ICS 03.060
A 11

中华人民共和国国家标准

GB/T 27910—2011

金融服务　信息安全指南

Financial services—Information security guidelines

(ISO/TR 13569:2005,MOD)

2011-12-30 发布　　2012-02-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用重新起草法修改采用国际标准 ISO/TR 13569:2005《金融服务　信息安全指南》。

考虑到我国国情,在采用 ISO/TR 13569:2005 时技术内容做了以下修改:

——删除了原文中的 5.2 法律和法规符合性,因为这部分内容主要描述了国外的法律法规要求,与国内情形不同;

——鉴于 ISO/IEC 17799:2005 已于 2007 年 7 月正式更改编号为 ISO/IEC 27002:2005,标准中对该标准的无日期引用更换为对 ISO/IEC 27002 的无日期引用;

——将原文中的一些错误进行修正,如附录 D.2.4 中的“E.2.3”改为“D.2.3”等。

为便于使用,本标准还做了下列编辑性修改:

——删除 ISO 前言。

与本部分规范性引用的国际文件有一致性对应关系的我国文件如下:

GB/T 22081　信息技术　安全技术　信息安全管理实用规则(GB/T 22081—2008,ISO/IEC 27002:2005,IDT)

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会(SAC/TC 180)负责归口。

本标准负责起草单位:中国金融电子化公司。

本标准参加起草单位:中国人民银行、中国农业银行、招商银行、上海浦东发展银行、中国信息安全测评中心、中钞信用卡产业发展有限公司。

本标准主要起草人:王平娃、陆书春、王韬、杨倩、李曙光、刘运、王连强、戴忠华、唐步天、李同勋、陈杰、李安安、赵志兰、贾树辉、田洁、景芸、张艳、马小琼。

引　言

随着计算机和网络技术的引入，金融业务的实现方式发生了巨大变化，具体体现在对电子交易的依赖性不断增加，从而带来了对信息和通信技术安全进行管理的需求。每天大量的资金和证券交易信息通过电子通信方式进行传输，这些通信方式均由基于业务规则的安全策略所控制。

开放环境中巨额、海量的电子交易给金融机构带来了巨大风险。高度互连的网络和日益增加的技术高超的恶意攻击者给银行和银行客户加重了风险，并且当金融交易涉及重要的支付系统时，这些后果可能对国内外金融市场产生不良影响。

为了在开放环境中拓展金融业务的同时，进行有效的风险管理，金融机构应该建立一个强有力且有效的企业级的信息安全方案。金融机构应像建立业务惯例和相关协议、外部采购流程、保险等适当的安全控制措施一样，来精心构建信息安全方案，降低风险，满足国内外法律法规的要求。

正如巴塞尔协议给我们的警示，运营、法律和法规风险可以导致或者恶化信贷和流动性风险。管理这些风险已成为金融机构信息安全方案的核心。为具体掌握风险，每一个机构必须按照其自身业务活动对其进行诠释。运营风险包括欺诈和犯罪活动、自然灾害、恐怖活动等，必须给予仔细考虑。针对小概率事件也必须制定应对计划，例如 2004 年 12 月亚洲海啸和 2001 年 9 月 11 日的恐怖袭击。

本标准给不同规模和类型的金融机构提供了审慎且成本合理的业务信息安全管理方案，同时它也为金融机构服务提供商提供了指南。对于面向金融业的培训机构和出版商，本标准也可作为原始文档。

本标准的目标是：

——定义信息安全管理方案；

——提出方案的策略、组织和必要的结构化组件；

——提出在金融应用中基于可接受的审慎业务措施来选择安全控制措施的指南；

——提出信息安全管理方案中系统化解决法律法规风险的金融服务管理需求。

本标准并未面向所有金融机构提供一个单一的、一般性的解决方案。每个金融机构必须进行风险分析并选择适当的措施。本标准是提供过程管理的指南，而不是具体的解决方案。

金融服务　信息安全指南

1　范围

本标准为金融机构提供了制定信息安全方案的指南。该指南包括策略讨论，机构和方案的结构化法律法规组件。本标准探讨了在选择和实施安全控制措施方面应考虑的内容，以及在现代化金融服务机构中管理信息安全风险的要素，并给出了基于机构业务环境、实践和规程方面应考虑的建议。本标准还包括对法律法规符合性问题的讨论，这需要在方案的设计和实施阶段予以考虑。

本标准适用于金融机构制定信息安全方案时的参考。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO 9564(所有部分)　银行业务　个人识别码的管理与安全(Banking—Personal Identification Number (PIN) management and security)

ISO 10202(所有部分)　金融交易卡　使用集成电路卡的金融交易系统的安全体系(Financial transaction cards—Security architecture of financial transaction systems using integrated circuit cards)

ISO 11568(所有部分)　银行业务　密钥管理(零售)(Banking—Key management (retail))

ISO/IEC 11770　(所有部分)信息技术　安全技术　密钥管理(Information technology—Security techniques—Key management)

ISO 15782(所有部分)　金融业务证书管理(Certificate management for financial services)

ISO 16609:2004　银行业务　采用对称加密技术进行报文鉴别的要求(Banking—Requirements for message authentication using symmetric techniques)

ISO/IEC 27002　信息技术　安全技术　信息安全管理实用规则(Information technology—Security techniques—Code of practice for Information security management)

ISO/IEC 18028(所有部分)　信息技术　安全技术　IT网络安全(Information technology—Security techniques—IT network security)

ISO/IEC 18033(所有部分)　信息技术　安全技术　加密算法(Information technology—Security techniques—Encryption algorithms)

ISO 21188　用于金融服务的公钥基础设施　业务和策略框架(Public key infrastructure for financial services—Practices and policy framework)

3　术语和定义

下列术语和定义适用于本文件。

3.1

访问控制　access control

指仅允许经授权的人员或应用进行信息访问(或信息处理设施访问)的功能，包括物理访问控制(在未授权人员和被保护的信息资源之间放置物理障碍)和逻辑访问控制(采用其他方法进行限制)。