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)。

3.2

可核查性 accountability

确保实体活动可追溯到惟一实体的属性。

[ISO 7498-2:ISO/IEC 13335-1:2004,定义 2.1]

3.3

警报 alarm

安全违规、异常、危险状态的指示,需要立即关注。

3.4

资产 asset

对于机构有价值的任何事物。

[ISO/IEC 13335-1:2004,定义 2.2]

3.5

审计 audit

指确认控制措施得当,充分满足功能,并且报告针对相应管理级别的不足之处。

3.6

审计日志 audit journal

系统运行的时序记录,该记录足够重建、复审、检查环境的系列事物和周边行为,或导出一笔交易从起始到输出最终结果路径中的每个事件。

[ISO 15782-1:2003,定义 3.3]

3.7

鉴别 authentication

确认实体声称身份的过程。

[ISO/IEC TR 13335-4:2000,定义 3.1]

3.8

真实性 authenticity

应用到如用户,过程,系统和信息等实体上的属性,以确认对象或资源的身份是其所声称的。

3.9

可用性 availability

授权实体在需要时可访问和可使用的性质。

[ISO 7498-2:ISO/IEC 13335-1:2004,定义 2.4]

3.10

备份 back-up

业务信息的存储,一旦遇到信息资源丢失,可确保业务的持续性。

3.11

生物特征 biometric

可测量的用于识别个人身份或验证声称的生物或行为特征,该特征可有效区分一个人和其他人。

[ANSI X9.84:2003]

3.12

生物特征识别 biometrics

基于生物或行为特征,确认个人身份或验证其声称身份的自动方法。

3.13

卡鉴别方式 card authentication method CAM

一种概念,允许对金融交易卡以机读的方式进行惟一性识别,并且防止卡的复制。

3.14

分类 classification

把信息进行划分(例如按照潜在欺骗、敏感性或信息关键度)以便应用适当控制措施的方法。

3.15

机密性 confidentiality

信息对未授权的个人、实体或过程不可用或不可泄漏的特性。

[ISO 7498-2;ISO/IEC 13335-1:2004,定义 2.6;ISO 15782-1:2003,定义 3.19]

3.16

应急计划 contingency plan

使公共机构在自然或其他灾害之后能恢复运行的规程。

3.17

控制措施 control

见防护措施。

3.18

公司信息安全策略 corporate information security policy

建立信息安全方案的意图和目标的一般声明。

3.19

信用风险 credit risk

一方在到期日或未来的任意时候不能偿还其债务而产生的风险。

[CPSS,全局性重要支付系统核心原则]

3.20

关键度 criticality

为完成交易,对某项信息或者信息处理设施的需求度。

3.21

密码学 cryptography

用于加密或者信息鉴别的数学过程。

3.22

密码鉴别 cryptographic authentication

基于数字签名及按照 ISO 16609 产生的报文鉴别码进行鉴别的方式,其中所用密钥是按照 ISO 11568分发的,或者通过对报文的成功解密推出(该报文使用 ISO/IEC 11770 分发的密钥,通过 ISO 18033与 ISO/TR 19038 或 ANSI X9.52 加密)。

3.23

密钥 cryptographic key

用于控制加密,或者鉴别等密码过程的值。

注:获得正确的密钥信息才能保证报文的正确解密或报文完整性的验证。

3.24

信息破坏 destruction of information

无论何种原因,导致信息不可用的任何情形。

3.25

数字签名 digital signature

对一个数据单元进行密码变换,以提供数据源鉴别、数据完整性和签名人抗抵赖性服务。

[ANSI X9.79]

3.26

信息泄漏 disclosure of information

未经授权的信息浏览或可能的浏览。

3.27

双重控制 dual control

利用两个或多个不同实体(通常是人)协同操作保护敏感功能和信息的过程。

注 1：对交易中易受攻击要素提供物理保护，各个实体负有同等的责任。单个人不可以接触和使用这些要素(如加密密钥)。

注 2：对手工密钥和证书的产生、传输、导入、存贮和恢复，双重控制要求实体间密钥分割。

注 3：当要求使用双重控制时，要特别注意确保彼此之间的独立性。见密钥分割。

[ISO 15782-1:2003，定义 3.31]

3.28

加密 encryption

一个信息转换过程，可使信息转换到除了特定密钥持有者以外，其他人均无法理解的形式。

注：加密可为加密过程和解密过程(加密的逆过程)之间的信息提供保护，避免信息泄漏。

3.29

防火墙 firewall

防火墙是放置在两个网络之间的组件的集合。该组件具有以下共同特性：

——所有网络间的信息往来都必须经过防火墙；

——经本地安全策略定义，只有授权的通信被允许；

——防火墙本身对渗透具有免疫性。

3.30

识别 identification

判断实体惟一身份的过程。

3.31

映像 image

在信息处理系统中处理和存储文档的数字化表示。

3.32

事故 incident

任何非预期和非期望的可能导致损害交易活动或信息安全的事件，例如：

——丢失服务，设备或设施；

——系统故障或过载；

——人为错误；

——不符合策略或指南；

——破坏物理安全安排；

——不可控的系统变更；

——硬件或软件故障；

——访问侵害。

[ISO/IEC 13335-1:2004，定义 2.10]

3.33

信息处理设施 information processing facility

任何信息处理系统、服务、基础设施或放置它们的物理场所。

[ISO/IEC 13335-1:2004，定义 2.13]

3.34

信息 information

任何以电子形式、书面形式、会议讲话或者其他媒体形式出现的，由金融机构用于做决定、转账、设置利率、放贷、处理交易及其他类似数据，包括处理系统的软件组件。

3.35

信息资产 information asset

机构的信息或者信息处理资源。

3.36

信息安全 information security

涉及定义、实现和维护信息或信息处理设施的机密性、完整性、可用性、抗抵赖性、可核查性、真实性和可靠性的所有方面。

[ISO/IEC 13335-1:2004，定义 2.14]

3.37

信息安全官(ISO) information security officer (ISO)

负责执行和维护信息安全方案的人员。

3.38

信息设备 information resources

用于处理、沟通或者存储信息的设备，不管其在机构之内还是机构之外，例如电话、传真和计算机。

3.39

完整性 integrity

维护资产准确和完整的性质。

[ISO/IEC 13335-1:2004，定义 2.15]

3.40

密钥 key

见密钥(cryptographic key)。

3.41

空头支票 kitting

使用无效支票获得信用或金钱。

3.42

法律风险 legal risk

由于未预期到的法律或法规的实施或者由于合同无法执行而造成损失的风险。

[CPSS，全局性重要支付系统核心原则]

3.43

保证函 letter of assurance

代表信函的接受方，说明信息安全控制措施的文档，用于所持有信息的保护。

3.44

流动性风险 liquidity risk

当一方没有充足的现金偿还其到期债务时而产生的风险，虽然未来的某些时候可能有能力偿还。

[CPSS，全局性重要支付系统核心原则]

3.45

报文鉴别码 message authentication code，MAC

发送方附加在报文之后的代码，它是对报文进行密码处理的结果。

注：如果接收方能够产生相同代码，那么就可以确信报文没有被修改，并由适当的密钥持有人所产生。

3.46

信息更改 modification of information

信息的未授权变更或者意外变更，不论其是否被检测到。

3.47

须知 need to know

对具有某些职责的人员，限制其对信息和信息处理资源进行访问的一个安全概念。

3.48

网络 network

若干用户共享的通信和信息处理系统的集合。

3.49

抗抵赖性 non-repudiation

证明一个活动或事件已经发生，且不可否认的能力。

[ISO/IEC 13335-1:2004，定义 2.16]

3.50

操作风险 operational risk

由与设备运行相关的因素导致的信贷或流动性风险，例如技术故障或操作错误。

[CPSS，全局性重要支付系统核心原则]

3.51

信息所有者 owner of information

负责收集和维护特定信息的人或者功能。

3.52

口令 password

用于鉴别用户的字符串。

3.53

审慎业务实践 prudent business practice

被普遍接受的必要的业务实践集。

3.54

可靠性 reliability

计划行为和结果的一致性。

[ISO/IEC 13335-1:2004，定义 2.17]

3.55

残余风险 residual risk

风险处置后仍残余的风险。

[ISO/IEC 13335-1:2004，定义 2.18]

3.56

风险 risk

威胁利用一个或一组资产的脆弱性对机构造成损害的潜在可能性。

注：可根据事件的概率和结果的组合来衡量。

[ISO/IEC 13335-1:2004，定义 3.19]

3.57

风险接受 risk acceptance

与策略例外相联系的经核准的风险。

3.58

风险分析 risk analysis

估计风险程度的系统过程。

[ISO/IEC 13335-1:2004,定义 2.20]

3.59

风险评估 risk assessment

风险识别,风险分析和风险评价的整个过程。

[ISO/IEC 13335-1:2004,定义 2.21]

3.60

风险评价 risk evaluation

按照事先制定的准则分析风险级别、确定需要实施风险处置领域的过程。

3.61

风险识别 risk identification

通过分析业务目标、威胁和脆弱性等进行识别风险的过程,以此作为进一步分析的基础。

3.62

风险管理 risk management

识别、控制、清除或最小化不确定事件的全部过程,该不确定事件可影响信息和通信系统资源。

[ISO/IEC 13335-1:2004,定义 3.22]

3.63

风险处置 risk treatment

选择和实施措施以改变风险的过程。

3.64

防护措施 safeguard

处置风险的实践、规程或机制。

注:"防护措施"术语可等同于术语"控制措施"。

[ISO/IEC 13335-1:2004,定义 2.24]

3.65

安全 security

系统免于未授权访问、或遭受不可控损失和影响的性质和状态。

注 1:实践中绝对的安全是不存在的,系统的安全性是相对的。

注 2:在一个以各种状态展现的安全系统中,安全是在各种操作下所保持的特定"状态"。

3.66

服务器 server

给其他计算机提供若干服务的计算机,例如处理通信、文件存储接口或打印设施等。

3.67

登录 sign-on

完成用户身份识别和鉴别。

3.68

知识分割 split knowledge

把关键信息拆分多个部分,使得必须具备最小数量的部分才能执行一项活动。

注:知识分割常用于双重控制的实施。

3.69

储值卡 stored value card

能够存储和转移电子现金的介质。

3.70

系统性风险 systemic risk

由于参与者无法履行义务或系统自行中断，导致其他系统参与者或金融系统其他部分的其他参与者在必要时无法履行义务的风险。

注：这样的错误将导致流动性或信贷问题的广泛扩散，结果将威胁系统或金融市场的稳定性。

[CPSS，全局性重要支付系统核心原则]

3.71

威胁 threat

导致系统或机构受损的事故的潜在原因。

[ISO/IEC 13335-1:2004，定义 2.25]

3.72

令牌 token

用户控制的包含在电子商务中用于鉴别和访问控制的信息的设备(例如磁盘，智能卡，计算机文件)。

3.73

用户 ID user ID

用于惟一标识系统中每个用户的字符串。

3.74

脆弱性 vulnerability

可能被一个或多个威胁所利用的一个或一组资产的脆弱性。

[ISO/IEC 13335-1:2004，定义 2.26]

4 符号和缩略语

ATM	自动柜员机
CEO	首席执行官
CFO	首席财务官
CIO	首席信息官
CISO	首席信息安全官
COO	首席运营官
CPSS	支付和结算系统委员会
CTO	首席技术官
DMZ	非军事区
ETF	电子资金转账
FTP	文件传输控制
HTTP	超文本传输协议
HTTPS	安全超文本传输协议
ICT	信息和通信技术
IDS	入侵检测系统
IP	网际协议
IPSEC	IP 安全协议
IT	信息技术
LAN	局域网

