP_ISP.1)

应制定信息安全长期规划。

7.2.8.2.3 信息安全短期规划(MSP_ISP.2)

长期规划制定者应能够将信息安全长期规划合理分解,形成信息安全短期规划。

7.2.9 管理保障控制类:系统开发管理(MSD)

7.2.9.1 管理保障控制类系统开发管理(MSD)介绍

信息安全应贯穿至系统开发的整个生命周期中,组织机构在系统的需求分析、设计、实施和交付中应综合信息安全的考虑。

7.2.9.2 安全需求管理(MSD_SRM)

7.2.9.2.1 安全需求管理子类介绍

组织机构应确保安全是信息系统的必要组成部分。组织机构应在系统开发的需求分析阶段识别系统的所有安全要求,并经商讨后予以文档化,以作为信息系统整个业务的综合组成部分。

7.2.9.2.2 需求分析和规范(MSD_SRM.1)

组织机构应根据信息安全相关法律法规、政策标准的要求和业务需求,在系统开发的需求分析阶段,综合考虑、分析安全需求,并将安全需求分析的结果文档化作为系统开发需求的一个综合组成部分。

7.2.9.3 系统设计管理(MSD_SDM)

7.2.9.3.1 系统设计管理子类介绍

组织机构应根据系统安全需求分析的结果,将系统的安全考虑综合至系统的设计中。

组织机构应能标识出在系统设计过程中潜在的安全风险,为设计说明中的安全性设计提供评判依据,确保系统设计阶段的重要环节均能得到较好的安全风险控制。

7.2.9.3.2 满足安全需求(MSD_SDM.1)

信息系统的设计应能满足需求分析阶段所得出的安全需求。

7.2.9.4 工程实施管理(MSD_ENM)

7.2.9.4.1 工程实施管理子类介绍

实现安全防护体系,满足信息系统安全工程的要求。

7.2.9.4.2 遵循系统设计(MSD_ENM.1)

组织机构应依据系统设计方案,制定工程实施方案。

7.2.9.4.3 工程实施管理(MSD_ENM.2)

应依据工程实施方案,对工程实施过程进行严格控制。

7.2.9.5 交付管理(MSD_IRM)

7.2.9.5.1 交付管理子类介绍

保证信息系统在正式运行之前的完整交付。

7.2.9.5.2 交付验收(MSD_IRM.1)

依据系统验收标准,严格交付验收过程。

7.2.9.5.3 运行审批(MSD_IRM.2)

信息系统在正式运行之前应得到组织机构的授权。组织机构的高级管理人员签署并批准。

7.2.10 管理保障控制类:运行管理(MOP)

7.2.10.1 管理保障控制类运行管理(MOP)介绍

组织机构应建立完善的信息和通信技术运行管理体系,通过访问控制、漏洞管理、审计和监控管理、系统的安全配置以及系统的维护等措施,确保信息处理设施正确、安全地运行。

7.2.10.2 系统漏洞管理(MOP_TVM)

7.2.10.2.1 系统漏洞管理子类介绍

减少来自于已发布的技术漏洞攻击所产生的风险。

7.2.10.2.2 漏洞管理(MOP_TVM.1)

组织结构应以有效的、系统化的和可重复的方式实施技术漏洞管理,并且应采取测量措施以确定其有效性。

7.2.10.2.3 漏洞监控(MOP_TVM.2)

组织结构应及时获得自己所使用信息系统技术漏洞的最新信息。

7.2.10.2.4 漏洞控制(MOP_TVM.4)

一旦已经识别了潜在的技术漏洞,组织机构应标识相关的风险和所要采取的行动,采取及时适当的措施来响应潜在的技术漏洞。

7.2.10.3 逻辑访问控制管理(MOP_LAC)

7.2.10.3.1 逻辑访问控制子类介绍

组织机构应基于业务和安全要求来控制对信息、信息处理设施和业务过程的访问,防止非法访问造成对系统的破坏。

7.2.10.3.2 用户访问控制(MOP_LAC.2)

组织机构应确保只有授权用户才能访问信息系统,禁止未授权访问。

为防止非法访问信息系统和服务,组织机构应根据已有的访问控制要求管理内部和外部人员的访问权限。

7.2.10.3.3 网络访问控制(MOP_LAC.3)

组织机构应制定网络访问控制策略,采用网络隔离、强制路径、用户身份鉴别、网点身份鉴别、网络路由控制、网络服务安全等手段加强网络访问控制。

7.2.10.3.4 操作系统访问控制(MOP_LAC.4)

组织机构应选择安全性较高的操作系统,并对操作系统进行合理配置,保证其访问控制能力。

7.2.10.3.5 应用和信息访问控制(MOP_LAC.5)

敏感系统应有专用的或隔离的计算机环境,并对应用系统的访问进行控制。

7.2.10.4 审计和监控管理(MOP_AMM)

7.2.10.4.1 审计和监控子类介绍

组织机构应充分发挥系统的审计功能,并把其对系统的影响降到最低。

7.2.10.4.2 审计工具的使用(MOP_AMM.1)

在进行审计时,组织机构应采取一些控制措施保护正在使用的系统及审计工具,也应采取一些保护措施来保证审计工具的完整性。应防止滥用审计工具。

7.2.10.4.3 监控系统的使用(MOP_AMM.2)

组织机构应实施对信息处理设施和系统的操作和运行监控,并定期审核监控结果(日志信息)。

7.2.10.4.4 **日志信息保护**(MOP_AMM.3)

应对日志设备和日志信息进行保护防止窜改和非授权访问,以确保获取信息的完整性和真实有效性。

7.2.10.5 **安全配置管理**(MOP_NSM)

7.2.10.5.1 **安全配置管理子类介绍**

确保对系统的网络、网络服务、主机以及应用系统实施安全的规则进行合理配置和管理,避免由于规则配置不当对系统造成威胁和破坏。

7.2.10.5.2 **网络控制**(MOP_NSM.1)

应充分控制和管理网络,以保护免受威胁以及维护使用网络的系统和应用的安全,包括在传送中的信息。

7.2.10.5.3 **网络服务的安全**(MOP_NSM.2)

识别整个网络服务的安全特征、服务级别和管理要求,包括所有网络服务协议,不论这些服务是内部还是外部提供的。

7.2.10.5.4 **主机安全配置**(MOP_NSM.3)

主机的配置应遵循合理的规则和标准。

7.2.10.5.5 **应用系统安全管理**(MOP_NSM.4)

应用系统应设计有适当的访问控制、数据保护、审计跟踪记录或活动日志等安全功能。对投入使用的应用系统,应确保开启了所有安全功能并进行正确配置和使用。

7.2.10.6 **IT运行管理**(MOP_ITM)

7.2.10.6.1 **IT运行管理子类介绍**

组织机构应执行日常的IT运行管理,维护信息和信息处理设施的完整性、可用性、保密性。

7.2.10.6.2 **网络日常监控**(MOP_ITM.1)

定期监控系统的运行状况,及时发现隐患,确保系统的有效运行。

7.2.10.6.3 **信息备份管理**(MOP_ITM.2)

组织机构应备份信息和软件,并根据已定义的备份策略定期测试备份数据。

7.2.10.6.4 **恶意代码的控制**(MOP_ITM.3)

软件和信息处理设施易引入恶意代码,组织机构应保护软件和信息的完整性,防止在系统中引入恶意代码。组织机构应探测、防护和控制恶意代码,并实施正确的用户意识流程。信息系统应使用能够自动更新的恶意代码保护措施。

7.2.10.6.5 **介质的管理**(MOP_ITM.5)

应对信息介质进行有效的控制和物理保护,防止文档、计算机介质(例如:磁带、磁盘)、输入/输出数据和系统文件的非授权暴露、修改、去除和破坏以及对业务活动的中断。

7.2.10.6.6 **文件的管理**(MOP_ITM.6)

对系统文档进行保护,防止未授权访问。

7.2.10.6.7 **计算机设备使用的管理**(MOP_ITM.7)

