ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20983—2007

信息安全技术
网上银行系统信息安全保障评估准则

Information security technology—Evaluation criteria for online banking 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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
网上银行系统信息安全保障评估准则
GB/T 20983—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 5.5 字数 155 千字
2007年10月第一版 2007年10月第一次印刷
*
书号:155066·1-29959 定价 50.00 元

GB/T 20983-2007

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、中国工商银行。

本标准主要起草人：吴世忠、王海生、陈晓桦、王贵驷、李守鹏、江常青、彭勇、张利、张燕、史有恒、黄大为、黄朝锋、班晓芳、李静、王庆、邹琪、钱伟明、江典盛、陆丽、李娟、姚轶崭、孙成昊、门雪松、杜宇鸽、杨再山。

引　言

0.1　网上银行系统信息安全保障的含义

网上银行业务是指商业银行等银行业金融机构利用计算机和互联网为客户提供的银行服务。网上银行是银行传统业务的电子化表现形式，拓展了银行服务的时间和空间。网上银行是现代信息技术在银行管理及其金融服务中的拓展，是促使金融服务组织机构与服务形式创新的重要成果之一。网上银行通过国际互联网这一公共资源及其相关技术实现银行与客户之间安全、方便、友好连接，为客户提供多种金融服务。

信息安全保障是网上银行系统建设和运行中必须解决的基础和根本性问题，它关系到客户与银行的切身利益。网上银行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银行行业的特点，以风险和策略为出发点和核心，即从网上银行系统所面临的风险和所处的环境出发制定网上银行系统的安全保障策略，在网上银行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，达到保护网上银行的信息和信息系统资产，从而保障网上银行业务安全、可靠开展的最终目的。

网上银行系统信息安全保障涵盖以下几个方面：

a）网上银行系统信息安全保障应贯穿网上银行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，以获得网上银行系统信息安全保障能力的持续性。

b）网上银行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，以全面保障网上银行系统安全。在安全技术上，不仅要考虑具体的产品和技术，更要考虑网上银行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，不仅要考虑网上银行系统建设的最终结果，更要结合系统工程的方法，注重工程各个阶段的规范化实施；在人员安全上，要考虑与网上银行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）网上银行系统信息安全保障是贯穿全过程的保障。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，降低网上银行系统的风险，从而实现网上银行系统信息安全保障。

d）网上银行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银行系统的安全，保障网上银行系统所支持的业务，从而达到实现组织机构使命的目的。

e）网上银行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，向网上银行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标的信心。因此，它是一种通过客观证据向网上银行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）保障网上银行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。保障网上银行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 网上银行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，结合网上银行系统的具体特点，给出了网上银行系统的信息系统安全保障要求。

制定本标准的意义在于：

a) 为网上银行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) 有利于网上银行系统所有者编制其信息系统的安全保障要求；

c) 有利于网上银行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银行系统进行安全检查、检测、审计、评估和认证。

目　次

信息安全技术
网上银行系统信息安全保障评估准则

1 范围

本标准规定了网上银行系统的描述、安全环境、安全保障目的、安全保障要求及网上银行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银行系统在进行网上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。

网上银行 online banking

商业银行通过互联网等公众网络基础设施，向其客户提供各种金融业务。

4 系统描述

4.1 网上银行系统概述

网上银行系统是商业银行通过互联网等公众网络基础设施，向其客户提供各种金融业务服务的一种重要的信息系统。在进行网上银行系统的信息安全保障工作时，首先必须建立对网上银行系统的充分了解和理解。本标准所使用的网上银行系统的描述框架如图1。