LEAP	轻量级扩展代理平台
MAC	报文鉴别码
OS	操作系统
PC	个人电脑
PDA	个人数字助理
PEAP	保护扩展鉴别协议
PIN	个人识别码
POTS	普通老式电话业务
RF	射频
SMTP	简单邮件传输协议
SSH	安全壳
SSL	安全套接层
USB	通用串口总线
VPN	虚拟专网
VTAM	虚拟终端存取方法
WAN	广域网
Wi-Fi	无线相容性认证标准
WS	Web 服务
XML	可扩展标记语言

5 公司信息安全策略

5.1 目的

现今所有金融服务机构高度依赖信息技术(IT)以及信息通信技术(ICT)的应用,因此需要保护信息和管理信息资产的安全。为使管理者履行他们的职责,必须考虑信息安全并且使信息安全管理成为机构管理计划的组成部分。

制定信息安全方案是一个审慎业务实践,它帮助金融服务机构识别和管理风险。本标准推荐一个通用的,基于策略方法来实施信息安全管理的指南,使得金融机构根据其业务目标提炼出其所需要的信息安全管理方案,保护 IT 资产的策略和规程应支持业务目标。基于策略的方法适用于不同规模、不同的管理风格和不同组织形式的机构。

本标准提供指南而非具体的解决方案,这些指南可用于信息安全管理的各个方面,并在制定和维护信息安全方案方面提供协助。其他相关文献,特别是 ISO/IEC 27002,提供了通用的、对实施和保护很有价值的具体信息,比较而言,本标准将讨论法律法规的要求,当金融机构建立基于策略的信息安全管理方案时必须考虑这些要求。

5.2 制定安全策略

在确立机构信息安全目标和评估法律法规影响之后,应制定与已确立商业目标一致的行动计划。这个计划用于作为制定一个公司信息安全策略(策略)[1]的路线图。

公司制定一个考虑到公司目标及其组织特殊性的策略是很关键的。该安全策略应与公司业务、文化和业务运营的法律法规环境相一致。策略的制定对确保风险管理安全方案处理结果的适用性和有效性是至关重要的。机构管理者应对策略的制定和有效实施提供支持。安全策略同公司商业目标结合

1) 本文档通篇中"策略"代表"公司信息安全策略"。

时，该策略将有助于资源使用效率的最大化，并且确保对一系列不同信息系统环境有一个一致的安全方法。

5.3 文档层次

5.3.1 综述

5.3.1.1 概要

本指南描述了三个层次的信息安全方案文档。分别为公司信息安全策略(策略)文档，安全实践文档和可操作的安全规程文档[2)]。文档的层次和每层的含义如图1所示。

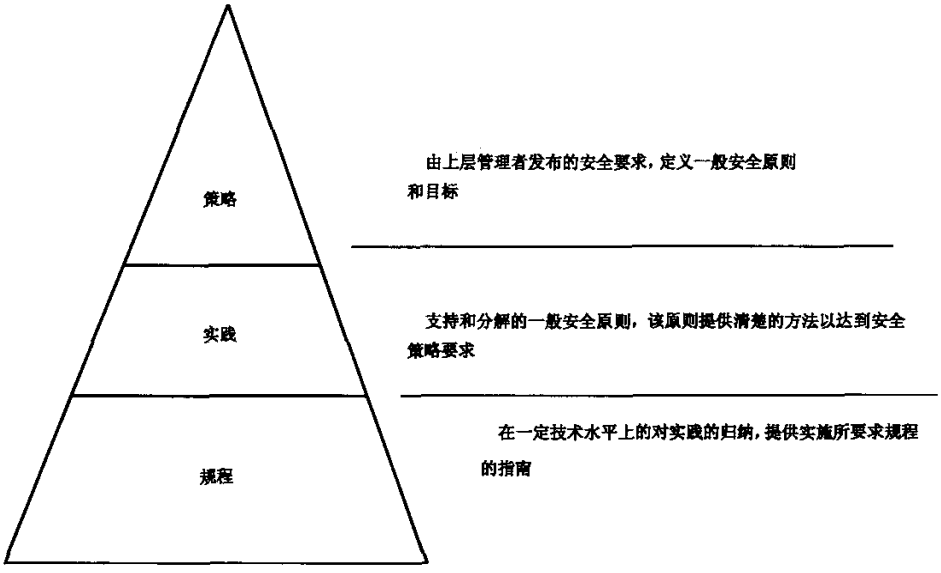


图1 方案文档

信息安全文档应从高层的机构目标到底层的实施安全策略的设备的具体安全设置。一般性信息和特定信息最好由多个层次文档进行涵盖。层次数量应保持最少，本指南推荐三层：策略文档、安全实践文档和可操作的安全规程文档。

当最新出现的技术引入机构时可要求附加文档。策略文档经常是简单的一页，规程文档可包含很多页以说明机构内单独的、特殊的环境、业务单元和策略。在某些情况下，一个单一的、有明确界限的系统也可有自己的安全实践文档。所有的实践和规程应采用从宏观描述到详细描述的结构，并同公司风险评估和整体策略保持一致。

5.3.1.2 公司信息安全策略

策略文档是信息安全方案的所有文档系列中最小的。典型情况下，策略用很少的文字来说明：管理者把各种形式的信息作为应保护的有价值的公司资源。策略应覆盖较广的范围，尽可能简明扼要的阐述，但应提供被保护资产的详细信息，例如客户数据，雇员记录，合作伙伴的约定和过程。例如，一个非常简单的策略文档可包含这样的单一声明："公司所有信息资产的机密性、可用性和完整性应通过合适的安全控制措施得到保护"。

2) 这个术语和层次没有定义。机构可以使用更多的层次和不同的术语。

策略文档是一个概要的文档、应在一定范围内可理解，是信息安全方案的文档中对机构的影响最大的文档。在特定的时间内，应仅存在一份策略文档实例并应在全机构颁布。它应由负责信息安全的董事会成员，例如首席执行官(CEO)和首席信息官(CIO)签署。

策略文档本质上应是公开的，并广泛分发，可为所有公司股东得到。它应强调保护和提供信息资产是管理者和所有雇员的责任，最高级别管理者应得到安全方面的培训并对安全问题有清醒认识。

所有股东应清晰认识到以下内容：策略文档是由公司官员和董事会人员直接授权的。策略文档应根据本地和国际相关法律法规的约束说明机构的运营目标，根据国内和国际标准认可的合理原则和实践构建信息安全方案的基础。

策略文档应基本保持固定。仅当战略目标转变时、已知业务风险变更时或影响公司运营法律法规环境的事件出现时，它才应变更。公司官员和董事会人员指明变更的控制参数和规程。

5.3.1.3 代表

当制定策略时，来自各种职能部门的代表应参与。制定组应包括董事会董事、执行官、法律代表、风险管理委员会和审计委员会成员。在策略的形成过程中，制定组将从专家和业务人员处获得有关方面的信息，例如信息技术、物理安全和财务功能。

5.3.1.4 信息分类

实施信息安全策略的一个方面是信息分类。类似于军事系统分为“最高机密”、“机密”和“非密”一样，金融机构的信息也有不同的价值。信息资产分类的结果将指出何时应实施好的、更好的或最好的控制，有很多不同类型的分类体系，对金融机构来说，重要的是定义信息分类级别和信息分类对制定可接受风险决策的影响。例如，某个风险对公开信息是可接受的但对高一级分类信息则是不可接受的。信息分类的一个好处是管理者可告知雇员：期望雇员如何处理信息。如果一个文档、文件或数据库包含不同级别的信息，应根据其中含有的最高级别信息对应的规程处置。

认识到信息级别在它使用周期中可变化是很重要的。这些变化应置于机构策略控制下。

5.3.2 安全实践文档

安全实践文档衍生于策略文档。这些文档描述了机构应遵守的一般安全条款。在创建信息安全方案中它们反映最高级别管理者的意图和设置的目标，文档目的是通过独立的技术方法实施策略。每个安全实践文档在范围上比策略文档狭窄。每个实践文档在技术上中立并且包含机构安全要求的描述内容。特定实践文档的大小是变化的和依赖主题的。

实践文档的数量应保持最少。文档需要的数量依机构规模和业务需要以及机构活动范围和复杂性而有所区别。影响机构的法律法规同样影响所需实践文档的数量。

实践文档不是公开的[3]。它本质上是通用目的、技术中立的。与策略文档相比缺乏概括性，因仅应用于机构的某个方面，所以可能对机构没有整体影响。例如，一个简单的实践文档仅包含如下简单内容：

“对公司信息资产的访问应以与资产敏感性相对应的方式鉴别。双因素鉴别(基于生物特征识别和基于口令)是可接受的最低鉴别级别。在访问被资产所有者分类为“机密”的资产时仅应采用三因素[4]鉴别。双因素鉴别(基于生物特征识别和基于口令)的访问控制系统应遵守如下规则……”

虽然实践文档的权限衍生于必须严格遵守的策略，但比策略文档更具有可变性。这是因为当识别

3) 可能有时需要为规则制定者提供实践文档。

4) 名词“三因素”通常解释为：“你有什么，你知道什么和你是什么”。你有什么——可以是一张卡或一个标志。你知道什么——可以是 PIN 或口令。生物特征可以代表你是什么。

出新的风险，应用了新的控制措施时，它们容易频繁地发生变更。每个实践文档有其严格限制的读者，因为它通常影响机构或业务单元的一个特定部分而不影响机构的整体安全管理方案。

实践文档包含一个指导读者和每个实践文档的所有者的章节，这是有好处的。实践所有者可能是一位业务经理、一位IT经理或运行主管。文档中包含给定实践信息的分类方法也有好处，分类的目录指明了要求的信息保护级别。

5.3.3 可操作的安全规程文档

可操作的安全规程文档衍生于一个或多个安全实践文档。它们的长度随规程的主题和复杂性而不同。在所有文档中这些文档的范围最狭窄。它们是策略如何实施的专业技术性描述。这些文档应用于实际的业务系统中，特定供货商的产品细节都包含在依赖平台的文档中。

应根据需要制定相应的规程文档。制定文档时应保证文档是完整的、准确的和恰当的，并且不能同其他实践或策略冲突。在一个非常简单的规程文档中可能包含如下内容：

“使用‘pwadmin’命令确保用户口令满足公司访问控制和鉴别实践文档中建立的标准。接下来的命令是……”

规程文档应符合机构整体策略和规程所依据的实践。规程文档不能与基于策略的实践冲突，并应对法规限制、外部生产标准和其他规程文档予以考虑。

规程文档应包括：先前的包含任何残余风险标识的安全风险分析和管理审查结果、随后行动的结果（诸如控制措施执行的安全符合性检查的结果）、日常信息安全行动监控和审查列表以及安全相关事故的报告。

6 信息安全管理——安全方案

6.1 概要

实施策略需要信息安全方案。在公司管理的最高层次上，公司管理的企业文化和强制控制措施应和员工交流，并定期强调这些企业文化和控制措施的重要性。信息安全既是个人的责任，也是基于团队合作的过程。信息安全方案的制定、维护、改进和监控需要机构内多个专业部门的协同参与。业务经理和信息安全职员应紧密协作。诸如审计、保险、法规符合性、物理安全、培训、职员、法律等方面的规定应用于支持信息安全方案。

6.2 方案建立

本标准最重要的建议是机构应建立一个信息安全方案。在公司管理的最高层次上，方案应遵循机构建立的策略。信息安全方案应提供符合策略的、覆盖整个机构的信息安全建立和维护机制。