信息系统计算机设备应在整体设计上通过使用一套优化的方法和过程,能更好地实现服务。系统运行环境中的计算机,应采用规范统一的办法进行管理标识和使用,保持与其他的设备协调一致、正常工作。

7.2.11 **管理保障控制类:业务持续性和灾难恢复管理**(MBD)

7.2.11.1 **管理保障控制类业务持续性和灾难恢复管理**(MBD)**介绍**

业务持续性管理是指通过预防及恢复措施的结合使用,把业务因灾难或安全故障(例如,由于天灾、意外、设备失效及故意破坏)的停顿降到可接受的程度。组织机构应分析灾难、安全故障及服务停顿的影响,以便制订及实施业务持续性和灾难恢复计划来保证业务进程能够在规定时间内恢复。

7.2.11.2 业务持续性管理(MBD_BCM)

7.2.11.2.1 业务持续性管理子类介绍

防止业务过程中断,保护关键业务流程不会受信息系统重大失效或自然灾害的影响,并确保及时恢复。

通过业务持续性管理过程的实施,综合使用预防及恢复控制,把因灾难或安全故障(例如,来自于天灾、意外、设备故障及故意破坏行动)而造成的业务中断降低到可接受的程度。

应分析灾难、安全故障及业务中断的影响。应开发和实施持续性计划以保证业务过程能够在所需的时间范围内恢复。应经常修改和实践这些计划,使之最终变成所有其他管理过程的不可分割的一部分。

7.2.11.2.2 建立业务持续性管理流程(MBD_BCM.1)

组织机构应建立业务持续性管理流程,满足组织机构在信息安全方面的业务持续性需求。

7.2.11.2.3 业务持续管理的组织结构和职责(MBD_BCM.2)

组织机构应建立业务持续性管理组织结构,并明确其职责。

7.2.11.2.4 业务持续性与风险评估(MBD_BCM.3)

组织机构应识别引起业务过程中断的信息安全事件,并分析中断发生的可能性和造成的影响。

7.2.11.2.5 制定和实施业务持续计划(MBD_BCM.4)

应制定和实施业务持续性计划,以确保关键业务过程中断或失效后能够在规定的时间内和要求的等级上恢复系统运行,并确保信息的可用性。

7.2.11.2.6 业务持续规划框架(MBD_BCM.5)

应建立一个单独的业务持续性计划框架,以确保所有计划的一致性,以维护信息安全要求的一致性并识别测试和维护的优先级。

7.2.11.2.7 测试和维护业务持续性计划(MBD_BCM.6)

应该定期测试和更新计划,以确保计划最新且有效。

7.2.12 管理保障控制类:应急响应管理(MER)

7.2.12.1 管理保障控制类应急响应管理(MER)介绍

应急响应管理并有效的解决事故,尽量减少它们对业务的影响,减小类似事故再次发生的风险。

应该按照一种正规的流程来妥善处理各类事件(包括故障、掉电、过载、用户或者计算机工作人员操作失误、违规存取)。

7.2.12.2 汇报安全事件和安全漏洞(MER_REW)

7.2.12.2.1 汇报安全事件和安全漏洞子类介绍

确保能够及时通报同信息系统有关的安全事件和漏洞。

7.2.12.2.2 信息安全事件报告(MER_REW.1)

应通过恰当的管理途径尽快报告信息安全事件。确保与信息系统相关的安全事件和漏洞信息能够传达到每个人,并能够及时采取正确的行动。

应该有事件汇报和改进流程。所有员工和第三方用户应该知道不同类型安全事件和漏洞信息的汇报流程。要求信息安全事件和漏洞信息应该尽快汇报给指定的联系方。

7.2.12.2.3 报告信息安全漏洞(MER_REW.2)

应要求所有的员工、承包方和第三方用户注意并报告系统或服务中已发现或疑似的安全漏洞。

7.2.12.3 应急响应管理(MER_IMI)

7.2.12.3.1 应急响应管理子类介绍

确保使用持续有效的方法管理信息安全事故。

7.2.12.3.2 职责和程序(MER_IMI.1)

应建立管理职责和程序,以快速、有效和有序地响应信息安全事故。

7.2.12.3.3 应急预案的制定与定期演习(MER_IMI.2)

应制定并实施应急预案计划、应急预案定期演习、灾难恢复定期演练。

7.3 安全保障工程要求

7.3.1 工程保障控制类:风险过程(PRM)

7.3.1.1 系统定义(PRM_SDF)

7.3.1.1.1 工程保障目标

系统定义工程保障控制子类的目标是识别网上证券交易系统的任务和使命,即系统的任务要求和它所要达到的能力,这些能力包括系统应执行的功能、所需的接口及这些接口相关的能力、所要处理的信息、所支持的运行结构以及运行的威胁等。

7.3.1.1.2 详细系统描述(PRM_SDF.1)

描述网上证券交易系统的目的、任务和使命;网上证券交易系统的信息类划分、边界、信息流;网上证券交易系统的业务体系、技术体系和管理体系等。

7.3.1.2 评估威胁(PRM_ATT)

7.3.1.2.1 工程保障目标

评估威胁工程保障控制子类的目标是对网上证券交易系统安全的威胁进行标识和特征化。

本工程保障控制子类产生的威胁信息将与评估脆弱性得到的脆弱性信息以及评估影响得到的影响信息一起用于评估安全风险中。虽然收集威胁、脆弱性和影响信息的活动被分组为几个单独的过程域,但它们是互相依赖的。其目标是要得到足以用作判定的威胁、脆弱性和影响的组合。因此,确定威胁调查的范围应结合相应的脆弱性和影响。

威胁容易变化,所以必须定期监视威胁,以确保一直维持理解本过程域产生的结果。

7.3.1.2.2 标识自然威胁(PRM_ATT.1)

标识由自然原因引起的威胁。

由自然原因引起的威胁,包括地震、海啸和台风。不过,并非有威胁的所有自然灾害都会在所有地方发生。例如,在大部分内陆中心地带就不可能出现台风。因此,重要的是标识出在特定地方到底会发生哪一种具有威胁的自然灾害。

7.3.1.2.3 标识人为威胁(PRM_ATT.2)

7.3.1.2.3.1 工程保障控制组件控制

标识出无意的或有意的人为原因所引起的威胁。

人为原因引起的威胁基本上有两种:一是由意外原因引起的威胁;二是由有意行为引起的威胁。某些人为威胁在目标环境中并不适用,应在进一步分析后予以取消。

7.3.1.2.4 标识威胁的测量块(PRM_ATT.3)

7.3.1.2.4.1 工程保障控制组件控制

标识特定环境中合适的测量块和适用范围。

大多数的自然威胁和许多人为威胁都有其与之相关的测量块。大多数情况下,整个的测量块并不适用于特定情况。因此,在特定情况下,有时需要最大化事件发生概率、有时需要最小化事件发生的概率,这样考虑才恰当。

7.3.1.2.5 评估威胁源能力(PRM_ATT.4)

评估人为威胁的威胁源的能力和动机。

本工程保障控制组件集确定成功对系统进行攻击的潜在的人类敌对势力的才能和能力。才能指的是敌对者的攻击知识(例如,他们是否拥有知识、经过训练)。能力则衡量一个有才能的敌手能够进行攻击的可能性(例如,他们是否拥有资源)。

7.3.1.2.6 评估威胁的可能性(PRM_ATT.5)

评估威胁事件发生的可能性是怎样的。对自然事件发生的机会以及故意行为或个别意外事件的评

估中，需要考虑多种因素。考虑的诸多因素并不一定要进行计算或衡量，只需要报告中有一致的度量标准。

7.3.1.2.7 **监视威胁及其特征**(PRM_ATT.6)