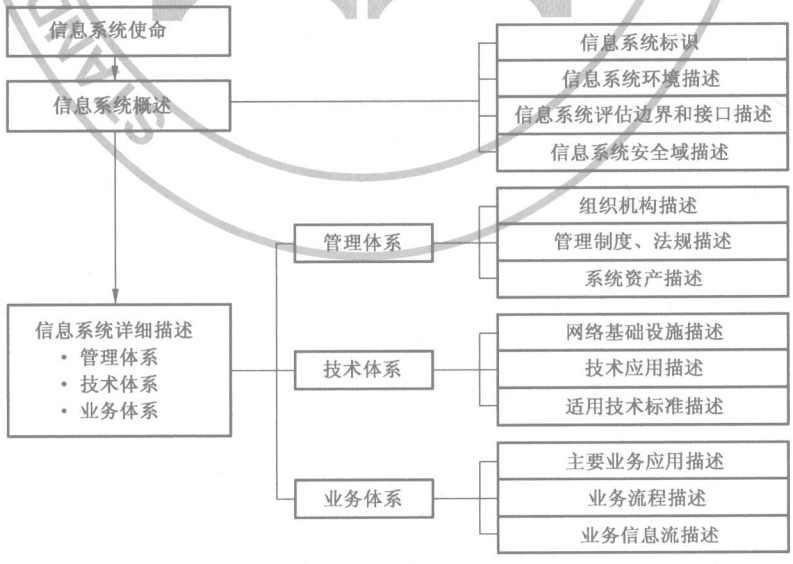

图1 网上银行系统描述框架

网上银行系统的描述框架包括三个部分：

a) 信息系统使命：即从目的和意义出发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。通常，信息系统使命描述了信息系统的高层要求。

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、所属的组织机构及其地点和包含最终用户的组织机构及其地点等相关信息；

2) 信息系统环境描述：描述系统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：描述所要评估的系统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（描述系统的使用者）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：给出同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：描述信息系统的物理资产（指信息系统中的各种硬件、软件和物理设施）和信息资产（指在信息系统计划组织、开发采购、实施交付、运行维护和废弃这一信息系统生命周期过程中产生的同信息系统系统本身相关的有价值的信息以及信息系统所存储、处理和传输的各种相关的办公、管理和业务等信息）。

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：描述系统的网络层次等网络体系结构说明；

◆ 技术应用描述：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 使命描述

网上银行系统是商业银行通过互联网等公众网络基础设施，向其客户提供各种金融业务服务的一种重要的信息系统。网上银行系统将传统的银行业务同互联网等资源和技术进行融合，将传统的柜台通过互联网向客户进行延伸，是商业银行在网络经济的环境下，开拓新业务、方便客户操作、改善服务质量、推动生产关系变革等的重要举措，提高了商业银行的社会效益和经济效益。

4.3 系统概要描述

4.3.1 系统标识

在系统标识中应标明以下内容：

——名称：××银行网上银行系统

——所属银行：××银行

——版本：×××

——时间：××××-××-××

——版权信息：××

4.3.2 系统环境描述

描述系统运行环境以及系统开发、集成和维护的环境。在网上银行系统信息安全保障目标中用户（系统的使用方）应给出其所评估的网上银行系统的详细环境描述。

4.3.3 评估边界和接口描述

描述所要评估系统的边界和接口。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，在具体描述时必须用图表或文字清晰地描述和界定所要评估的系统边界和接口。

图 2 给出了网上银行系统的一个通用概念化的图表描述实例，具体特定的网上银行系统可以参考此图对其评估边界和接口进行详细描述。

网上银行信息系统安全域通常由五个部分组成：

——外部区域：网上银行的公众用户和第三方系统可以通过互联网或专用网访问网上银行业务系统；

——网上银行业务系统；

——银行内部其他系统；

——各银行内部核心业务系统；

——公钥基础设施。

其中评估边界不包括客户端、互联网、公钥基础设施和核心业务系统。

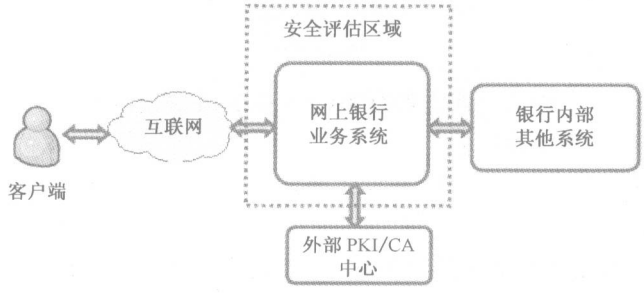

图 2 网上银行系统评估边界和接口描述示意图

4.3.4 安全域描述

网上银行系统是一个涉及多种不同的应用系统、用户对象、数据敏感程度、主管部门等的复杂信息系统。在网上银行系统的描述中，应根据应用系统、用户对象、数据敏感程度、主管部门等划分安全域。

