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

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、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。

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。

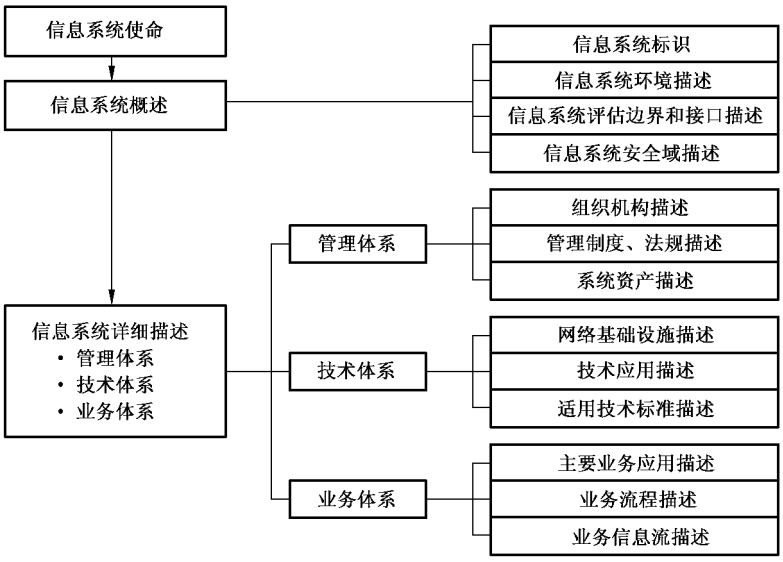

图 1 网上银行系统描述框架