监视威胁分布情况及威胁特征的不断变化。

任何位置和状态下的威胁分布情况都是动态的。新的威胁可能变得相关，而现有威胁的特征也可能发生变化。因此有规律地监视现有威胁及其特征并检查新的威胁很重要。本工程保障控制组件与标识协调机制(PEN_ISR)中的“监视威胁、脆弱性、影响和环境变化”工程保障控制组件的一般监视活动紧密相连。

7.3.1.3 **评估脆弱性**(PRM_AVL)

7.3.1.3.1 **工程保障目标**

标识和特征化系统的安全脆弱性。

评估安全脆弱性的目标是获得对一给定环境中系统安全脆弱性的理解。

评估安全脆弱性的目的在于标识和特征化系统的安全脆弱性。本工程保障控制组件包括分析系统资产、定义具体的脆弱性，以及系统脆弱性的全面评估。与安全风险和脆弱性评估相关的术语因上下文环境而不同。在本标准中，“脆弱性”除了传统所说的弱点、安全漏洞或可能被威胁攻击的系统中的信息流外，还指系统可能被恶意利用的方面。这些脆弱性独立于任何特定的威胁或攻击。可以在系统的生命周期中的任何时候执行这一系列脆弱性评估活动，来支持在已知环境中的对系统进行开发、维护或运行等决策。

7.3.1.3.2 **选择脆弱性分析方法**(PRM_AVL.1)

选择用于标识和特征化给定环境中安全系统脆弱性的方法、技术和标准。

包括定义系统建立安全脆弱性的方法，这种方法允许标识和特征化安全脆弱性，包括根据威胁及其可能性、运行功能、安全要求或其他相关过程域对脆弱性进行分类和优先级排列。通过标识分析的深度和广度，安全工程师和顾客可以确定评估范围是否包括目标系统以及分析的全面性。应在预先安排和指定时间内，在一个已知的并记录有配置的框架内进行分析。分析的方法论应包括预期结果，应清楚地描述分析的具体目标。

7.3.1.3.3 **标识脆弱性**(PRM_AVL.2)

标识系统安全脆弱性。

系统的安全和非安全的相关部分中都可能存在系统脆弱性。支持安全功能或与安全机制配合的非安全机制中经常有可利用的脆弱性。应遵循选择脆弱性分析方法(PRM_AVL.1)中的攻击场景方法，以便能确认脆弱性。应记录发现的所有系统脆弱性。

7.3.1.3.4 **收集脆弱性数据**(PRM_AVL.3)

脆弱性具有其自身的性质，本工程保障控制组件意在收集与这些性质相关的数据。脆弱性的测量块可以与 PRM_ATT.3“标识威胁的测量块”中的威胁的测量块相同。应标识并收集脆弱性被利用的难易程度以及脆弱性出现的可能性的数据。

7.3.1.3.5 **合成系统脆弱性**(PRM_AVL.4)

评估系统脆弱性并将特定脆弱性及各种特定脆弱性的组合结果进行综合收集。

分析脆弱性或脆弱性的组合会让系统产生的问题。应分析脆弱性的附加特征，例如脆弱性被利用的可能性以及成功利用脆弱性的机会。分析结果也可包括处置合成的脆弱性的推荐方法。

7.3.1.3.6 **监视脆弱性及其特征**(PRM_AVL.5)

监视脆弱性的不断变化及其特征的变化。

任何位置和状态下的脆弱性分布情况都是动态的。新的脆弱性会变得有相互关系、现有脆弱性的特征可能变化。因此，监视现有脆弱性及其特征并定期检查新的脆弱性很重要。本工程保障控制组件与 PEN_MSP.2 监视威胁、脆弱性、影响、风险和环境变化的一般监视活动紧密相连。

7.3.1.4 **评估影响**(PRM_AIM)

7.3.1.4.1 **工程保障目标**

评估影响的目标在于标识对系统的影响，并评估影响发生的可能性。影响可能是有形的，例如收入的损失或经济惩罚；也可能是无形的，例如声誉和信誉的损失。

本工程保障控制子类的目标是标识和特征化风险对系统的安全影响。

7.3.1.4.2 **对影响进行优先级排列**(PRM_AIM.1)

标识、分析并优先级排列系统的运行、业务或任务，也应考虑对业务战略的影响。这将可能改变和缓解组织可能遭受的影响，进而会改变其他控制子类或组件得出的风险优先级排列次序。因此当计算潜在影响时把这些影响包括在内很重要。本组件与 PEN_ISR“确定安全要求”的活动相关。

7.3.1.4.3 **标识系统资产**(PRM_AIM.2)

标识支持系统的安全目标或关键能力(运行，业务或任务功能)所必需的系统资源和数据。通过评估给定环境中每项资产提供支持的重要性，来定义每项资产。

7.3.1.4.4 **选择影响的度量**(PRM_AIM.3)

选择用于评估影响的度量。

有许多度量标准可用来衡量事件的影响。最好预先确定哪种度量标准适用于当前的特定系统。

7.3.1.4.5 **标识度量关系**(PRM_AIM.4)

标识所选评估影响的度量标准之间的关系以及所需度量标准转换因子。

评估影响可能需要使用不同的度量标准。必须找出不同度量标准之间的关系，以保证在整个影响评估中对所有暴露所使用方法的一致性。有时，有必要把各种度量标准方法组合起来，以便能够产生出统一的结果。因此需要建立产生统一结果的方法。这通常因系统不同而不同。当使用定性的度量标准时，在综合阶段也需要有定性因子合并的指南。

7.3.1.4.6 **标识和特征化影响**(PRM_AIM.5)

利用多重度量标准或统一度量标准标识和特征化意外事件的意外影响。

从 PRM_AIM.1(对影响进行优先级排列)和 PRM_AIM.2(标识系统资产)中标识出的资产和能力出发标识出产生损害的后果。对于每种资产，后果可能为损坏、泄密、不通或消失。对能力的影响可能包括中断、延迟或削弱。

创建了相对完整的度量关系表之后，可以使用在 PRM_AIM.3(选择影响的度量)和 PRM_AIM.4(标识度量关系)中标识出的度量来特征化影响。这一步需要研究精算表、年鉴或其他资源。还应考虑每种影响的度量的不确定性。

7.3.1.4.7 **监视影响**(PRM_AIM.6)

监视影响的不断变化。

任何位置和状态下，影响都是动态的。新的影响可能产生相互关系。因此，监视现有影响并定期检查新的影响很重要。本工程保障控制组件与 PEN_MSP.2 监视威胁、脆弱性、影响、风险和环境变化的一般监视活动紧密相连。

7.3.1.5 **评估安全风险**(PRM_ASR)

7.3.1.5.1 **工程保障目标**

评估安全风险的目标是标识给定环境中系统的安全风险，并按照既定方法论对风险进行优先级排列。本安全保障控制子类着重要基于对能力情况以及资产相对威胁的脆弱情况的理解来确定这些风险。本活动特别包括标识和评估暴露发生的可能性。“暴露”是指会造成重大损害的威胁、脆弱性和影响的组合。可以在系统的生命周期中的任何时候执行这一系列风险评估活动，来支持在已知环境中的对系统进行开发、维护或运行等决策。

7.3.1.5.2 **选择风险分析方法**(PRM_ASR.1)

选择在给定环境中分析、评估、比较和优先级排列系统的安全风险的方法、技术和标准。

本组件定义用于标识给定环境中系统安全风险的方法，可以用这种方法分析、评估和比较安全风险。应该依据威胁、运行功能、系统脆弱性、潜在损失、安全需求等相关问题，得到对风险进行分类和分级的方案。

7.3.1.5.3 标识暴露(PRM_ASR.2)

标识威胁、脆弱性、影响三元组(暴露)。

标识暴露的目的在于找出威胁和脆弱性的组合中的相关项，进而标识出现威胁和脆弱性造成的影响。在选择系统保护措施时必须考虑这些暴露。

7.3.1.5.4 评估暴露的风险(PRM_ASR.3)

评估每项暴露的风险。

标识暴露出现的可能性。

7.3.1.5.5 评估总体不确定性(PRM_ASR.4)