安全域是一种逻辑的划分，它是遵守相同的安全策略的用户和系统的集合。通过对安全域的描述和界定，就能更好对网上银行系统的信息系统安全保障进行描述。

以图 2 网上银行系统评估边界和接口示意图为例，在安全评估区域内的网上银行业务系统的安全域可根据需要进一步划分子安全域。图 3 为网上银行系统的子安全域划分示例。

具体而言，网上银行系统主要包括：客户端、网上银行访问子网和网上银行业务系统、CA 和中间隔离设备。如图 3 所示：

——外部区域：网上银行的用户，安装网上银行客户端，通过互联网访问网上银行业务系统；

——安全域 1：网上银行访问子网，主要提供客户的 web 访问和证书认证；

——安全域 2：网上银行业务系统，主要进行网上银行的业务处理；

——银行内部系统：银行处理系统，主要进行银行内部的数据处理。

图中 CA 是证书颁发和管理机构，它主要为银行客户、银行工作人员以及网上银行 web 服务器等设备提供公开密钥证书服务。某些银行安全区域 1 和安全区域 2 合为一个安全区域。

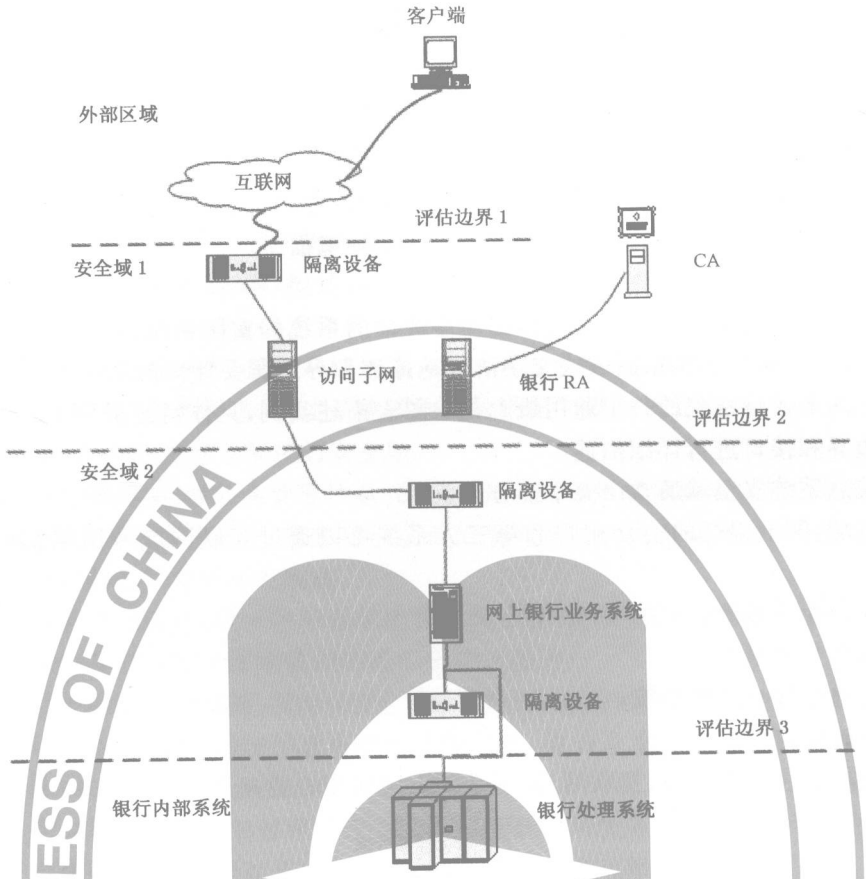

图 3 网上银行系统子安全域划分示例

4.3.5 信息系统安全评估边界描述

根据信息系统安全域的实际情况划分，在具体描述时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。

图 2 给出了网上银行系统的安全评估边界，其与外部系统边界的连接点称为与互联网的接口，即客户端与互联网的接口、网上银行 web 服务器与互联网的接口。有的网上银行 web 服务器与银行之间以专用网络连接，此时这种接口的安全视为系统内部安全，不认为是系统外部接口。