制定一个详细的信息安全过程和规程可能要求机构内不同业务职能角色的合作，包括审计、风险、符合性、保险、负责法律法规符合性的官员以及合伙人和客户。

6.3 安全意识

安全意识方案应包括安全教育和安全意识，确保所有雇员了解与他们和他们周围人的活动相联系的安全问题并保持警觉。方案的结构应能使雇员知道他们的安全职责，应给对安全方面有兴趣的雇员提供资源并鼓励他们扩充知识。

6.4 审查

应指派一个或更多的机构官员承担对信息安全方案的责任，及时审查和更新方案，同时当新的威胁和技术出现时，确保必要的防护资金投入。方案应包括建立履行信息安全方案所需要的职责的详细的

过程和规程，以检查和报告信息安全方案的合理性及符合性。

各个层次的管理者，包括执行层，可得到所有的监控和审查报告。应明确对任何策略例外或偏差进行考虑的规程并形成文档。还应有对产品必要的审计、符合性记录和监控安全审计日志信息的规程。应引起特别关注的是：识别审计日志信息的风险、为减少这些风险制定的要求，以及那些为确保信息安全资产得到充分保护所规定的要求。

6.5 事故管理

所有信息安全事件应迅速报告、文档化并根据机构实践予以解决。当未预期到的信息安全事件很可能破坏业务运营和威胁信息安全时，它们就成为必须说明的信息安全事故。安全专家在重新评估风险和选择实施安全控制中都使用事故和事件。进行信息安全方案改进时也使用事件和事故。

6.6 监控

应建立正式的机制报告入侵、系统故障和其他安全事故，应在审查过程中使用安全事故论证结果和事故管理文档结论，以影响防护措施投资和保护资产的控制措施，使其在过期后能得到重新评价和变更。

6.7 符合性

应由独立的审查确保实践符合已建立的策略并且有充分和有效的控制措施。任何被许可免除的审查应及时文档化并限定时间以便可定期重新评估。

6.8 维护

已制定的控制措施，如防火墙和病毒扫描软件应定期更新以便有效防护新威胁。

6.9 灾难恢复

信息安全方案应标明在破坏事件中对机构持续业务运营活动起关键作用的信息资产。应在方案中对灾难后业务的恢复制定详细的书面计划。在制定计划时，应考虑掌握关键技能的员工、法律协定、信息备份系统以及可用作替代的支持关键业务活动的处理资源和场所等方面，并且这些灾难恢复计划应定期检查和评估。

7 信息安全机构

7.1 承诺

机构范围内信息安全方案目标的承诺，应基于机构对信息安全需要的理解。机构应通过愿意为信息安全活动投入资源和说明其信息安全需要来证明履行其承诺，机构最高层应关注信息安全对机构的意义，以及信息安全的范围和程度。

信息安全目标应在整个机构发布。每个雇员和承包商应知道他们的角色、责任和他们对信息安全的贡献，应赋予他们适当的权力去完成这些目标。

7.2 机构结构

7.2.1 角色和责任

信息安全方案的目的是确保信息资产的机密性、完整性、可用性。达成这些目标是一项跨专业部门的工作。应适当划分责任并分配给相应角色。规程应确保所有重要的工作以有效方式执行并完成。

7.2.2 管理者

金融机构的管理者对机构和股东负有监督机构业务管理实践的责任。有效的信息安全实践构成审慎业务实践，并体现其对建立公众信任的重视。管理者应传达信息安全是机构的重要目标的观念，并支持信息安全方案。

7.2.3 审计委员会

金融机构审计委员会在监管中协助董事会，作为一个独立的部门负责目标检查、平衡内部控制和财务报告。信息安全方案中的监督和检查是审计委员会的一部分职责，通常通过机构内部审计部门或外部审计师进行。

7.2.4 风险管理委员会

董事会下的风险管理委员会应审查安全方案，只要这些信息安全项目减少机构运营风险(从而减少财务风险)，就应为这些项目提供资金支持。风险管理委员会通过资助和支持能够实现机构信息安全策略的项目，体现出机构的安全承诺。如5.2中详细讨论的，委员会必须确定法律法规对信息安全方案的影响。

7.2.5 法律部门

机构可依靠自己法律部门的专业知识来解决信息安全管理某些方面的问题。法律部门有责任监管机构信息安全方案的法律、法规和案例等方面的变更。

应要求法律部门审查涉及雇员、客户、服务提供商、承包商和供货商的合同，以确保涉及信息安全方面的法律条款在合同中充分体现。这样的审查可包括隐私或工作场所安全条款以及雇员淘汰和投诉规程。

安全事故的法律问题及其对机构的影响可能需要法律部门的建议。机构可能希望依靠专家建议来评估安全事故处理规程的含义，确保符合运营环境方面的法律要求，这些要求由于当地规定不同而不同。法律部门应参与处理安全事故后续规程的制定、维护和改进，例如证据保留。

7.2.6 执行官

作为机构最高官员的首席执行官(CEO)或者总经理，对机构运营负有最终责任。CEO应授权建立符合公认标准的信息安全方案并对其提供支持，监管主要风险评估决策，参与宣传信息安全的重要性。

很多机构设有类似的首席执行官、首席财务官(CFO)、首席技术官(CTO)和首席运营官(COO)等角色，许多机构开始在机构高层引入另外的角色，例如首席信息官(CIO)和首席信息安全官(CISO)。CTO、CIO和CISO角色有很多其他变化，但每个金融机构应有一位资深官员或首席信息安全官最终向CTO或CIO汇报工作。

7.2.7 业务经理

专门的业务经理和机构内的其他经理，监督和管理机构雇员和代理商，这使得他们成为信息安全方案的参与者。每个经理应理解、支持和遵守机构的策略、实践和规程，并确保雇员、供货商和承包商也这样做。业务经理应创造积极的氛围鼓励雇员、供货商和承包商报告信息安全相关问题。

7.2.8 雇员

安全方案的要求应包含在雇员雇佣合同中。所有员工都应知道自身活动和周边活动的安全含义，以便他们能够主动报告任何可疑的信息安全事件。

7.2.9 外围

应在供货商服务协议和承包商协议中包含安全方案要求。供货商和承包商应理解、支持、遵守机构和业务部门的信息安全实践和规程，他们应遵守公司信息安全策略。当机构因经济或其他业务原因选择外包银行业务时，风险管理不可能外包，其责任仍属于机构。

7.2.10 安全角色

7.2.10.1 简介

这里说明了信息安全方案中个人的三个安全角色。这些角色被赋予执行信息安全方案所需要的不同的责任和功能。这里的三个角色是从功能性方面进行定义的，机构对人员如何监督和管理是不同的。

在一些机构中，信息安全人员存在于单独的管理部门中。另外一些机构中，业务部门的人员除他们的业务职责外还被分派了信息安全职责。也可能同时存在两种方法的混合。

无论信息安全方案采取何种结构，执行官和经理应支持它并使其有效。在大型机构中，设置其他角色可能对有效地实施特定功能更为有帮助，例如，一个安全架构师。在更小型的机构中，人员可能需要分派多重角色。

7.2.10.2 首席信息安全官(CISO)

首席信息安全官负责设计、实施和管理信息安全方案。在 CISO 的指导下，其他层次的人员执行信息安全方案的策略和实践中规定的职责。CISO 可有专门团队，对信息安全人员实施管理控制。在另外一种情况下，CISO 对那些除了业务责任之外还负有信息安全责任的人员进行有限的操作控制。不管机构类型和管理风格如何，CISO 都是在实施信息安全方案方面对董事和执行官负有最终责任的人。

CISO 按照机构确定的有利于其业务成功的条件管理信息安全方案。CISO 负责：

——向执行官提出预算并说明信息安全方案的合理性；

——设计符合业务战略的安全架构；

——管理实施安全架构和履行信息安全职责的其他级别的人员；

——完成使安全架构生效的风险评估并弥补需要关注的缺陷；

——发布安全策略、实践和规程并管理一个安全意识方案；

——保持对目前的威胁和脆弱性的了解，掌握解决它们的最新安全技术；

——确保本机构被恰当地纳入该机构业务所开展的国家的重要基础设施保护的工作中。

7.2.10.3 信息安全官(ISO)

信息安全官是机构中按 CISO 指示肩负制定、实施和维护信息安全方案职责的任何人员。ISO 可以是 CISO 的助手也可在机构业务部门控制之下。一个 ISO 可能是一个专门的职位，例如因为具有丰富的知识和经验而成为安全架构师。一些 ISO 因拥有专业的信息安全技术如风险评估、威胁知识等等而成为整个机构的资源。一些 ISO 可为特定业务部门提供信息安全方面的指导和建议。如果 ISO 既理解业务目标又了解机构内部过程，其工作将获得最高效率。

ISO 应：

——理解安全架构、实践和规程；

——制定本地实践，发布并在合适的时候更新实践；

——从事风险评估；

——监控和审计安全实践；

——帮助 IT 系统从攻击中恢复；

——给出改进实践和规程的建议；
——跟踪最新的安全威胁、技术和方法；
——提高信息安全意识。

7.2.10.4 安全操作者

安全操作者执行最详细的、日复一日的活动以完成信息安全方案的目标。安全操作者可能是CISO的助手，也可能属于机构其他部门。他们应熟悉所在业务部门的硬件、软件和所需的安全规程。

因为安全架构中可使用不同的技术，安全操作者需要执行大量的规程。一些典型的职责描述如下：安装和维护网络设备的安全设置；安装操作系统安全补丁；维护和更新正确的访问控制文件；收集安全信息、审计信息、监控系统和网络活动发现安全问题。这些范围广泛的工作显示出安全操作者在信息安全方案成功运行中的重要性。

安全操作者负责：
——理解如何支持安全架构和方案；
——实施和维护安全实践和规程；
——监督安全规程并在合适的时候报告它们的状态；
——纠正安全错误和对抗攻击；
——在一个错误或攻击后重建与业务恢复有关的适当的安全规程；
——对改进实践和规程提出建议。

8 风险分析和评估

8.1 过程

希望对其安全态势进行评估的机构应执行信息安全方案中的一个或多个风险分析过程。这些过程用于评估机构的整体安全态势以及特定项目、系统和产品的安全。因为管理风格和机构规模及结构不同，可能需要多个策略使风险分析适合其使用的环境[5]。

一个风险评估过程应给出降低机构安全风险到可接受级别的建议。这些建议应指导选择合适的控制措施。这些控制措施是评估并给出可能损失的结果，损失是一个或多个威胁利用了系统的可识别脆弱性而产生的。一般用于风险评估的机构资产包括：设施和设备、软件应用、公司数据库、通信系统和计算机操作系统。

附录C给出了一个实施风险评估方法的例子和一个典型的风险评估过程的例子。其他风险评估模型可在另外的资源中找到，例如ISO/IEC 13335(所有部分)。附录C中的例子提供了一个例证，不宜直接用作实施检查列表。

8.2 风险评估过程

金融机构和所有其他企业受到业务风险的影响。企业信息资产风险以多种形式存在，应系统地加以分析。风险评估需要考虑信息的脆弱性、威胁和风险。每个银行业务应用提供工作过程、潜在威胁及脆弱性位置等方面的背景和理解。这种理解对执行风险评估是重要的。风险评估分三步：

1) 通过完成风险评估矩阵，评估每个脆弱性区域潜在威胁的风险(见附录C.1)；
2) 通过完成风险评估表确定每个脆弱性区域的组合的风险级别(见附录C.3)；
3) 使用步骤2的结果和可用的控制措施确定合适的安全策略和防护措施。

更详细的风险目录列表和它们如何用于风险评估过程在附录C中给出。

5) 额外信息见ISO/IEC 13335(所有部分)。

8.3 安全建议和风险接受

在一个相关的系统集合内，或通过一个单一的系统或单一的应用，或一个系统内的特定的功能便可执行风险评估，以此来评价机构的风险。期望机构风险评估是机构内所有关键功能的简单组合是不现实的。