评估暴露的风险的总体不确定性。

每项风险本身都具有不确定性。总体的风险不确定性是 PRM_ATT.5(评估威胁的可能性)、PRM_AVL.3(收集脆弱性数据)、PRM_AIM.5(标识和特征化影响)中所标识的威胁、脆弱性、影响及其特征的不确定性的总和。本组件与"PAS_EAE 建立保证论据"中的作为保障可以改变和降低不确定性的活动紧密相关。

7.3.1.5.6 风险优先级排列(PRM_ASR.5)

按优先级排列风险。应根据组织优先级、发生的可能性、所具有的不确定性和可用资金来对已标识的风险进行排序。可以降低、避免、转移或接受风险，也可以组合使用这些风险处理方式。降低，可以针对威胁、脆弱性、影响或风险本身。应根据 PEN_MSC"确定安全要求"中标识的风险承担者的需求、业务优先级和整体系统架构来选择处理方式。

7.3.1.5.7 监视风险及其特征(PRM_ASR.6)

监视风险分布情况的不断变化及其特征的变化。

任何情形下风险的分布情况都是动态的。新的风险可能变得相互关联，同时现存风险的特征可能变化。因此，监视现存风险及其特征、定期检查新的风险很重要。本组件与 PEN_MSP.2 "监视威胁、脆弱性、影响、风险和环境的变化"中的一般监视活动密切相关。

7.3.2 安全工程保障控制类：工程过程(PEN)

7.3.2.1 确定安全要求(PEN_ISR)

7.3.2.1.1 工程保障目标

确定安全要求的目标是要明确地标识系统的安全需求。确定安全要求涉及定义系统的安全基础，以满足所有法律、策略和组织的安全要求，这些需求根据预期的系统运行安全环境上下文、组织当前安全性和系统环境、标识出的一系列安全目标进行裁剪。定义一系列系统安全要求作为批准系统安全的基线。

确定安全要求的目标是包括客户在内的各方对安全需求达成共同理解。

7.3.2.1.2 获得对客户安全需求的理解(PEN_ISR.1)

应获得对客户安全需求的理解。

本工程保障控制组件的目的是要收集全面理解客户的安全需求所需的所有信息。这些需求受到安全风险对客户的重要性的影响。系统将要运行的预期环境也影响客户的安全需求。

7.3.2.1.3 标识可用的法律、策略和约束(PEN_ISR.2)

应标识出管理系统的法律、策略、标准、外部影响和约束。

本工程保障控制组件的目的是要收集所有影响到系统安全的所有外部影响。适用性的决定应标识支配系统预期环境的法律、规章、策略和商业标准。应决定全局和本地策略之间优先权。必须标识出系统客户设置于系统的安全要求，并提炼隐含的安全要求。

7.3.2.1.4 **标识系统安全关联性**(PEN_ISR.3)

标识系统的用途以便确定安全上下文环境。

本工程保障控制组件的目的是要标识系统上下文如何影响安全。这涉及理解系统的用途。为安全考虑描述所处理的任务和运行场景。本阶段需要对系统面临的或可能遭受的威胁的高层理解。为可能对安全的影响而描述性能和功能要求。为隐含的安全要求而检查运行约束条件。

环境可能也包括与其他组织或系统的接口,以便定义系统的安全边界。确定接口的要素包括安全边界的内部和外部。

许多组织外部的因素也不同程度影响组织的安全需求。这些因素包括政治倾向以及政治焦点的变化、技术开发、经济影响、全球事件和信息战。由于这些因素都不是静态的,需要监视和定期评估变化带来的潜在影响。

7.3.2.1.5 **收集系统运行的安全思想**(PEN_ISR.4)

收集系统运行的高层安全思想。

本工程保障控制组件的目的是要开发整个企业的高层安全思想,包括角色、职责、信息流、资产、资源、人员保护和物理保护。此描述应包括讨论如何在系统要求的约束下管理企业。特别在运行安全概念中提供系统的这一思想,应包括系统架构、规程和环境的高层安全思想。系统开发环境的要求也在本阶段获得。

7.3.2.1.6 **收集安全的高层目标**(PEN_ISR.5)

收集定义系统安全性的高层目标。

本基本实践的目的是要标识应满足怎样的安全目标,以便为系统在其运行环境中提供足够的安全性。在 PAS_EAF"建立保证证据"中确定的系统的保障目标,可能影响安全目标。

7.3.2.1.7 **定义安全相关需求**(PEN_ISR.6)

定义一致的一系列要求,这些要求定义了系统所执行的保护的说明。

本工程保障控制组件的目标是要定义系统的安全要求。本实践应确保每项要求都与适用的策略、法律、标准、安全要求和系统的约束相一致。这些要求应完整定义系统的安全需求,包括非技术性的要求。通常需要定义或指定对象的逻辑或物理边界,以确保涵盖了所有方面。要求应与系统的目标影射或关联。应清晰简明地规定安全要求且不应互相矛盾。只要可能,安全应最小化对系统功能和性能的影响。安全要求应为评估系统在其预期环境中的安全性能提供基础。

7.3.2.1.8 **达成安全协议**(PEN_ISR.7)

达成对具体安全要求符合客户需求的协议。

本工程保障控制组件的目的是要在各方之间达成安全要求的共识。标识出一般客户群而非特定客户时,要求应满足一系列目标。指定的安全要求应是管理策略、法律和用户需求的完整、一致的反映。应标识出问题并再处理直到达成共识。

7.3.2.2 **高层安全设计**(PEN_HSD)

7.3.2.2.1 **工程保障目标**

信息系统的高层安全设计包括系统的体系结构、设计和实现的需求,制定相应的设计原则和建议、安全体系结构建议、保护的原则,得到安全模型、安全体系结构,进行可靠性分析:确定所有的安全机制都能对应到高层安全设计,并且所有的高层安全设计都有具体的安全机制来保证。

7.3.2.2.2 **设计安全模型**(PEN_HSD.1)

为当前特定的信息系统设计安全模型,描述系统的安全原理。

7.3.2.2.3 **设计安全体系结构**(PEN_HSD.2)

为当前特定的信息系统设计安全体系结构。

7.3.2.3 详细安全设计(PEN_DSD)

7.3.2.3.1 工程保障目标

本工程保障控制类信息系统安全工程师分析设计的约束条件,分析折衷办法,进行详细的系统和安全设计并考虑生命周期支持。信息系统安全工程师检查所有系统安全需求落实到了组件。最终的详细安全设计结果为实现系统提供充分的组件和接口描述信息。

7.3.2.3.2 分配安全机制(PEN_DSD.1)

将高层设计中的思想落实为具体的安全机制。

7.3.2.3.3 确定安全产品(PEN_DSD.2)

根据高层设计和分配的安全机制等要求,从可选的安全产品中选择最适合的产品。

7.3.2.3.4 系统接口设计和优化(PEN_DSD.3)

对系统设计中的接口进行设计和优化。

7.3.2.3.5 提供安全工程指南(PEN_DSD.4)

为参与工程的各方提供安全工程指南。

7.3.2.4 安全工程实施(PEN_SEE)

7.3.2.4.1 工程保障目标

本工程保障控制类信息系统安全工程师把系统设计转移到运行、参与对所有系统问题的多学科综合分析,并为认证认可活动提供输入。例如验证系统已经实现了对抗威胁评估中识别出的威胁;追踪与系统实现和测试活动相关的信息保护保障机制;为系统生命周期支持计划、运行规程、培训材料维护提供输入。

7.3.2.4.2 工程的实施(PEN_SEE.1)

按照项目计划和具体实施方案进行安全工程的实施。

7.3.2.4.3 系统的试运行(PEN_SEE.2)

对完成的安全系统进行试运行。

7.3.2.4.4 系统的测试(PEN_SEE.3)

制定测试计划、对所完成的系统进行安全测试。

7.3.2.4.5 工程的交付(PEN_SEE.4)