图 2 中银行内部其他系统不属于本标准规定的范围，其安全性由各商业银行自行负责。

4.4 系统详细描述

4.4.1 网上银行系统管理体系

在管理体系中，描述的内容涉及到法律法规和规章制度，以及系统现有的管理组织结构和重要资产等。

4.4.1.1 组织机构描述

在网上银行系统组织机构概述中，应包括与网上银行系统管理、使用、开发、集成、支持相关的组织机构的描述，特别是与安全保障管理相关的组织机构的描述。

4.4.1.2 管理制度和法规描述

管理制度、法规描述部分要求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，在网上银行系统信息安全保障目标中用户应给出其所评估的网上银行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。

4.4.1.3 系统资产

资产是网上银行系统所要保护的对象，所有威胁都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银行系统使命的实现。

在网上银行系统中，资产分为物理资产和信息资产。

4.4.1.3.1 物理资产

物理资产：指网上银行系统中的各种硬件、软件和物理设施。例如：系统的各种网络设备和软件资产。在网上银行系统信息安全保障目标中，应详细列出所评估的特定网上银行系统中的所有重要资产。下面仅列出在网上银行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) 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)；
4) 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)；
5) 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；
6) 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；
2) 网络操作系统；
3) 网络管理软件；
4) 数据库管理软件；
5) 业务应用软件。

4.4.1.3.2 信息资产

信息资产：指在网上银行系统计划组织、开发采购、实施交付、运行维护和废弃这一网上银行系统生命周期过程中产生的同网上银行系统本身相关的有价值的信息以及网上银行系统所存储、处理和传输的各种相关的业务、管理和维护等信息。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。下面仅列出在网上银行系统中所包含的部分信息资产示例作为参考：

——网上银行业务信息：客户档案信息、客户操作记录、安全信息和交易业务数据等；

——网上银行业务管理信息：柜员档案信息、柜员操作记录、安全信息；

——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、路由信息、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。

4.4.2 网上银行系统技术体系

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使用的技术标准进行描述，这些描述将帮助了解网上银行系统并为进一步描述业务系统提供基础和支持。技术体系描述包括业务支持层、系统服务层和基础设施层的描述。见图 4。

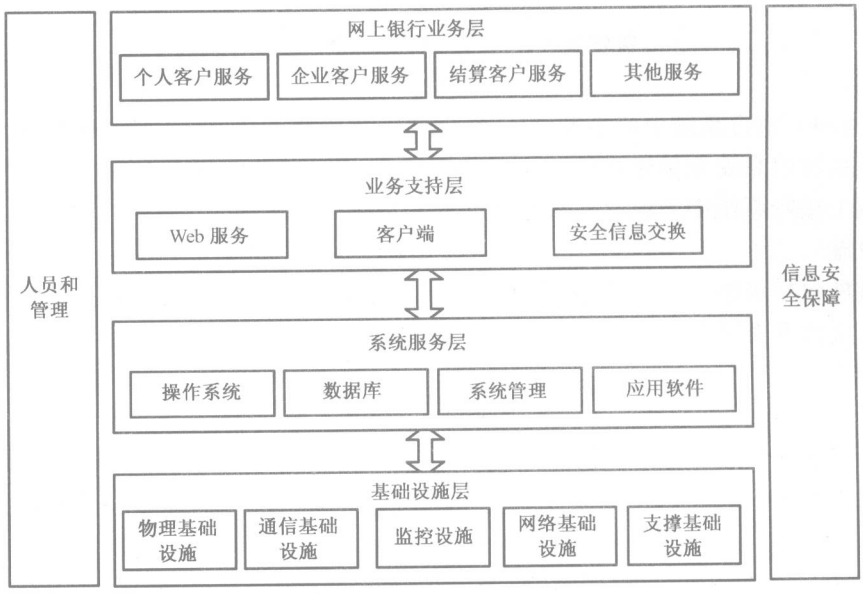

图 4　网上银行系统逻辑层次结构

4.4.2.1　业务支持层

业务支持层为具体的网上银行服务提供支持，如 web 服务、网上银行客户端、安全信息交换等。

4.4.2.2　系统服务层

系统服务层为业务支持层和业务层提供所需的各种通用服务，如操作系统服务、数据库服务、系统管理服务、应用软件服务等。

4.4.2.3　基础设施层

基础设施层向各类网上银行应用提供必要的基础环境、可靠有效的信息传输服务通道，是各类信息的最终承载者。因此，基础设施层位于整个技术体系结构的底层。具体包括有物理基础设施、通信基础设施、监控设施、网络基础设施、支撑性基础设施等。