随着新技术的出现，脆弱性和威胁也不断地发生改变。在系统中发现新脆弱性，则引进新的或升级的产品进行应对，使得机构持续成长和发展。因此，一个机构内的不同的系统和不同机构的类似系统，它们的风险评估级别的描述和结论可能有显著的差异。

不过，任何风险评估都产生对评估系统的一组安全建议。这些可执行的建议说明了与系统相联系的风险。适度接受风险是业务经理的责任。在很多情况下，附加的控制措施用于(或在设计和开发阶段可能已经使用)把风险降低到可接受的级别。风险接受最好考虑机构的安全实践。考虑到执行安全策略的例外情况，业务经理应同信息安全团队一同工作，以确保将来满足策略要求，或者将长期的策略例外视为可接受的残余风险。

9 安全控制实施和选择

9.1 风险减缓

任何系统都存在脆弱性，一旦遭受攻击可能会导致机构财务损失、生产率损失和信誉损失。减缓这些风险，使风险最小化是机构内业务经理和与其他团队一起工作的信息安全团队共同的责任。管理安全有许多方面，例如上面讨论的最高管理层信息安全职责、CISO 对实施和管理信息安全方案的责任、安全方案自身等方面。

9.2～9.7 讨论了可用和可考虑的减缓风险的重要过程和通用技术，这些主要用于处理评估发现的高风险或处理新的脆弱性。业务经理应记住将安全融入系统设计的优点而不要试图在现存的系统上修补漏洞。

使用这些技术可提供直接的控制措施覆盖机构的风险。机构需要评估已计划好的和现存的控制如何减少风险分析中识别的风险，识别额外的可使用的或可开发的控制措施，开发信息安全架构和决定不同类型的约束。选择适当的和经过证明的控制措施来使已评估的风险降低到可接受的残余风险级别。另外的控制措施选择的详细说明见 ISO/IEC 13335[4](所有部分)。

9.2 约束识别和审查

很多约束可影响控制措施的选择。在提出建议和实施期间，这些约束应予以考虑。典型的约束和需要考虑的事情包括：

约束	需要考虑的事情。
时间	控制措施应在管理者接受的日期内实施，应在系统生命周期内实施并且只要管理者认为需要就应一直发挥作用。
财务	控制措施在实施上不应过于昂贵以致超出设计它们用于保护的机构资产的价值。
技术	控制措施应在技术上可行并与系统相兼容。
社会	控制措施可针对一个国家、地区、机构，甚至机构内一个部门，并确保为员工所接受。
环境	选择的控制措施需适应：可用空间、气候条件、自然环境和城市地理等等。
法律	控制措施既要考虑类似个人数据保护方面的法律因素、又要考虑非 IT 方面的法律法规，如消防法、劳动法等法律法规。

9.3 逻辑访问控制

9.3.1 概要

逻辑访问控制指系统采用的一组技术控制方法以及根据机构实践来限制信息访问的应用。一般来说，应给用户所需的最低访问权限以完成他们的工作任务，但经常由于系统的限制、设计或其他约束导致用户有一些额外的访问权限。不管怎样，保证系统访问的可核查性是至关重要的：例如知道谁被授权访问，知道个人访问了什么，知道什么时候访问发生了。其中最重要的是：一旦定义就应强制执行访问限制。以下控制措施应置于合适位置以完成有效的访问控制。

9.3.2 用户标识

有很多不同类型的用户有理由访问金融机构的信息和信息系统。用户包括雇员、客户、系统管理员和经理。在多数情况下，需要在某种程度上知道，哪种类型的用户试图获得对特定应用的访问。经常需要知道的不仅仅是类别，而是确切识别谁在试图获得访问权限。

传统上每个信息系统都有自己的识别过程。随着系统的快速扩展，多样化的系统的识别过程不断产生新的需求。外包这些识别服务可能是可行的。下面的指南适用于任何识别服务提供商。

为了在用户标识中提供更高的信任级别，机构应建立和执行在用户 ID 发布之前要求证明用户身份的策略。审慎业务实践要求将“知道你的客户”和“知道你的雇员”结合到用户 ID 发布活动中。更进一步，机构应建立和执行规程以确保每个用户 ID 在发布之前是惟一的，并可追溯到被识别的个人和发布者。

9.3.3 授权

授权是为已验证身份的用户提供执行系统特定功能的活动。机构应决定每个用户的访问权限。除非专门授权，不允许用户访问任何信息或应用。

基于角色的访问控制(RBAC)的维护记录有几种样式。一种传统的样式是使用列表维护每个用户的权限。通常在双重控制下工作的系统安全管理员追踪和维护这样的记录。安全软件把用户 ID 和记录进行匹配并根据这些记录允许用户访问信息和应用。

另一种样式针对分散的维护记录，每个系统有一个访问控制列表，或对不同应用的单独访问(例如瘦客户端、肥客户端、web、多层结构、web 服务等等)。

9.3.4 用户鉴别

9.3.4.1 机制

用户鉴别是指(例如，规程的、物理的或通过硬件/软件)验证用户身份的过程。用户可以是机构内部的也可是机构外部的，失败的用户身份鉴别可导致机构无法证明一个人对其活动是否负有责任，并可能造成对数据和计算机资源的未授权访问。

有几种不同类型的鉴别机制。它们基于一个或多个特征：用户所知(例如口令)、用户所有(例如智能卡)、用户的某种物理特征(指纹或其他生物特征)。混合多重鉴别机制可确保更高等级的鉴别。

9.3.4.2 数字证书

数字证书用于签名或加密信息，以及为用户、程序代码和设备提供鉴别。基于证书的数字签名可用于提供鉴别信息来源、数据完整性和抗抵赖服务。基于证书的数据隐私服务可用于加密。

ISO 15782 说明了在金融服务中 X.509 证书中的证书管理需要的控制和语法。ISO 21188 提供关于机构中如何管理证书安全策略的详细信息以及证书业务声明中必需的要素。

9.3.4.3 口令

现在使用最普遍的鉴别方式是口令。口令是由字母、数字和键盘特殊字符的任意组合构成的一个字符串。与一个用户相联系的口令被认为是用户使用权利(例如访问系统中的特定程序、功能和文件)的授权证明。

口令可以是动态的(例如通过软件自动的,一般是频繁的生成和变更)或静态的(例如由用户自主决定的不频繁的变更)。很多出版物和 WEB 页面上可找到生成和控制口令的指南。标注日期为 1985 年 4 月 12 日(CSC-STD-002-85)的"美国国防部保护口令管理指南"提供了机构内生成、控制和使用口令的技术处理方法。http://computing. fnal. gov/security/userguide/password. htm 上的讨论提供了关于这个问题以及口令共享、组成和长度、变更和存储的一般处理方法。

9.3.4.4 生物特征识别

生物特征识别是一门通过生理特征来识别人员的科学,可以通过这些生理特征准确识别每个个体,这些生理特征具有高度惟一性。指纹可能是已知的最好的生物特征。已存在能读取指纹的电子设备,这些设备能将图像与已存储在系统中的图像做对比。其他的用于生物特征识别系统中的生理特征还包括眼睛视网膜、手形、脸部特征和声音。

ISO 19092[11]描述了在金融服务中如何将生物特征识别信息作为机构信息安全管理方案的一部分来进行管理。该技术报告说明了控制目标、控制措施、管理生物特征识别信息的详细事件日志以及如何达到这些目标。

9.4 审计日志

审计日志是系统生成的活动的记录,由机构使用,以提供一种重现事件和建立可核查性的手段。审计日志对问题或争论的解决至关重要,并且提供遵守法规的证据。审计日志帮助制止未授权活动并提供对这种活动的早期检测。所有系统应根据机构策略提供不同级别的审计日志。另外,级别的细节应尽可能详细,并与运营需要和机构策略保持一致。实用性方面,审计应提供重大安全事件的实时警告。

审计系统应支持即时调查和报告可疑活动。以帮助制止和检测未授权活动。管理者应按时(一般按天)执行对审计日志信息的审查,所有安全例外和异常事件都应调查和报告。

所有审计日志信息应根据业务要求保存一段合适的时间。这些信息应得到保护,免受偶然或恶意删除、篡改和伪造。

9.5 变更控制

为保护机构信息处理设施的完整性,应实施控制措施变更规程。如果没有变更控制,错误的处置或缺失服务将导致财务和效率的损失。变更控制因如下原因而存在:硬件变更、为应用软件和操作系统的补丁管理而发生的变更和手动规程的变更。这些变更控制规程也应说明如何管理紧急变更。

业务经理应确保由他们控制的系统变更控制过程的正确性。信息安全团队应准备好帮助管理安全相关的变更并管理信息安全团队直接负责管理的安全系统的变更。

9.6 信息安全意识

信息安全方案的一部分应是安全意识运动,以教育雇员保护机构的有价值信息。这部分方案以积极的方式影响雇员对信息安全的态度。安全意识应经常强调。

一个安全意识方案应包括一个对新雇员和新公司雇员的安全意识培训。无论何时引入新应用还是对已有应用作大范围修改,都应对用户进行培训。信息安全方案中应纳入公开报道的信息安全相关

问题。

不同层次的管理者和员工有不同的关注点。当描述每个群体时应强调他们的特殊关注点。应使用所有层次和技能的人都理解的方式表述。经理们应知道泄露、风险、潜在损失和法规、审计的要求。这应在业务条款中描述，并且伴随与管理者职责领域相关的例子以及积极有效的信息。

9.7 人员因素

劳动力是金融机构最重要的资产。雇员的兴趣和合作在任何成功的信息安全方案中都是至关重要的。通过提升安全意识，提示雇员注意机构技术或操作规程中的异常，这些异常可能表明有安全问题。

另一方面，人也会犯错误。他们可能错误使用技术，他们可能犯罪，这些人为的错误使 CISO 有必要同机构所有部门就信息安全方案的制定和安全意识展开对话。其他部门可提供他们对机构雇员的观察以减少错误和犯罪活动的机会。

机构中某些职位应设置为“可信的”，这种职位允许或需要访问敏感的人事或财务信息。另一种可信的职位是对机构计算机或 IT 资产拥有广泛权力和强大能力的职位。被选择到“可信”位置的人员应极其忠诚并经过背景调查。应劝告可信位置上的雇员：不许与他们的家人和熟人讨论敏感的业务规程。业务竞争对手可能试图通过“社会工程”引诱人们泄露信息给未授权的人。引诱者对人们的工作、技术讨论显示虚伪的兴趣和奉承使雇员无意中透露敏感信息。

10 IT 系统控制

10.1 保护 IT 系统

保护 IT 系统有很多种控制措施，其中可包括机构策略。然而第 10 章中，控制措施表示为系统设置和外部对策(例如加密)，这些控制措施用于提供鉴别、授权、机密性、完整性、可用性和其他安全服务。本章将讨论目前正在使用和未来可能用到的对策和控制措施。

除了初始的控制措施和策略，机构应采取步骤确保它们长期运作并得到维护，否则，随着时间推移，当新的脆弱性出现和发布的新补丁被忽视时，系统的安全将受到侵害。一个运作良好的安全方案应包括维护过程和规程以确保所要求的控制措施是合适的并能保持及时更新。

10.2 硬件系统控制

保护 IT 环境中的硬件系统对信息资产的完整性是至关重要的。附录 D 讨论了一些极其重要的保护关键资源的控制措施。本标准不包含一个机构可能使用的所有 IT 资源的综合列表，但将对几个主要资源进行简短的讨论。附录 D.1 提供了可使用的减少对这些资源威胁的一些合适的控制措施。每个讨论遵循一个相似的模板。关键要点在每个讨论中都加以说明，例如，为何一个专门的系统很重要，最重要的安全领域是什么，哪些控制措施需要考虑。