系统交付给用户,包括相关的说明和指南等。

7.3.2.4.6 安全培训(PEN_SEE.5)

对用户进行系统安全及安全运行维护相关知识的培训。

7.3.2.4.7 提供用户指南(PEN_SEE.6)

向运行系统的用户和管理员提供安全指南。

本工程保障控制组件的目的是要开发安全指南并提供给系统用户和管理员。本运行指南告诉用户和管理员安全地安装、配置、操作和废弃系统必须做什么。为确保这成为可能,应在生命周期早期开始开发运行安全指南。

7.3.2.5 提供安全输入(PEN_PSI)

7.3.2.5.1 工程保障目标

提供安全输入的目标是为系统架构者、设计者、实施者或用户提供他们所需的安全信息。信息包括安全架构、设计或实施可选方案以及安全指南。应根据 PEN_ISR"确定安全要求"中标识的安全需求,开发、分析、提供并与组织成员协调这些输入。

本工程保障的目标是:

a) 检查与安全相关的所有系统问题,并根据安全目标解决这些问题;

b) 项目组的所有成员都理解安全问题，他们才能各司其职；

c) 解决方案反映了提供的安全输入。

7.3.2.5.2 理解安全输入要求(PEN_PSI.1)

与设计者、开发者以及用户合作来确保参与方对安全输入需求有共同的理解。

安全工程与其他学科相协调来决定有助于那些学科的安全输入的类型。安全输入包括各类指南、设计、文档，以及其他学科需要考虑的与安全相关的概念。输入可以采用多种形式，包括文档、备忘录、电子邮件、培训和咨询。

这些输入基于 PEN_ISR“确定安全要求”中的需求。例如，可能需要为软件工程师开发一系列安全规则。其中一些输入与环境相关更甚于系统。

7.3.2.5.3 确定安全约束和考虑(PEN_PSI.2)

确定工程选择方案所需的安全约束和考虑。

本工程保障控制组件的目标是要标识出用于得出成熟的工程可选方案的所有安全约束和考虑。安全工程组进行分析以确定要求、设计、实施、配置和文档化的所有安全约束和考虑。标识约束可以在系统生命周期的所有时间。可以以多种不同的抽象程度来标识。注意这些约束既可能是积极的(总是如此)，也可能是消极的(决不如此)。

7.3.2.5.4 标识安全选项(PEN_PSI.3)

标识安全工程问题的可选方案。

本工程保障控制组件的目标是要标识安全工程问题的可选方案。本过程是反复进行的，并将安全要求转化到实施中。这些解决方案可以有多种形式，例如架构、模型和原型。本安全工程保障控制组件涉及分解、分析和重组安全要求直至标识出有效的可选解决方案。

7.3.2.5.5 分析工程选项的安全性(PEN_PSI.4)

应用安全约束和考虑来分析和优先级排列工程可选方案。

本工程保障控制组件的目的是要分析和按优先级排列工程可选解决方案。使用确定安全约束和考虑(PEN_PSI.2)中标识出的安全约束和考虑，安全工程师可以评估每个工程可选解决方案并为工程组提出建议。安全工程师也应考虑来自其他工程组的工程指南。

这些工程可选解决方案不局限于已标识出的安全可选解决方案(PEN_PSI.3)，也可以包括来自其他学科的可选解决方案。

7.3.2.5.6 提供安全工程指南(PEN_PSI.5)

向其他工程组提供安全指南。

本工程保障控制组件的目标是要开发安全指南并提供给工程组。工程组使用安全工程指南来做出选择架构、设计和实施的决定。

7.3.2.5.7 提供运行安全指南(PEN_PSI.6)

向运行系统的用户和管理员提供安全指南。

本工程保障控制组件的目的是要开发安全指南并提供给系统用户和管理员。本运行指南告诉用户和管理员安全地安装、配置、操作和废弃系统必须做什么。为确保这成为可能，应在生命周期早期开始开发运行安全指南。

7.3.2.6 监视安全态势(PEN_MSP)

7.3.2.6.1 工程保障目标

监视安全态势的目标是要确保标识和报告所有的违规、尝试违规或可能导致违背安全的错误。监视外部和内部环境的所有可能影响系统安全的因素。

监视安全态势的目标是：

a) 检测和跟踪内部、外部安全事件；

b) 按照策略响应事故；

c) 按照安全目标标识和处理运行安全态势的变更。

7.3.2.6.2 **分析事件记录**(PEN_MSP.1)

分析事件记录来确定事件的起因、如何处理事件，以及将来可能出现的事件。

检查安全相关信息的历史记录和事件记录(由日志记录组成)。应标识感兴趣的事件以及关联事件和各种记录的因素。于是多条事件记录可以被融合为一条记录。

7.3.2.6.3 **监视变化**(PEN_MSP.2)

监视威胁、脆弱性、影响、风险和环境的变化。

检查任何可能正面或负面影响当前安全态势效果的变更。

任何系统实现的安全应与其内部、外部环境相关的威胁、脆弱性、影响和风险相关联。这些都不是静态的，变更会影响系统安全的有效性和适当性。必须监视所有变更，分析变更以评估它们对安全有效性的重要程度。

7.3.2.6.4 **标识安全突发事件**(PEN_MSP.3)

标识安全相关的事故。

确定是否发生了安全事故，标识详细情况，如果有必要的话产生一份报告。检测安全事故可能使用历史事件数据、系统配置数据、完整性工具和其他的系统信息。由于某些事故的发生持续一段很长的时间，所以此分析很可能要随时间推移对比系统的状态。

7.3.2.6.5 **监视安全防护措施**(PEN_MSP.4)

监视安全保护措施的性能和功能的有效性。

检查保护措施的性能，以标识保护措施性能的变化。

7.3.2.6.6 **评审安全态势**(PEN_MSP.5)

检查系统的安全态势来标识必要的变更。

系统的安全态势会因威胁环境、运行需求和系统配置的变化而变化。本实践复查实施安全的原因，以及其他原则实施安全的要求。

7.3.2.6.7 **管理安全突发事件响应**(PEN_MSP.6)

管理对安全突发事件的响应。

通常，系统的持续可用性是很关键的。许多事件不能预防，因此响应破坏的能力是必需的。应急计划要求标识系统失去功能性的最长时间；标识系统功能的关键元件；标识和开发恢复战略和计划；计划的测试；计划的维护。

有时，意外事件计划包括事故响应和对抗敌对源(例如病毒、黑客等)的活动。

7.3.2.6.8 **保护安全监视的记录数据**(PEN_MSP.7)

确保适当地保护安全监视的记录数据。

如果监视活动的结果不可靠那么就没意义了。本活动包括相关日志、审计报告及相关分析的封装和归档。

7.3.2.7 **管理安全控制**(PEN_MSC)

7.3.2.7.1 **工程保障目标**

管理安全控制的目标是确保系统预想的安全已被集成到系统设计中，最终的运行状态中的系统也确实达到了这种安全要求。

管理安全控制的目标是正确配置和使用安全控制措施。

7.3.2.7.2 **建立安全职责**(PEN_MSC.1)

建立安全控制措施的职责和可确认性，并传达到组织中的每个人。

安全的某些方面可以在常规管理框架下进行管理，然而另外一些方面则需要更专业的管理。

规程应确保只可追溯并被授权执行的职责来管理安全问题。也应确保所采用的任何安全控制措施都清晰并持续运作。另外，还应确保无论采用什么组织结构都传达到不仅是组织结构内部而是整个组织范围。

7.3.2.7.3 **管理安全配置**(PEN_MSC.2)

管理系统安全控制措施的配置。

所有设备的安全配置都需要管理。最佳基本实践认为系统安全很大程度上依赖于相关的组件(硬件、软件和规程)，常规的配置管理不能了解使系统安全所需的相互依赖关系。

7.3.2.7.4 **管理安全意识、培训和教育大纲**(PEN_MSC.3)