4.4.3　网上银行业务体系

4.4.3.1　业务应用描述

网上银行业务主要包括几个方面：

——个人客户服务：针对银行的个人客户开展的网上银行业务，包括：账户查询、账单支付、转账/汇款业务、证券业务、债券基金业务、外汇买卖、服务设置、主动通知、代理缴费、B2C 等服务；

——企业客户服务：针对银行的企业客户开展的网上银行业务，包括：账务查询、网上转账、代发工资、签发电子票据、证券业务、债券基金业务、外汇买卖、代理缴费、内部资金调拨、报表统计、主动通知、B2B 等服务；

——其他服务：针对银行开展的网上银行新业务，包括：政府财政部门、税务、审计，以及今后可能推出的新业务等服务。

4.4.3.2　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、长度以及数据传送的一般方式。在网上银行系统中存在 3 种类型的信息流：外部信息流、中间信息流、内部信息流。在网上银行系统信息安全保障目标文档中应根据具体的主要业务应用，并参考本准则中所提出的信息流分类方法进行详细描述。

——外部信息流：客户端与网上银行访问子网之间的信息流、RA 与 CA 之间的信息流；

——中间信息流：访问子网与网上银行业务系统之间的信息流；

——内部信息流：网上银行业务系统与银行内部系统之间的信息流。

5 系统安全环境

5.1 假设

假设建立在网上银行系统环境所预期的应用环境和使用方式上。假设按 A-1、A-2……A-N 编号，假设一般分两类：

a) 网上银行信息系统的开发环境和运行环境的假设；

b) 网上银行信息系统安全服务假设。

5.1.1 系统环境安全假设

环境假设主要包括：

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的一部分。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 网上银行系统的开发应采用不断持续改进的方法。

A-3 网上银行系统使用不可信任的通信网络来建设通信能力。

A-4 网上银行系统用户有责任保护自己的口令，防止口令泄露。

A-5 网上银行系统的系统管理员有能力管理系统，信任系统管理员不会滥用权限，能够遵守由系统安全管理文件所确定的安全策略和程序，不会故意破坏安全。

A-6 系统已实现物理安全，系统内关键设备应位于受控的访问设备中，以阻止外部人员和内部非授权人员对其的物理访问。

A-7 系统可能受到精通系统安全的高水平攻击者的有预谋、有组织攻击。

5.1.2 系统安全服务假设

网上银行系统安全服务假设有：

A-8 网上银行系统存在若干不同安全域：

a) 每个安全域具有不同的管理和策略要求；

b) 外部区域是一个特殊的安全域，它没有管理，没有安全策略，是敌对行为主要来源；

c) 连接及使用公众网受有关法令、规范和制度的管理。

A-9 网上银行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-10 其他系统的接入不能降低网上银行信息的整体安全状态，必须针对潜在的风险进行检查。

A-11 在法律执行调查过程中，为协调机构提供网上银行系统单方的意见。

5.2 威胁

在系统描述中的资产部分描述了为保障网上银行信息系统的安全需要保护的资产，本条将描述在网上银行信息系统的安全环境中针对这些资产可能施加的相关威胁。需要指出的是，在本标准中并没有列出所有的威胁，而只列出与网上银行信息系统的安全运行相关的主要威胁。

威胁指能够通过未授权访问、毁坏、暴露、数据修改或拒绝服务对系统造成潜在危害的任何环境或事件。因此，威胁应通过已确定的威胁源、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，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：

——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；

——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）；

——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；

——邻近攻击；

——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，他们具有对网上银行系统的合法访问权限。内部人员安全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攻击。

非恶意攻击是由于内部人员的无意行为造成了对网上银行系统的攻击，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

这类攻击主要包括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。典型的被动攻击有：

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

主动攻击为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。典型的主动攻击有：

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) 邻近攻击(接近攻击)

此类攻击的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或秘密进入的，也可以是两种都有，典型的邻近攻击有：

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银行软件和硬件的开发、生产、运输、安装阶段，攻击者恶意修改设计、配置等行为。典型的分发攻击有：