一个未说明、有时机构也缺乏考虑的是硬件系统的供应商的问题。通常对其采用信任的态度，即设备供应商和制造商为金融机构的利益工作，或知道他们的安全目标和策略。然而，由制造商和销售商配置好的机器可能提供对信息和网络连接的未授权访问。随机选购和在网络中分散部署机器能帮助防护这种恶意或偶然的威胁。在更高级别的安全应用中，可能需要考虑在机构和供货商之间建立可信任的控制措施。

特别地，对密码设备，应重点考虑硬件评估，例如 FIPS140-2[6)][17]。对其他设备，在选择和使用时应依赖于遵循适当的或行业标准保护轮廓的通用准则评价。

---

6) FIPS 140-2 即将形成国际标准 ISO/IEC 19790。

10.3 软件系统安全

现代金融机构几乎完全自动化地处理全部交易，所以信息安全方案的核心是软件安全。因为软件的复杂性、大量交互以及访问软件的多重途径，确保软件系统的安全是困难的。另外，许多系统如防火墙、Web 服务器和应用服务器设计为可在许多硬件平台上运行。因为有很多详细讨论每个类型软件系统的文献存在，附录 A.2 的材料仅在宏观上讨论了软件系统安全。

10.4 网络和网络系统控制

虽然一个机构的复杂的处理系统，包括终端系统和不同类型的服务器，常常被认为是最重要的，但系统之间最主要的通信量发生在网络上，既没有加密，也没有特别好的管理。多数互联网和很多公司专用的“租赁线路”使用相同的开放协议和路由系统，在某些情况下与其他公司共享同样的网络设备和交换机。

网络通信容易遭受重新路由攻击、拷贝、数据包嗅探[7]攻击而完全难以被网络和使用网络的系统检测到。加密常常被看作通信安全的灵丹妙药，但对很多企业来说，网络层加密过于昂贵，在性能、吞吐量和时延上开销太大。虽然可使用 SSL、IPSEC 和其他安全通信协议，但它们对网络安全的第一道防线也不是必须的。为管理网络安全，可考虑 ISO/IEC 18028 中的指南。

作为替代，第一道防线通常是机构和电信供应商之间的合同安排以及对电信供应商的信任。因此，使用知名的电信供应商，精心定义的服务条款和考虑周到的合同语言，常常是第一位和最重要的控制措施。下一个最重要的网络控制措施是系统边界控制(如 10.5 所描述)，该措施用于保护、监控和管理机构内网和外网之间的连接。

10.5 边界和连接控制

10.5.1 概述

增加公司网络开放性的文献已经很多。由于 web 服务、业务伙伴、外包支持、伴随记录系统的客户交互、临时和合同制劳工以及雇员访问(这些都是远程访问，从家庭和外部连接到其他业务)，原来曾经稳定、紧密控制的边界现在变的开放了。日益增加的边界渗透意味着边界和连接系统成为公司信息安全一个关键要素。这种渗透性也意味着越来越多的设备可能成为恶意活动的进入点。这些设备需要考虑用防火墙、入侵检测或其他可能的控制措施来保护，如附录 D.1.1 终端系统的讨论中指出的那样。

企业与大的网络工作环境之间的所有这些边界连接都很关键。任何边界都代表了攻击企业脆弱性的机会。企业需要为如何应用边界控制措施制定自己的策略。例如，一个机构要求隔离以达到高等级的安全环境，具体的例子如：所有用户和终端系统应以物理方式在机构的建筑内部连接。另一方面，一个机构可在一个安全数据库内保护它所有的信息资产，这个数据库在一个安全 web 应用服务器、多层防火墙和入侵检测软件之后，或者有功能强大的用户鉴别检查。合适的措施取决于机构资产、风险评估和他们的策略。

10.5.2 防火墙

防火墙代表了在网络层提供边界控制的成熟技术。尽管实际功能和性能不同，所有防火墙设置在企业连接其他实体或互联网的边界路由器和交换机与企业内部网的路由器之间。一个设计很好的防火墙是保护企业网络的基本要素。

防火墙基于地址、端口、协议和(某些情况下)包的内容监控网络通信。在很多机构中，防火墙仅开

7) “数据包嗅探器”是一个程序，当信息“包”在网络中传输时，对其进行分析，寻找可用于攻击的信息，例如 e-mail 报文的内容、用户名和密码或网络地址。

放所有可用地址、端口和协议中一个非常小的部分。例如，一个防火墙保护一个复杂的 web 服务器仅允许 HTTP 协议 80 端口或 HTTPS 协议 443 端口(也就是 SSL)通过。其他端口如 FTP 服务、SMTP (e-mail)，可开放也可关闭，这取决于机构的需要和策略。

很多机构应用两层防火墙创建一个 DMZ 或称为非军事区。web 服务器和其他面向外部的服务器和服务置于两个防火墙层之间。对大企业内部服务和数据的请求通信被重定格式和重定向。外部防火墙可仅支持 HTTP 通信，内部防火墙可允许 SSH(安全壳)或其他服务，以支持管理 web 服务器的访问，或允许 web 服务器访问内部数据库。一个通用的实践是针对内部和外部位置使用两种不同类型(不同的制造商)的防火墙。

历史上，防火墙是特殊用途的软件，位于网络路径上，保护企业的大部分特定应用。它们是坚固的网络边界设施中最主要的一部分。在过去的两三年中，防火墙已整合到终端系统中，常称为用户防火墙。主要网络连接使用的专用防火墙、个人计算机和其他终端系统上的个人防火墙的使用正在持续发展。

最近的趋势是防火墙功能和入侵检测能力相结合。

10.5.3 入侵检测系统(IDS)

防火墙频繁地根据地址、端口和协议接受或拒绝连接。在这些参数中，可能存在许多含有真实攻击或恶意软件的数据流——当然主体是支持合法的业务活动的数据流。入侵检测系统观察包内的数据并将它们同已知攻击的特性作对比。检测系统通过 e-mail、电话或纸面向机构内的适当人员发出警报。有两种主要类型的 IDS：网络检测型 IDS 连接到网络路由器、交换机和服务器，以此来检查网络通信；基于主机的检测类型的 IDS 是装入服务器或终端系统的软件，用于检查连接到特定设备的通信。企业部署两种检测类型的数量日益增长[8)]。

IDS 系统依赖已知攻击特征进行安全检测，对于未知特征的新的有效攻击，IDS 可能无法检查到，因而具有一定的局限性。IDS 系统开始寻找系统行为中的异常，例如一般使用 HTTP 通信的地方出现 FTP 通信，或者在奇怪的时间或以不正常的量进行通信。这种异常情况检测的能力正变得日益精确和复杂，但它们的价值并未得到广泛的证实。虽然如此，很多机构和多数 IDS 供应商开始增加 IDS 的分析能力或寻找异常的分析，不仅在边界上，而且在企业网络内部。

一些分析工具是纯粹的工具，依靠其他设备捕获的数据用于查找异常。防火墙和 IDS 系统开始整合：供货商经常销售同时具有防火墙和 IDS 功能的产品。这些产品也经常用于——特别是当 IDS 包括异常检测功能时——执行入侵保护。在这些新出现的入侵保护系统中，会关闭检测到的被用于攻击的网络连接，以在攻击完成前终止或预防它。虽然这是完美的可接受的实践，但应有一个权衡，因为其他合法的通信可能正在通过同一个连接。机构应自己权衡允许合法通信的价值和可能的攻击损失。

允许可能的攻击与攻击可能造成的损失的价值对比判断，是 IDS 系统局限性最重要的部分。事实上任何 IDS 系统都有一定数量的误报。就是在某些情况下 IDS 发布一个看上去像攻击的警告但实际上是合法的。同样地，存在(非常少)一个攻击未检测到而通过的可能性。IDS 系统允许机构有相当大的自由度调整系统，以最小化误报和漏报。

10.5.4 其他保护对策

有很多其他的保护网络边界和连接的对策。不同的应用案例需要不同的考虑。例如，一个封闭的业务部门可有一个内部网的直接连接，或者可通过一个简单的防火墙路由，而不是通过两层防火墙。这些构成机构内部网络的路由器和交换机应被保护并妥善管理。很多作为路由功能之后的保护层的防火墙功能已经由网络基础设施完成了。在网络、防火墙和 IDS 之上，有两个其他主要对策：加密和鉴别。

8) JTC 1/SC 27 信息安全技术组已经开始制定一个 IDS 标准，ISO/IEC 18043。

加密显然可用于保护秘密信息。这可在许多层上和许多地方做，但应考虑成本。这些权衡需要根据机构策略和公司信息价值来评估。

鉴别用于设备和设备的用户（包括软件“用户”）。设备可通过使用 IPSEC 或在某种程度上通过 SSL 来鉴别。终端用户可通过 SSL 来鉴别，虽然 SSL 实际上不能真正鉴别用户（例如，一些浏览器记住用户名和口令，任何使用该计算机和浏览器的任何人在 Web 服务器看来都是同一个用户）。使用多因素而非仅依靠用户 ID 和口令可加强鉴别，但这样的话用户需要拥有一个令牌或智能卡，拥有一个与数字证书关联的私钥或者指纹（或其他生物特征）。

11 实施特定控制措施

11.1 金融交易卡

11.1.1 概述

金融交易卡可以是在磁介质上存贮信息的磁条卡或者是可处理信息，执行加密功能和比磁介质存储更多信息的“智能卡”[9]。因为智能卡比磁条卡有更多的灵活性，未来将开发这种卡的其他应用。请参考 ISO 10202 智能卡安全相关问题。

金融卡协会维护着他们自己的最低安全标准，这些标准主要用于金融机构和给金融机构提供服务的合同商。除了那些安全方案外，使用金融交易卡的机构应采用下列的安全控制措施。

11.1.2 物理安全

在处理阶段为保护交易卡信息免受破坏、泄露和篡改，卡个人化设施应放置在公安部门定期巡逻的地方和消防部门能服务的地方。这些设施应能通过备用电力发出入侵警报而得到保护。

11.1.3 内部人员滥用

为防止欺诈交易通过访问卡的信息而发生，所有包含合法的账户信息、账号、PIN、信贷限额和账户余额的介质应存储在只对选择过的员工开放的限定区域。卡的生产和发布功能应与 PIN 的生成和发布功能在物理上独立。

11.1.4 PIN 的传输

为防止 PIN 被未授权的人截取而丢失，应根据 ISO 9564-1 到 ISO 9564-4 或 ISO 10202-1 到 ISO 10202-8处理 PIN。ISO 9564 描述了提供有效的国际的 PIN 管理所需的最小安全措施方面的基本原则和技术。它也描述了应用于在线环境中金融交易卡发生交易时 PIN 保护技术，以及 PIN 数据互换的标准方法。ISO 9564 也包含了离线 PIN 环境和电子商务环境中 PIN 的管理和安全。机构应使用这些技术手段来管理和保护自动柜员机（ATM）和收单方部署的销售点（POS）终端中 PIN 信息。

注：ISO 13491-1[5]描述了金融服务设备（POS、ATM）需要的密钥管理控制措施。

本标准不覆盖非 PIN 交易数据的保密、保护 PIN 防止丢失、客户或发行方雇员故意的滥用，保护交易报文防止变更或替代，例如对一个 PIN 验证的授权响应，保护 PIN 或交易防止重放，或特定的密钥管理技术。负责实施技术以管理和保护自动柜员机（ATM）和收单方部署的销售点（POS）终端中 PIN 信息的机构，可使用这些技术。ISO 10202 描述了整个生命周期中，从卡制造到卡发行，从客户和雇员的使用到终止，IC 卡保护的原则。ISO 10202 还描述了交换要求的最低安全级别和安全选择权，即允许