管理所有用户和管理员的安全意识、培训和教育程序。

所有员工的安全意识、培训和教育需要以与其他意识、培训和教育相同的方式进行管理。

7.3.2.7.5 **管理安全服务及控制机制**(PEN_MSC.4)

管理对安全服务和控制机制的定期维护和管理。

安全服务和机制的一般管理类似于其他服务和机制的管理。包括保护服务和机制不受有意或无意的破坏的措施，成文时要符合法律和策略的要求。

7.3.2.8 **协调安全**(PEN_COS)

7.3.2.8.1 **工程保障目标**

协调安全的目的是确保各方了解并参与到安全工程活动中。安全工程不可能孤立地取得成功，所以本活动很关键。协调包括在所有项目人员和外部组之间保持开放的沟通。可以使用各种机制在各方之间协调和沟通安全工程的决定和建议，这些机制包括备忘录、文档、电子邮件、会议和工作小组。

协调安全的目标：

a) 项目组的所有成员深入了解并参与到安全工程活动中以发挥其作用；

b) 沟通和整理安全决定和建议。

7.3.2.8.2 **定义协调目标**(PEN_COS.1)

定义安全工程协调目标和相互关系。

许多组需要了解并参与到安全工程活动中。通过检查项目结构、信息需求和项目要求，决定与这些组共享信息的目标。建立与其他组的关系和义务。成功的关系有很多种形式，但必须所有参与方接受。

7.3.2.8.3 **标识协调机制**(PEN_COS.2)

标识安全工程的协调机制。

有很多方法可以在所有工程组中共享安全工程的决定和建议。本活动标识项目安全协调的不同方法。

很多安全人员在同一个项目工作是很常见的。在这种情况下，所有安全工程师应朝一个共同的目标努力工作。需要如此进行接口标识、安全机制选择、培训和发展工作，以确保放入运行系统中时每个安全组件都按预期运行。另外，所有安全工程组必须理解安全工程工作和工程活动，以便清晰地将安全集成到系统中。客户也必须了解安全相关的事件和活动，以确保标识并适当处理要求。

7.3.2.8.4 **促进协调**(PEN_COS.3)

促进安全工程协调。

成功的关系有赖于良好促进。不同优先权的不同组之间的沟通可能会产生冲突。本工程保障控制组件确保以恰当的、建设性的方式解决争端。

7.3.2.8.5 **协调安全决定和建议**(PEN_COS.4)

用标识出的机制去协调有关安全的决定和建议。

本基本实践的目的在于在各种安全工程组织、其他工程组织、外部实体及其他合适的部门中沟通安全决定和建议。

7.3.3 安全工程保障控制类：保障过程(PAS)

7.3.3.1 验证和确认安全(PAS_VVS)

7.3.3.1.1 工程保障目标

验证和确认安全的目的是要确保解决方案验证和确认了安全。通过观察、演示、分析和测试，根据安全要求、架构和设计来验证解决方案。根据客户的运行安全需求来确认解决方案。

验证和确认安全的目标：

a) 解决方案满足安全要求；

b) 解决方案满足用户的运行安全需求。

7.3.3.1.2 标识验证和确认的目标(PAS_VVS.1)

标识用于验证和确认的解决方案。

本工程保障控制组件的目的是要分别标识验证和确认的对象。验证说明正确实施了解决方案，而确认说明解决方案是有效的。这涉及在整个生命周期与所有工程组协调。

7.3.3.1.3 定义验证和确认方法(PAS_VVS.2)

定义验证和确认每种解决方案的方法及严密程度。

本工程保障控制组件的目标是要定义验证和确认每种解决方案的方法及严密程度。标识方法涉及选择如何验证和确认每项要求。严密程度应表明验证和确认工作的详细审查应如何严格，同时也受到来自 PAS_EAE"建立保证证据"的保障战略的输出的影响。例如，有些项目可能要求粗略检查与要求的一致性，而另外一些可能要求更严格的检查。

方法学也应包括：从客户运行安全需求、到安全要求、到解决方案、到验证和确认结果的持续可追溯的方法。

7.3.3.1.4 执行验证(PAS_VVS.3)

验证解决方案贯彻了先前抽象的要求。

本工程保障控制组件的目标是要验证解决方案是正确的，通过说明它实现了先前抽象的要求，包括 PAS_EAE"建立保证证据"中的保障要求。有很多验证要求的方法，包括测试、分析、观察和演示。所使用的方法在 PAS_VVS.2"定义验证和确认的方法"中标识。不仅要检查单独的要求，还要检查整体系统。

7.3.3.1.5 执行确认(PAS_VVS.4)

确认解决方案，表明解决方案满足了先前抽象的需求，最终满足了客户的运行安全需求。

本工程保障控制组件的目的是要确认解决方案满足先前抽象的需求。确认说明解决方案有效地满足了这些需求。有很多方法确认满足了这些需求，包括在运行或典型测试设置环境中测试解决方案。所使用的方法在 PAS_VVS.2"定义验证和确认的方法"中标识。

7.3.3.1.6 提供验证和确认的结果(PAS_VVS.5)

为其他工程组收集验证和确认结果。

本工程保障控制组件的目标是要收集并提供验证和确认的结果。应以易于理解和使用的方式提供验证和确认的结果。应追溯结果，以表明从需求、到要求、到解决方案和到测试结果的可追溯性没有丧失。

7.3.3.2 建立保证证据(PAS_EAE)

7.3.3.2.1 工程保障目标

建立保证论据的目标是要清楚地传达已经满足了客户的安全需求。保证论据是一系列固定的保证

目标，这些保证目标由来自各种来源和抽象程度的保障证据的组合所支持。

本过程包括标识和定义保证要求；证据的产生和分析活动；以及支持保证要求所需的其他证据活动。另外，要收集、包装和准备呈现这些活动收集到的证据。

本安全保障控制子类的目标是工作产品和过程清楚地提供已经满足了客户安全需求的证据。

7.3.3.2.2 **标识保证目标**(PAS_EAE.1)

由客户确定保证目标，标识系统所需的信心度。系统安全保证目标描述贯彻系统安全策略的信心度。目标的充分性由开发者、集成者和客户确定。

标识新的以及修改已有的安全保证目标要与所有安全组织协调一致，包括工程组织内的组以及工程组织外的组(例如，客户、系统安全认证者、用户)。

安全保证目标要更新以反映变更。修改安全保证目标的变更，例如：客户、系统安全认证者或用户可接受的风险级别的变更，需求或需求的解释的变更。

必须沟通以明确安全保证目标。如有必要应适当进行解释。

7.3.3.2.3 **定义保证策略**(PAS_EAE.2)

定义所有保证目标对应的安全保证策略。

安全保证策略的目标是要规划并确保实施和正确贯彻安全目标。通过安全保证策略的实施产生的证据应对系统安全度量足够管理安全风险有适度信心。需要通过安全策略的开发和制定，有效地管理保证活动。提早标识和定义保证需求是产生必要的支撑证据的关键。通过持续的外部协调、理解和监视客户保障需求的满意度，确保高质量的保障。

7.3.3.2.4 **控制保证证据**(PAS_EAE.3)

标识和控制安全保证证据。

通过与所有安全工程过程域交互作用来标识不同抽象程度的证据，按照安全保证策略中所定义的那样收集安全保证证据。控制这些证据以确保已有工作产品流行开来以及与安全保证目标的相关性。

7.3.3.2.5 **分析证据**(PAS_EAE.4)

安全保障证据的分析。

进行保证证据分析，以提供这样的信心：收集的证据满足安全目标进而满足客户的安全需求。保证证据的分析决定若要推断满意地实施了安全特征和机制，系统安全工程和安全验证过程是否足够充分和全面。另外，分析证据以确保工程结果相对基线系统是全面、正确的。如果保证证据不充分，这种分析可能有必要对系统和支撑安全目标的安全工作产品及过程进行修正。

7.3.3.2.6 **提供保证证据**(PAS_EAE.5)