——利用开发制造商的设备修改软硬件配置；

——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 威胁描述

综合上述威胁分类和分析，网上银行系统安全评估准则的威胁将主要根据威胁源、攻击方式、资产、影响方式和影响结果进行分析，参照表1。

表1 网上银行系统威胁描述

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 —银行客户 —商业和专业组织 —政府	—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
	内部员工（内部用户）	—普通员工 —系统管理员				
自　然						
环　境						

从上表可以看出，网上银行系统的安全威胁是多级别的，因此，网上银行系统整体上必须具有应对这些攻击的能力，但具体到每一个应用系统则需要区别对待，认真分析。

5.2.3 具体的信息系统安全保障威胁

基于前面的威胁分类和威胁模型，结合网上银行系统的特点，列出网上银行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方式编号。

a） 人员威胁

T-1 未授权用户可能获得对网上银行系统的逻辑访问。

T-2 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禁止其访问的网上银行系统资源或执行未获准的访问权限的操作。

T-3 某些人进行拒绝服务攻击，攻击可能导致网上银行系统资源不可用。

T-4 某些人可能物理地攻击网上银行系统从而危及它的信息安全保障。

T-5 安全相关的事件可能没有记录或不可追踪。

T-6 外部用户可能侵害网上银行系统的通信能力。

T-7 网上银行系统的体系结构、设计、实现和维护缺陷可能导致信息安全保障失效。

T-8 某人可能引入未授权软件到网上银行系统中。

T-9 某人可能篡改网上银行系统的相关保护机制。

T-10 可信任角色的人，如网上银行系统的管理人员和维护人员，可能导致信息安全保障失效。

T-11 网上银行系统运行不正确可能导致信息安全保障失效。

T-12 网上银行系统失效中不正确的重起和/或恢复可能导致信息安全保障失效。

T-13 网上银行系统环境的改变可能引入或恶化脆弱性。

T-14 对策和策略的局限和缺陷可能被知识渊博的对手获取。

T-15 授权用户使用非技术手段可能获得无恶意的、未授权的访问控制。

T-16 非授权用户使用非技术手段可能获得处理资源或信息的访问。

T-17 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-18 攻击者欺骗用户与伪造的系统服务进行交互。

b) 自然威胁

T-19 自然灾害或恶意攻击可能导致关键操作的暂停和/或网上银行系统服务的中断。

c) 环境威胁

T-20 电力系统故障可能导致关键操作的暂停和/或网上银行系统服务的中断。

5.3 组织安全策略

网上银行信息系统的安全策略是网上银行信息安全保障活动的基础和出发点，指导如何对资产（包括敏感性信息）进行管理、保护和分配，指导整个网上银行信息系统安全体系的设计与实施，所有网上银行信息系统安全控制措施（包括技术控制措施和管理控制措施）的选择、运营和维护。制定安全策略是每一个开展网上银行业务的机构都必须完成的工作，安全策略一定要与相关组织机构的业务相关，一个设计良好的策略是系统整体安全目标能否实现的关键。

网上银行信息系统安全策略的制定应建立在充分了解其业务需求和信息安全需求的基础上，并符合相关的国家法律法规、标准、政策以及行业主管部门颁布的信息安全保障规定、标准和规范。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。安全策略应采用通俗易懂的语言解决网上银行信息系统的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，安全策略是通过规定一套规则来指导网上银行信息系统的建设、运行、维护和管理。这些规则清晰地定义哪些行为是被允许的。

网上银行信息系统的其他各类文档，如网上银行信息系统的技术方案、管理制度及操作手册、工程实施过程文档和验收报告、应用软件开发过程等等，都必须满足信息安全策略的要求，所有这些文本应该清晰地说明信息安全策略所规定的规则。通过使用管理控制措施和技术控制措施，来实施这些规则。规则能够实现信息系统的五个主要安全保障目的：

——可用性；

——保密性；

——完整性；

——可追查性；

——抗抵赖性。

信息安全策略是网上银行信息系统安全的基础，要充分反映相应组织机构的业务安全保障要求，体现了组织机构的核心价值和任务。因此，网上银行信息系统信息安全策略的制定、签署和实施必须由本组织机构的最高负责人负责。

网上银行的特点决定了网上银行信息系统的安全策略是一个多层次结构，典型的网上银行信息系统信息安全策略具有三个层次：系统高层安全策略；系统及子系统级策略；安全产品级策略。策略按P-1、P-2……P-N编号。