9) “智能卡”这个术语描述了具有不同功能和能力的支付卡片大小的设备。这些设备与人们熟知的磁条卡（用于贷记、借记、ATM 和 POS 交易）具有几乎一致的外观。智能卡包括集成电路卡（ICC），储值卡和非接触式卡。

金融交易卡发卡方或供应商按应用策略选择一个合适的安全级别和安全策略。ISO 10202 中还描述了加密密钥关系、正确使用密钥算法和金融交易过程安全所需的密钥管理技术。ISO 10202 也描述了可加入到卡接受设备中的应用模式的安全要求。

11.1.5 员工

为防止将贷记卡处理责任分派给不合适的员工，在法律允许的情况下，应对所有处理凸印卡或背面未签名卡的雇员，包括兼职的和临时的雇员，进行信用和犯罪记录检查。

11.1.6 审计

为确保控制和审计信息的完整性，要求维护对打印塑胶表、图版、雕版和编码的设备、签名贴箔面板、全息图、磁带、完工的半成品和成品、样本卡、卡持有者账号信息和废物处理设备的控制措施和审计日志。

11.1.7 防止伪造卡

为防止销售划款中泄露信息用于生产伪造磁条卡，加密校验码应编码到磁条中并且这些编码在交易中应尽可能验证。

为防止截取信息用于生产伪造卡，物理卡鉴别方式(CAM)应用于验证卡的真实性。

11.1.8 自动柜员机

自动柜员机允许客户查询余额、取现和存款、付账单或者办理其他的一般柜员业务。这些设备可位于机构建筑内部、与机构建筑相连的外部或者远离任何机构办公地点。

为减少抢劫客户和恶意破坏机器，可提出更多的防护建议，但这超出了本标准的范围。这些设备的制造商和 ATM 网络的供应商一般出版使用 ATM 的安全指南。这些文档应予以参考。ATM 交易应遵守卡支付设计中规定的安全要求。

11.1.9 持卡者身份和鉴别

最普遍使用的鉴别持卡者的方法是个人识别码(PIN)。它们用于控制访问 ATM 和 POS 设备。应教育用户使其理解 PIN 安全是他们自己的责任。除了 PIN，生物特征识别和其他技术开始用于持卡者识别。

为防止未授权交易导致猜出 PIN 而使卡被未授权的人使用，尝试 PIN 输入的数量应限制为三次。三次尝试没有成功，建议锁住卡并联系拥有者。

11.1.10 鉴别信息

为防止信息进出 ATM 的传输中被未授权篡改，要求每次传输使用 ISO 16609 规定生成的报文鉴别码并按 ISO 11568 规定分发。为防止未授权篡改、破坏或泄露驻留在 ATM 中的信息，对 ATM 内部的物理访问控制应与目前现金箱物理安全保护控制保持一致。

11.1.11 信息泄露

为防止由于泄露用户输入的 PIN 信息而导致未授权使用 ATM 和 POS 终端，仅允许使用带有符合 ISO 9564 标准的加密键盘的设备。应考虑加密所有来自 ATM 的传输信息。应根据 ISO 相关标准管理 PIN。

11.1.12 欺诈防护

为检测和防护欺诈使用 ATM，如空头支票、空白信封存款和抵赖交易，提出了一系列建议。这包

括限制每天每个账户交易次数和取款数量，双重控制下每天进行 ATM 资金平衡，安装摄像头防止欺诈或给予潜在的警告，尽可能维持 ATM 在线的运营，例如要求 ATM 具有完成交易前能检查账户余额的能力。如果在线运营是不可能的，应建立比在线运营更严格的发卡要求。

11.1.13 维护和服务

为防止维护和服务 ATM 期间未授权访问信息，在实施任何维护之前应确保 ATM 提示“停止服务”。对涉及打开 ATM 钞箱的服务应建立双重控制措施。

11.2 电子资金转账

11.2.1 未授权来源

与电子资金转账(EFT)有关的威胁和控措施应独立于它们使用的技术予以评价。为防止接受未授权来源的支付请求而遭受损失，应鉴别请求资金转账的报文的来源。应根据客户与合作方同意的安全规程鉴别来源。只要加密鉴别的成本和性能使得这种控制可行时，就推荐使用它。

按 ISO 16609 规定生成的 MAC 和按 ISO 11568 规定分发的加密密钥一起提供了加密鉴别。另外，按 ISO/IEC 18033(同 ISO/TR 19038[10]或 ANSI X9.52[14]一起)或 FIPS 197[18]，以及按 ISO 11568 的规定分发的密钥，成功解密加密的报文，可用于建立报文源鉴别，也可使用数字签名。

11.2.2 未授权变更

为防止因故意或意外变更报文内容导致错误的支付，应使用客户与合作方同意的指定安全规程鉴别报文中的支付日期、起息日、金额、币种、收益方姓名和可能有的收益方账号或 IBAN 组件。只要可行，所有文本都应鉴别。建议加密鉴别。

11.2.3 报文重放

为防止重放的报文导致未授权的重复支付，要求使用并验证报文标识的惟一性。在任何鉴别中应包括这个标识。

11.2.4 记录保留

为保存需要的证据证明支付的授权，无论传输报文使用何种介质，应记录资金转账要求的报文。证明授权需要的材料，包括支持加密的材料，应予以保存。

11.2.5 支付的法律基础

为确保正在进行的支付符合已签署的协议，应建立一个系统确保 EFT 请求基础协议是适当的和符合当前情况的。

11.3 支票

11.3.1 概述

支票，也称为可转让取款命令或提款权，是指示金融机构付款的书面命令。几种新的处理支票的方法增加了金融机构的安全问题。支票影像和其他截留设计是产生安全问题的技术例子。很多国家发布了支票处理操作的不同方面标准[10]。

---

10) X9 的 B 分委员会(美国)已发布了支票处理操作标准，例如 ANSI X9 TG-2 支票的理解和设计 、ANSI X9 TG-8 支票安全指南。为在金融机构间兼容并提升处理过程的性能，鼓励金融机构遵守 X9 技术指南 2(TG-2)和 X9 技术指南 8(TG-8)的建议。

11.3.2 新客户

当通过开放网络提供服务时，“了解客户”的要求面临特殊的挑战。虽然通过使用网页或其他电子媒介对金融服务进行宣传是可取的，但是，除非出现正确识别人员的普遍认可和强制的电子方法，否则个人还必须亲自到金融机构业务场所开立新账户。应遵守正常的客户验证规程。

11.3.3 完整性问题

应保护每个交易以确保识别用户身份、鉴别用户真实性、鉴别报文真实性、保护敏感信息的机密性、指令的抗抵赖性。

应通过机构的认证部门对交易请求使用鉴别密钥进行数字签名。正确的实施后，可确保正确识别用户，报文内容不可更改，用户和他的行为就实现了合法的绑定。

账号、PIN 或其他信息，一旦泄露，将允许对账户的未授权使用，因此这些应予以加密保护。

12 辅助项

12.1 保险

在设计信息安全方案时，信息安全官和业务经理应同保险部门、承保人(如果可能的话)协商。这样做可以使信息安全方案更有效，更好的使用保险费。

在索赔之前承保人可能要求可靠的控制措施，称为责任前条件或先例条件。责任前条件常处理信息安全控制措施。因为这些控制措施对保险的目的来说是恰当的，所以它们被整合进机构的信息安全方案。一些控制措施也可要求被担保，即从策略的开始，就显示其恰当性。

业务中断的保险范围，特别是失误和遗漏保险范围，一般应和信息安全计划结合。

12.2 审计

以下引用来自国际内部审计师协会定义的审计师角色：

“内部审计是一个独立的、为确保目标和协商而设计的活动，以增加价值和改进机构运营。它通过系统的、严格的方法评估和改进风险管理、控制措施、过程管理的效率来帮助机构完成它的目标。内部审计审查信息的可靠性和完整性、策略和法规的符合性、资产防护措施、经济的和高效的使用资源、已确立的可操作的目标。”

更明确来说，在信息安全领域，审计师应评估和测试覆盖金融机构信息资产的防护措施。致力于同信息安全官和其他人士及时沟通，对识别威胁、风险和已有或新产品的足够防护措施提出正确的观点。

审计师为管理者提供涉及控制环境的情况的客观报告，以及推荐经过需求和成本利益方面论证的改进措施，详述审计日志信息的保存和审查。在审计功能同其他功能结合的地方，要求管理者注意使潜在的利益冲突最小化。

12.3 灾难恢复计划

信息安全方案的一个重要部分是在破坏事件中继续重要交易的计划。灾难恢复是业务恢复计划的一部分，业务恢复确保信息和信息处理设备在中断后尽可能快地恢复。灾难恢复计划要确定必须实施保护的范围，并列出在灾难情况下的人员角色和人员责任。

灾难恢复计划应包括一个业务活动的重要性、优先级别的准确列表，并且应包括满足机构业务责任的合理的恢复时间框架。计划应确定能支持重要的业务活动的可用的灾备资源和场所。

在灾难事件中，当责任员工无法履行职责时，应确定能够恢复和运行信息处理资源的替代人员。如有可能，机构应寻求同服务提供商达成协议，以尽快恢复服务。灾难恢复计划应确保信息备份系统的可

用性，该系统能及时定位和恢复关键信息。

很重要的是，灾难恢复计划应确保备份信息，确保备份信息安全的存储和按拟定的计划备份，信息存储的位置应予以明确标识，同时应给出在现场和不在现场的要求。

灾难恢复计划应根据需要尽可能频繁的测试以发现问题，并且在运作中不断进行人员培训。周期性对灾难恢复计划进行重新评价，以确定它仍然满足要求。机构应指定测试和重新评估的最小频度。

12.4 外部服务提供商

金融机构需要外部提供至关重要的服务，例如数据处理、交易处理、网络服务和软件制作，应和机构内部处理活动一样接受相同级别的防护措施和信息保护。外部服务商合同应包括如下必要条款满足金融机构的要求：

——供应商应遵守机构的安全策略和实践；

——由公共会计事务所出具的供应商的有效报告给机构；

——机构内部审计员有权对提供商涉及金融机构的相关规程和防护措施进行审计；

——提供商应遵守交付系统、产品或服务的有条件转让契约。

除如上所述之外，在执行服务提供商的合同之前，金融机构内部的专家应对供应商实施独立的财务审查。

除非获得了信息安全防护已到位的书面保证，不能和服务提供商开展任何业务。CISO 应检查服务提供商的安全方案以判断是否和本机构的相一致。任何不足应通过和供应商的谈判或通过机构内的风险接受过程来加以解决。

除了信息安全要求，同服务提供商的合同应包括非泄露条款和因信息安全过失导致损失方面的清晰责任划分。

12.5 渗透测试组

使用渗透测试组，通常是承包商，在得到机构适当官员的同意下，利用专业知识通过对系统的渗透攻击来测试系统安全访问的有效性。这是系统安全方案获得保证的一种方法。

随着计算机系统变得越来越复杂，安全也变得越来越难以维护。使用渗透测试组可帮助发现机构系统特有的脆弱性。然而，应考虑一些问题。承包商应有足够的保证或足够的力量承担由于他们的工作带来的责任。