提供说明满足了客户的安全需求的安全保障论据。

开发全面的保证论据来说明与安全保证目标一致并提供给客户。保证论据是一系列固定的由不同抽象程度的保证证据组合支撑的保障目标。应检查保证论据的证据展示的不足和满足安全保证目标的不足。

附 录 A
（规范性附录）
网上证券系统信息安全保障符合性

信息安全保障必须从信息系统（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）出发，结合系统的特点，以风险和策略为出发点和核心，通过在信息系统生命周期中对技术、工程、管理和人员进行保证，确保信息的保密性、完整性和可用性特征，从而实现和贯彻组织机构策略并将风险降低到可接受的程度，达到保护信息和信息系统资产，从而保障实现系统使命的最终目的。

信息系统安全保障符合性声明是信息系统安全保障要求进行评估的依据。这些依据将支持：本要求是一个完整、紧密结合的要求集合，满足本要求的 TOE 在安全环境内提供一组有效的信息系统安全模型。

本符合性声明包含两部分：

——安全保障目的符合性声明：描述了第 6 章 安全保障目的中所描述的安全目的可追溯到第 3 章 安全环境中所指明的假设、威胁和策略中所指明的所有方面，并能覆盖所有这些方面。

——安全保障要求符合性声明：描述了第 7 章 安全保障要求中所提出的技术、管理和工程要求是满足第 6 章 安全保障目的中所描述的安全保障目的。

A.1 安全保障目的符合性声明

信息系统涉及技术、管理和工程，因此需要建立信息系统安全目的同技术、管理和工程目标的对应表，将信息系统安全目的分解为技术、管理和工程目标。表 A.1“安全保障技术目标与威胁、策略的对应表”和表 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”说明了技术、管理和工程的安全目标能对应所有可能的威胁和组织安全策略：即每一种威胁和组织安全策略都至少有一个或一个以上安全目标与其对应，因此是完备的；没有一个安全目标没有相应的威胁和组织安全策略与之对应，这证明每一个安全目标都是必要的；没有多余的安全目标不对应威胁和组织安全策略，因此说明了安全目标是充分的。

A.2 安全保障要求符合性声明

表 A.3“安全保障技术目标和安全保障技术要求映射”、表 A.4“安全保障管理目标和安全保障管理要求映射”和表 A.5“安全保障工程目标和安全保障工程要求映射”说明了安全要求的充分必要性基本原理，即每一个安全目标都至少有一个安全要求（包括功能要求或保证要求）组件与其对应，每一个安全要求都至少解决了一个安全目标，因此安全要求对安全目标而言是充分和必要的。

表 A.1　安全保障技术目标与威胁、策略的对应表

威胁、策略	安全保障技术目标																															
	OT-1	OT-2	OT-3	OT-4	OT-5	OT-6	OT-7	OT-8	OT-9	OT-10	OT-11	OT-12	OT-13	OT-14	OT-15	OT-16	OT-17	OT-18	OT-19	OT-20	OT-21	OT-22	OT-23	OT-24	OT-25	OT-26	OT-27	OT-28	OT-29	OT-30	OT-31	OT-32	OT-33
T-1	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√		√	√								√	
T-2				√						√				√			√	√															√
T-3										√	√						√	√	√			√											
T-4														√		√																	
T-5																					√												
T-6												√																					
T-7												√	√	√	√																		
T-8											√										√				√		√						
T-9											√																						√
T-10						√	√				√	√	√	√	√						√												√
T-11	√	√	√									√																			√		
T-12														√																			
T-13										√												√											
T-14		√				√	√					√												√							√		√
T-15				√						√											√	√			√			√					√
T-16																																	
T-17	√																								√	√				√			
T-18	√		√																							√				√			
T-19																															√		
T-20																															√		
T-21																√							√										√
T-22												√		√							√		√										√

表 A.10(续)

威胁 策略	安全保障目标																																
	O.1	O.2	O.3	O.4	O.5	O.6	O.7	O.8	O.9	O.10	O.11	O.12	O.13	O.14	O.15	O.16	O.17	O.18	O.19	O.20	O.21	O.22	O.23	O.24	O.25	O.26	O.27	O.28	O.29	O.30	O.31	O.32	O.33
T.24											√	√	√	√							√												√
T.25										√									√		√												
T-26										√														√									
T-27										√							√	√		√													
T-28									√									√							√		√						
T-29				√	√																												√
P-1	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
P-2	√	√		√	√	√	√	√	√			√																					
P-3	√	√		√	√					√	√									√	√	√	√		√		√						
P-4	√																			√	√		√				√		√		√		
P-5										√	√						√	√	√														
P-6																√																	
P-7	√		√					√	√											√						√	√			√		√	
P-8	√															√																	√
P.9						√	√		√			√		√	√	√								√									
P.10										√	√																						
P.11		√																														√	√
P.1												/	/		√																		
P.1.												/										√											
P.11											/						√	√	/					√			√						
P.1.											/						√	√	/		√												
P.16	√	√	√													√																	

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

威胁、策略	安全保障管理目标、安全保障工程目标																		
	OM-1	OM-2	OM-3	OM-4	OM-5	OM-6	OM-7	OM-8	OM-9	OM-10	OM-11	OM-12	OM-13	OP-1	OP-2	OP-3	OP-4	OP-5	OP-6
T-1		√				√					√			√	√	√	√	√	√
T-2		√				√			√										√
T-3		√				√			√										√
T-4		√				√	√												√
T-5		√				√				√									
T-6		√	√						√										
T-7	√	√	√																
T-8		√	√					√		√									
T-9		√																	√
T-10		√							√	√	√								
T-11		√								√			√						
T-12		√																	
T-13		√				√													√
T-14		√											√						
T-15		√	√						√				√						
T-16		√							√				√						
T-17		√							√										
T-18		√							√										
T-19		√							√				√						
T-20		√											√						
T-21													√						
T-22		√							√	√									

表 A.2(续)

威胁、策略	安全保障管理目标、安全保障工程目标																		
	OM-1	OM-2	OM-3	OM-4	OM-5	OM-6	OM-7	OM-8	OM-9	OM-10	OM-11	OM-12	OM-13	OP-1	OP-2	OP-3	OP-4	OP-5	OP-6
T-23		√				√													
T-24		√							√										
T-25		√							√										
T-26		√							√										
T-27		√				√			√										
T-28		√							√										
T-29		√				√			√										
P-1	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
P-2		√											√						
P-3		√								√			√						
P-4		√											√						
P-5		√											√						
P-6		√											√						
P-7		√											√						
P-8		√				√							√	√	√	√	√	√	√
P-9		√									√		√						
P-10		√									√		√						
P-11		√											√					√	
P-12	√	√	√										√						
P-13		√											√						
P-14		√	√						√			√	√						
P-15		√											√						
P-16		√		√									√						

表 A.3　安全保障技术目标和安全保障技术要求映射

安全保障技术目标		安全保障技术要求																							
		FDP_ACC	FDP_ACF	FDP_DAU	FDP_IFC	FDP_IFF	FDP_ITC	FDP_RIP	FDP_UCT	FDP_UIT	FDP_ETC	FDP_SDI	FIA_UID	FIA_ATD	FIA_SOS	FIA_UAU	FIA_AFL	FIA_USB	FCO_NRO	FCO_NRR	FPT_ITC	FPT_ITI	FPT_RPL	FPT_SEP	FPT_SSP	FPT_STM	FPT_TDC
序号		1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.
端到端	OT-1					√							√	√													√
	OT-2	√														√			√	√	√	√			√		√
	OT-3						√																			√	
	OT-4		√	√																							
	OT-5		√	√	√																						
	OT-6					√			√				√	√	√											√	
	OT-7					√			√				√	√	√											√	
	OT-8																		√							√	√
	OT-9	√	√																							√	
本地计算环境	OT-10	√	√			√																					√
	OT-11	√				√						√									√	√					√
	OT-12																									√	
	OT-13	√	√	√																							
	OT-14		√	√	√																					√	
	OT-15					√			√				√	√	√											√	
	OT-16					√			√				√	√	√												
	OT-17																		√								√
	OT-18							√																			
	OT-19							√																			
	OT-20		√			√																					
系统边界	OT-21		√																								
	OT-22		√																								
	OT-23		√																								
网络基础设施	OT-24					√																				√	
	OT-25																									√	√
	OT-26					√																					√
	OT-27																										
	OT-28		√	√																							
	OT-29		√	√	√																						
	OT-30					√			√				√	√	√												
	OT-31		√			√			√				√	√	√												
支撑性基础设施	OT-32																		√								√
	OT-33																									√	

表 A.3(续)

安全保障技术目标		安全保障技术要求																								
		FPT_AMT	FPT_FLS	FPT_ITT	FPT_RCV	FPT_RVM	FTA_MCS	FTA_TAH	FAU_ARP	FAU_GEN	FAU_SAA	FAU_SAR	FAU_STG	FMT_MOF	FMT_MSA	FMT_SAE	FTP_ITC	FMT_MOF	FMT_MSA	FMT_MTD	FMT_SAE	FMT_SMR	FTP_ITC	FCS_CKM	FCS_COP	FRU_FLT	FRU_RSA
序号		27.	28.	29.	30.	31.	32.	33.	34.	35.	36.	37.	38.	39.	40.	41.	42.	43.	44.	45.	46.	47.	48.	49.	50.	51.	52.
端到端	OT-1																							√			
	OT-2								√																		
	OT-3																							√	√		
	OT-4		√	√																							
	OT-5		√	√	√			√				√															
	OT-6					√					√	√	√					√		√	√	√					
	OT-7					√					√	√	√					√		√	√	√					
	OT-8																						√			√	√
	OT-9																√										
本地计算环境	OT-10																			√							√
	OT-11					√														√							√
	OT-12		√			√																					
	OT-13		√	√																							
	OT-14		√	√	√																						
	OT-15				√	√			√				√	√	√					√							
	OT-16					√			√				√	√	√												
	OT-17				√								√						√								√
	OT-18				√								√														
	OT-19				√																						
系统边界	OT-20												√							√							
	OT-21																			√							
	OT-22																										
	OT-23																										
	OT-24								√	√	√	√	√														
网络基础设施	OT-25																			√							√
	OT-26					√														√					√		√
	OT-27																			√							
	OT-28		√	√																√							
	OT-29		√	√	√															√							
	OT-30					√			√				√	√	√					√							
	OT-31					√			√				√	√	√					√							
支撑性基础设施	OT-32																		√					√	√		√
	OT-33								√	√	√	√	√														

表 A.4　安全保障管理目标和安全保障管理要求映射

安全保障管理目标	安全保障管理要求											
	MSO	MSP	MPS	MRM	MSD	MAM	MPE	MOP	MSP	MBD	MCM	MER
OM-1	√											
OM-2		√										
OM-3			√									
OM-4		√										
OM-5				√								
OM-6					√							
OM-7						√						
OM-8							√					
OM-9								√				
OM-10									√			
OM-11										√		
OM-12											√	
OM-13												√

表 A.5　安全保障工程目标和安全保障工程要求映射

安全保障工程目标	安全保障工程要求														
	PRM_SDF	PRM_ATT	PRM_AVL	PRM_AIM	PRM_ASR	PEN_ISR	PEN_HSD	PEN_DSD	PEN_SEE	PEN_PSI	PEN_MSP	PEN_MSC	PEN_COS	PAS_VVS	PAS_EAE
OP-1	√	√	√	√	√										
OP-2						√	√								
OP-3								√	√						
OP-4										√	√				
OP-5												√	√	√	√
OP-6															

参 考 文 献

[1] GB/T 19000—2000 质量管理体系 基础和术语(idt ISO 9000:2000)

[2] GB/T 19001—2000 质量管理体系 要求(idt ISO 9001:2000)

[3] GB/T 19004—2000 质量管理体系 业绩改进指南(idt ISO 9004:2000)

[4] ISO/IEC TR 15443-1: 2005. A framework for IT Security assurance - Part 1: Overview and framework

[5] ISO/IEC TR 15443-2: 2005. A framework for IT Security assurance - Part 2: Assurance methods

[6] ISO/IEC WD 15443-3, A framework for IT security assurance - Part 3: Analysis of assurance methods

[7] ISO/IEC PDTR 19791: 2004, Information technology - Security techniques - Security assessment of operational systems

[8] Information Assurance Technical Framework, Release 3.1. National Security Agency Information Assurance Solutions Technical, September 2002

[9] ISO/IEC 17799:2005 Information technology — Security techniques — Code of practice for information security management .

[10] ISO/IEC 13335-1: 2004 Information technology — Security techniques — Management of information and communications technology security (MICTS) - Part 1: Concepts and models for information and communications technology security management

[11] ISO/IEC 4th WD 13335-2: 2004, Management of information and communications technology security (MICTS) - Part 2: Techniques for information and communications technology security risk management

[12] ISO/IEC 1st CD 18028-1: 2004, Information technology - Security techniques - IT network security - Part 1: Network security management

[13] ISO/IEC FCD 18028-2: 2004, Information technology - Security techniques - IT network security - Part 2: Network security architecture

[14] ISO/IEC FCD 18028-3: 2004, Information technology - Security techniques - IT network security - Part 3: Securing communications between networks using security gateways

[15] ISO/IEC 18028-4:2005, Information technology - Security techniques - IT network security - Part 4: Remote access

[16] ISO/IEC 1st CD 18028-5: 2004, Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using Virtual Private Networks

[17] NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, November 2001

[18] NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems, January 2002

[19] NIST Special Publication 800-34 Continuity Planning Guide for Information Technology System, June 2002

[20] NIST Special Publication 800-50, Building an Information Security Awareness and Training Program, October 2003

[21] NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle, October 2003

[22] NIST Special Publication 800-53. Recommended Security Controls for Federal Information Systems, Feberuary 2005

[23] OECD Guidelines for Security of Information Systems and Networks: 'Toward a Culture of Security', 2002

[24] NSTISSI No. 4009 National Information Systems Security (INFOSEC) Glossary

[25] Carnegie Mellon University/Software Engineering Institute, CMU/SEI-2002-TR-011, CMMI℠ for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing(CMMI-SE/SW/IPPD/SS, V1.1) Continuous Representation. CMMI Product Team, March 2002

[26] Carnegie Mellon University/Software Engineering Institute, CMU/SEI-2002-TR-012, CMMI℠ for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing(CMMI-SE/SW/IPPD/SS, V1.1) Staged Representation. CMMI Product Team, March 2002

[27] System Security Engineering Capability Maturity Model (SSE-CMM®) Model Description Document, Version 3.0, June 15, 2003

[28] System Security Engineering Capability Maturity Model (SSE-CMM®) Appraisal Method. Version 2.0, April 16, 1999

[29] CoBIT®, 3rd Edition, Management Guidelines, COBIT Steering Committee and the IT Governance Institute™, July 2000

[30] CoBIT®, 3rd Edition, Audit Guidelines, COBIT Steering Committee and the IT Governance Institute™, July 2000

[31] CoBIT®, 3rd Edition, Control Objectives, COBIT Steering Committee and the IT Governance Institute™, July 2000

[32] Department of Defense Technical Reference Model, Version 2.0, 9 April 2001

[33] Department of Defense Technical Architecture Framework for Information Management, Volume 1: Overview, Version 3.0, 30 April 1996

[34] DoD Architecture Framework, Version 1.0, DoD Architecture Framework Working Group, August 2003

中华人民共和国
国家标准
信息安全技术 网上证券交易系统
信息安全保障评估准则
GB/T 20987—2007
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 5.75 字数 154千字
2007年10月第一版 2007年10月第一次印刷
*
书号:155066·1-29960 定价 52.00元

GB/T 20987-2007