机构不能仅依靠渗透测试报告来监控它的安全方案。

在与渗透测试组的合同中应注明结果不能泄露。任何安全问题的揭示应由机构掌控。

12.6 密码操作

IT 的发展已经给传统的控制信息的方法带来更多的挑战。广泛使用的加密设备使银行等金融机构有能力重新获得原先的安全级别，同时从日益增长的信息处理技术中获益。

像任何新出现的技术一样，存在误用密码解决方案的危险。对机构来说在基于防护的密码技术的选择、使用和持续评价上作出适当的决策是重要的。

假定已经认识到了密码防护措施的需要。这些防护措施在第 9～14 章中给出，包括应用加密、报文鉴别码和数字签名。每一个这样的服务也要求密钥管理或认证服务。

合适的密码防护可应对对信息机密性和完整性的威胁。像加密和鉴别这样的密码防护措施要求某种材料，如密码密钥，来保持秘密。

可能需要一个或多个设备来生成、分发和解释密码材料来支持密码防护。如有可能，应使用 ISO 关于银行业密钥管理的标准。

提供密码材料管理的设备应服从最高级别的物理保护和存取控制。密钥管理应在密钥分割下完成

以保护系统安全。

可靠的密码实践和有效的灾难恢复计划可能引起目标冲突。进一步协商灾难恢复和密码支持之间的责任是必要的，可确保一个功能不危害另一功能。

应以最小化损害可能的方式为客户提供密码材料。客户应知道密码材料安全措施的重要性。客户、商务合作者或服务提供商的密码系统之间的互操作必须在完整的书面文档保证下进行。

密码产品提供的安全性质量依赖于这些产品的持续的完整性。硬件和软件密码产品需要与它们要提供的安全级别相一致的完整性保护。使用合适的已认证的抗攻击和密钥归零集成电路，使得硬件系统比软件系统在某种程度上容易提供保护。如果环境允许，也可使用软件密码产品。应采用增强系统完整性的方法，例如自测试，来达到最大程度的可行性。

密码产品要服从政府关于使用、进口和出口法规的变化。各地关于密码设备使用、制造、销售和进出口的法规差异很大。应向当地律师和授权机构咨询。

12.7 密钥管理

任何技术，都有相对容易执行和维护的部分以及需要尽最大努力才能完成的部分。密码密钥管理就是需要仔细计划、培训和执行的技术。描述密钥管理的标准包括 ISO 11568。

密钥管理是密码技术的一部分，它提供安全生成、交换、使用、存储和废止密码机制中使用的密钥的方法。在计算机系统和网络中，将多种密码技术，如加密和鉴别相结合可实现很多安全目标。然而，如果没有密码密钥的安全管理，这些技术是没什么价值的。

密钥管理的主要功能是通过密码技术，提供所要求的密钥并且保护这些密钥免于任何形式的泄露。密钥管理的特殊的流程和安全要求依赖于基于密码技术的密码系统的类型，密码技术本身的属性，以及受保护计算机系统或网络的特性和安全要求。

最重要的是在计算机系统或网络内，为了应用的高效率，密钥管理应有足够的灵活性，但仍应维持系统的安全要求。

密钥管理服务应随时随地提供，包括在备份地点。密钥管理应作为机构灾难恢复计划的一部分。

12.8 隐私

金融机构拥有很多个人和机构的敏感信息。法律和制度要求在某种安全和隐私规则下处理和保留这些信息。某些技术和业务的发展，例如网络、文档镜像、目标市场和跨部门信息共享，导致必须充分考虑银行隐私保护。

金融机构应审查所有的隐私法律和制度，例如那些涉及信用信息方面的。应对目前出现的国内隐私法律保持关注，它们或由银行法律办公室，银行业界发起者提出，或由独立信息发起者提出。另外，从事国际业务的银行需要知道区域的、国际的或其他方面的适用的隐私法律制度。

金融机构应审查其操作来判断客户和雇员的信息是否得到足够的保护。在关于如何收集，使用，保护信息方面应给出专门的策略和规程。这些策略和规程应为相关雇员所了解。隐私策略和过程应说明：

——收集信息时应确保只收集与识别业务需求有关的，精确的信息；

——处理信息以提供合适的访问限制，包括决定谁能访问信息，进行质量控制以避免数据输入或处理的错误，防止不经意的未授权访问；

——共享信息，仅能以事先定义好的方式存在。信息以最初收集时的原因为使用目的。这种共享不能导致产生其他未经授权的隐私入侵的新机会；

——存储信息确保以受保护方式存在以避免未授权访问；

——发布信息使用和有效的程序，允许信息拥有人纠正信息错误，建立使用信息的标准；

——当不再需要时安全地销毁信息。

另外，对雇员的电子或其他形式的监控应符合各类不同的法律要求。在考虑雇主权利的同时，雇员隐私保护和处置权同样应得到考虑。

金融机构可考虑进行隐私审计。这种审计可评估机构隐私保护的执行情况和IT处理隐私问题的方式。

13 后续防护措施

13.1 维护

防护措施维护，包括这些防护措施的管理，是金融机构安全方案的重要组成部分。确保如下要求是所有级别管理者的责任：

——清晰地建立维护防护措施的责任；

——机构资源分配给防护措施的维护；

——防护措施周期性审查和重新验证以确保按计划持续执行；

——IT系统软/硬件的修改和升级不能使计划好的现存防护措施的性能发生改变或无效；

——技术的升级不能引入新的威胁和脆弱性；

——当发现新需求时，升级防护措施和/或加入新的防护措施；

——防护措施有任何变更时，审查、改进安全策略或增加新安全策略；

当完成上述维护活动时，应避免带来不利的或高成本的影响。

13.2 安全符合性

安全符合性检查，也称为安全审计或安全审查，是一项非常重要的活动。符合性检查用于确保遵守和符合IT系统安全计划，以及确保IT项目或系统在整个运行生命周期中能够有效保持一个适当的信息安全级别。这包括设计、开发和实施阶段，也包括应用升级，改进或修订。当重新布置或处理系统组件时也应保持小心。

执行安全符合性检查可使用外部或内部人员（例如审计师），并且通常依据与IT项目或系统安全策略有关的列表的使用。安全符合性检查应整合在IT项目或系统计划中。

另外，抽查技术对判断运营支持员工和用户是否遵守专门的防护措施和规程尤其有帮助。所做的检查应确保正确的安全防护措施被执行、使用，以及在合适的地方通过测试而恰当地验证。在发现防护措施不符合系统安全计划的地方，应建议区域经理，产生、实施和试验正确的行动计划并检查结果。

13.3 监控

监控是信息安全计划的重要的组成部分。监控可给管理者已实施的防护措施的指示，包括这些防护措施是否满足相关要求以及是否实施了防护措施维护方案。初始的安全计划可和监控的结果相比较以判断哪些防护措施起作用了，哪些没起作用。

很多防护措施生成安全相关事件的输出日志。这些日志应定期审查，如有可能，应使用统计技术分析以进行趋势变更的早期检测和重现不利事件的检测。资产、威胁、脆弱性和潜在的防护措施的所有变更对风险有重大的影响，及早检测出，就可以及早采取预防行动。仅从日志中分析过去事件会忽略日志的其他重要防护机能。

监控也应包括向相关信息安全官汇报的规程和一般基础上的管理。

14 事故处置

14.1 管理事件

安全事件是在信息系统或通信系统中已确定发生的情况，表明安全策略可能被破坏或保护资产的

防护措施的失败。任何事先未知或意外的情况可能有安全相关问题，应作为安全事件对待。一个安全事故是一系列一个或更多未知或意外的安全事件，对信息有重大的潜在威胁，对业务运营有伤害。安全事件的发生是不可避免的。应调查每个安全事件，判断是否是安全事故。调查应深度衡量事件的危害程度，或事件导致的潜在危害程度。

事故处置提供了对无意或有意破坏正常 IT 系统运营的行为的反应能力。应开发适合整个机构的 IT 系统和服务的事故报告和调查计划。这个计划包括报告 IT 和业务一线员工使其获得目前信息安全事故和相关威胁以及它们对 IT 资产和业务运营相关影响的一个泛围很广的见解。关于事故处置和管理事件的其他信息可在 ISO/IEC TR 18044[9] 中找到。

信息安全事故调查的基本目标是以敏感和有效的方式对事故作出反应并且从事故中获取教训，避免未来相似的不利事件。在某些情况下这些是必须的，对机构名誉采取特别防护措施，避免恶意通告不利的公开批评以保护安全事故相关信息的机密性。

事先准备好的带有已定义的决策的行动计划允许机构在合理的反应时间里限制进一步的损害，通过辅助方法继续业务。一个事故处理计划应包括按年代顺序文档化的所有事件和行动。这应导致事故来源的识别。这是达到第二个目标的前提，即通过改进防护措施来减少未来的风险。

完成事故分析并文档化是重要的，提出以下问题。

——事件和行动按年代顺序正确文档化了吗？

——按计划执行了吗？

——相关员工可得到所要求的信息吗？

——要求的信息能及时获得吗？

——下次员工建议所做有何不同？

——事故分析处理功能(检测/反应/报告)效率高吗？它能改进吗？

——有控制措施以防止安全事件再次发生吗？

回答这些问题并找出解决办法可减少未来事故的影响。

14.2 调查和取证

一些事故要求额外的调查。悬而未决的欺诈行为、不满意的雇员和一些法律问题要求能够在 IT 系统中进行调查。需要收集和分析系统日志、IDS 日志、有时还包括整个磁盘以支持一个调查。可能需要磁盘中数据的法律分析，包括寻找删除的文件，以及其他类型的详细分析。多数机构仅拥有有限的内部能力执行这些调查和分析。然而，所有安全方案应包括一些证据处理方面最小的训练和计划，包括谁将执行这些调查，他们如何开展工作以及他们能执行哪些类型的法律分析等等方面。不同机构和不同事故的实际需要有很大的不同。

14.3 事故处置

参加事故处置的所有人员应熟悉事故处置计划。计划应考虑很多潜在的问题：正常规定时间之外的事故，交流需要(包括机构内的交流以及与媒体和客户的交流)，备份和应急计划，与供货商和支持商(包括业务伙伴)的沟通。

14.4 突发事件问题

为保持突发事件期间的完整性，不应省略安全过程。仅局限于解决突发事件中产品问题的特定过程应就位并且恢复正常的变更规程应尽快制定。在任何变更中，所有变更内容，包括突发事件支持人员的变更，必须以书面方式记录。最后，应审查所有突发事件变更。

附 录 A
（资料性附录）
示 例 文 档

A.1 董事会关于信息安全的决议

决议：

信息是公司的资产。

作为一项资产，公司的信息和信息处理资源应加以保护，防止未授权或不恰当使用。

首席执行官指导建立信息安全方案，方案应与审慎业务实践保持一致，目标是恰当地保护公司信息资产。

A.2 信息安全策略

ABC 金融机构信息安全策略

ABC 金融机构认为所有形式的信息均为公司的资产，需要采取适当的控制措施保护这些资产，以防止未授权或者不正确使用。信息对公司高效的日常运作是至关重要的。该信息只能用于其希望的目的——ABC 金融机构业务行为。我们公司的策略是：只在已证实为“业务需要”的基础上才提供信息的访问，其他情况一概拒绝访问。

ABC 金融机构的每位业务部门高级管理者负责维护其信息资产的机密性、完整性和可用性，他们必须遵守所有由信息安全部门公布的有关公司的信息资产保护的策略、标准和规程。

所有雇员有责任了解、支持和遵守所有有关信息资产保护的公司策略、标准和规程。

A.3 雇员认知表格

公司认为信息是应保护的资产。

我有责任了解、支持和遵守所有有关信息资产保护的公司策略、标准和规程。

我已经获得一份公司信息安全手册，同意遵守其中的条款。

我同意仅出于履行本人工作职责的目的，使用我有权访问的公司信息和信息处理设备。

我理解，公司可审查我使用公司的信息处理资源产生的任何信息或消息。这包括但不限于文字处理设备、e-mail 系统和个人计算机。

我同意对可能危害公司信息资产的可疑行为和情形及时向我的主管汇报。

我理解滥用公司信息资产可导致对本人的纪律处分。

日期_____

打印的雇员姓名_____签名_____

证明人（或者主管）_____

A.4 登录告警屏幕

这是一个仅向合法授权人开放的私人计算机系统。授权人仅限于执行为完成相关职责所分配的职能。任何未授权访问将被调查，并在法律范围内进行起诉。如果你不是授权用户，请立刻切断连接。

或者：

该计算机系统仅向授权用户开放。任何未授权访问和尝试将被调查。如未经授权，请立刻切断连接。

A.5 传真警告

支付警告

警告

在没有授权机构的确认的情况下，不要依赖本传输付款或者发起其他交易。

所有者声明

本传真文档包含了ABC公司的机密信息或者特别信息。该信息用于本传真件上所列出的收件人。如果你并非收件人，请注意：禁止对本传真信息的任何泄露、复印、分发或者使用。如果你已经错误地收到了本传真，请立即电话告知发送者，以便我们能够取回这些文档，费用无须您支付。

A.6 信息安全公告

计算机病毒警告

根据国家报告，名为“The Michelangelo Virus”的计算机病毒已经在整个世界迅速传播开来，可能成为近年来最具破坏性的病毒。该病毒感染基于版本为2.XX或以上的DOS的系统中。

影响

该病毒于3月6日(Michelangelo的生日)爆发。在该日，病毒将覆盖关键的系统数据，致使系统不可用。感染的数据包括启动盘(无论软盘或者硬盘)上的启动记录和文件分配表(FAT)。

从已经损坏的盘中恢复用户数据将非常困难。

症状

已知症状包括以下两个方面：

可用/总共内存减少2 048字节；

软盘在DIR(目录)命令下变得不可用，或者以乱码字符显示。

特别注意：Michelangelo病毒不会在任何时间在PC屏幕上显示任何消息。

感染风险

病毒通过以下方式之一传播：

- 从已经感染的软盘启动(即使该启动并未成功)；
- 从硬盘启动，但是在A驱动器中已经放入感染过的磁盘，并且驱动器门已经关闭。

同时用于商业和家庭的磁盘可能比通常的磁盘具有更高的风险。

A.7 风险接受表

信息安全风险接受

本表格宜仅在业务过程或系统不符合信息安全策略、信息安全标准以及对将来可预见的问题没有计划可参照执行时填写。

公司_____请求单位代码_____

单位管理人_____请求单位名称_____

策略/标准的页码和条款编号_____日期_____

请求的风险接受(描述)_____

业务过程描述(可附加相关文档)

期间交易总数

期间交易总额

交易是否限时?(描述)

是否影响通用分类账户?

接收输出的管理级别

输出决议的关键程度

规定/法律上的考虑

输出分发给客户了么?(描述)

所处理的信息的最高级别

用于支持业务过程的系统的描述(可附加相关文档)

设备型号的描述(计算机编号、样式等)

网络连接的描述(LAN、VATM、拨号等)

处理地点

用户数

用户地理位置

与其他系统的接口的描述

可用性要求

其他的应用是否运行在本设备上?(描述)

系统是否由中央系统群提供支持?如果不是,描述支持安排

描述业务/系统对策略适用的要求

遵守策略的估计费用

描述现在或建议的降低风险的控制措施

现在或建议的降低风险的控制措施的估计费用

本决定所考虑的其他因素(其他可选的、附加的业务因素、其他公司的行动等)

推荐:(部门经理)日期:

审阅:(信息安全官)日期:

意见:

批准:(高级官员分配)日期:

风险接受编码(授权高级官员)

下次审查日期

信息安全级别

A.8 远程办公协议和工作分配

雇主-雇员远程办公协议

本协议在_____(以下称“雇员”)和_____(以下称“公司”)中有效。在法律的范围内,达成协议如下:

协议范围

雇员同意作为远程办公者为公司提供服务。雇员同意远程办公是自愿的,并且公司可在任何时候终止该远程办公,无论是否有原因。

除了本协议中明确的雇员的职责和义务,公司和雇员在雇用过程中雇员的职责、义务、责任和条件保持不变。

术语“远程办公地点”或者“远程办公室”指由雇员管理层批准的雇员居住点或者任何远程办公室地点。

协议条款

本协议应自雇员、雇主签署协议日期的较后者起生效,并在雇员远程办公中保持有效,除非终止。

协议终止

雇员作为远程办公者参与工作完全是自愿的,且仅适用于根据公司判断认为合格的雇员。员工不拥有进行远程办公的权利。然而,当雇员自愿且被挑选去远程办公,雇员将许诺远程办公不低于X月的周期。由于远程办公者工作的中断所造成的费用、危害或损失公司概不负责。本文本并非雇佣协议,不可作为雇佣协议进行解释。

补偿

工作时间、加班、轮班、假期:雇员同意工作时间、加班费、轮班和职位安排将遵守雇员和公司所达成的条款。

远程办公和附带设备

雇员同意由公司在远程办公地点提供的设备、软件、资料供应、器具等,仅限于授权人员用于业务目的,包括自我发展、培训和工作任务。远程通信设备仅供雇员业务使用。公司将不对雇员在进行私人业务期间所发生的远程通信费用负责。

公司可根据其自身判断,选择购买雇员远程办公使用的设备和相关供应品,或者允许雇员使用其自有设备。有关硬件(包括但不限于电脑、传真机、视频显示终端、打印机、调制解调器、数据处理器和其他终端设备)、计算机软件、数据和远程办公设备(即电话线)等的型号、特性、功能和/或质量完全由公司决定。

以上设备、数据和/或软件的移除或废止完全取决于公司的决定。购买的供雇员使用的设备应作为公司的财产。公司不承担雇员自有设备的丢失、损害或磨损等的责任。

雇员同意,工作期间,在远程办公地点应指定一工作区放置和安装所使用的设备。雇员应保持工作区的安全,以使雇员和设备远离危险。选择作为雇员远程办公区的地点必须经公司批准。如果公司的远程办公设备的初始安装和设置发生变更,由雇员负责其费用。

雇员同意,公司可到远程办公地点确定该地点是否安全且远离危险,或现场维护、维修、检测、重新索回公司拥有的设备、软件、数据和/或供应品。在发生意外时,有必要采取法律行动重新拥有公司所有的设备、软件、数据和/或供应品。如果公司获胜,雇员同意支付公司承担的所有费用,包括律师费用。

碰到设备失效或者故障,为了对该设备进行立即维修或者替换,雇员同意立即通知公司。遇到维修或者替换的拖延,或者其他雇员不可能远程办公的情况,雇员同意其被分配从事其他的工作,或者被分配到其他地点,具体安排完全由公司决定。

公司拥有的设备、软件、供应品以及家具、照明设备、环境保护和其他家用安全设备应按其预定用途

使用，且应在安全条件下使用和维护，避免故障和毁坏。

雇员同意，公司拥有的数据、软件、设备、设施和供应品应予以适当保护，并不能用于创建私人软件或数据。雇员应遵守公司所有关于利益冲突和机密性的策略和指南。工作相关活动所产生的任何软件、产品或者数据由公司所有，且必须以核准的形式和媒介生成。雇员同意，一旦雇佣关系结束，雇员将向公司归还所有属于公司的物品。

伤害责任

雇员理解，雇员对由于其自身造成的对第三人和/或雇员家人的伤害负责。雇员同意，在雇员提供的服务或者雇员在实施本协议的职责和义务中，由于其有意的误操作、粗心行为或者遗漏，无论直接或者间接导致的，将维护、赔偿和维持公司、其分支机构、雇员们、订约人、代理商，使之免于由于人员伤害（包括死亡）和财产损失所带来的所有控诉、索赔、或责任（包括任何相关损失、成本、费用合代理费），完全由公司的疏忽、有意误操作所导致的控诉、索赔或责任情况除外。

其他情况

雇员同意参与公司所有的，与远程办公相关的研究、调查、报告和分析，包括调查雇员可能认为的私人或者属于特权的方面。公司同意，如果雇员要求，雇员的个人答复应保持匿名，但是该数据可编辑并无需雇员的确认即可提供给公众。

雇员必须遵守公司所有的规章、政策、实践、指令和本协议，且明白，违背这些将导致失去远程办公和/或纪律处分，直至解除雇佣关系。

通过以下签名，确认我已经阅读过本协议，并且理解其含义。我确认我已有机会让我的法律顾问进行全面审查。

雇员签名：_____

日期：_____

当远程办公（或者说在另外一个地点工作，例如家里）对双方都有好处的时候，可以选择安排某些雇员进行远程办公。

远程办公不是一项雇员福利，而是满足公司需要的一种可选方式。雇员没有权利一定要去远程办公，公司可在任何时候中断该安排。

以下是远程办公者和其主管协商同意的远程办公条款：

1) 雇员同意在以下地点工作：_____；
2) 雇员将每个星期远程办公__天；
3) 雇员工作时间如下所示：_____；
4) 以下为雇员在预定交付日期，在远程地点进行工作的安排：_____；
5) 雇员将在远程办公地点使用以下设备：_____；
6) 以下为在远程办公地点的远程办公者，由于公司业务原因需要进行电话通信的协议条款：_____；
7) 雇员同意从_____获得所有在远程办公地点工作所需要的供应品；如果购买了公司办公室日常可以提供的供应品，这些支出通常不能报销；
8) 雇员将被要求经常性定期前往_____中心参加培训和团队/主管会议。

我已经在他/她参与公司远程办公计划之前，通读以上条款。

日期：_____

主管签名：_____

以上材料已经与我商榷。

日期：_____

雇员签名：_____

附 录 B
（资料性附录）
Web服务安全分析示例

B.1 高级别安全分析

B.1.1 概述

策略可以非常详细也可非常简略，与之相似，风险分析也有不同的详细程度。本条对 Web 服务进行高级别讨论，Web 服务是一种新兴技术，对于许多金融服务公司和其他使用互联网完成业务的公司非常重要。本示例分析仅仅是个例子，不宜被认为是特定的安全建议。如同本文档中所标明的一样，每个机构必须基于其特定策略和业务需要，作出其自身的安全和风险决定。

Web 服务(WS)是一个业界的通用词汇，指一系列新出现的基于可扩展标志语言(XML)的标准，这些标准允许计算机在互联网上交换数据，进行业务和交易。核心的 WS 功能允许生成可被其他计算机(而非人眼通过浏览器)访问的信息服务。Web 服务处理系统间、业务单元间和公司间互操作的能力很强。

Web 服务主要的组件包括：

——装载服务的应用服务器(即服务软件代码运行的场所)；

——服务的接口(通常被描述为 Web 服务描述语言，WSDL)；

——用 WSDL 接口描述的数据存储或目录，这样 WS 客户端可以找到(并使用)接口；

——要使用 Web 服务的 WS 客户端；

——允许 WS 客户端与服务对话的通信协议(简单对象访问协议，SOAP)。

Web 服务有许多定义，但是被广泛认可的定义是通过 W3C 标准简单对象访问协议(SOAP)披露信息的信息服务。SOAP 的客户端接口必须知道如何访问这些信息服务。这些访问可以用另一个 W3C 标准，Web 服务描述语言(WSDL)描述。基于 SOAP 服务的创建者发布了 WSDL 文件。

B.1.2 Web 服务安全

Web 服务安全应处理维护服务、服务描述、服务库、使用服务的客户端和通信协议的应用服务器。多个供应商和银行开发了 WS 安全框架和一些规范。另外，无处不在的 web 安全解决方案 SSL 可为 Web 服务提供一些安全。其他的 Web 服务安全详情将在本章讨论。

B.1.3 安全标准

SOAP 和 WSDL 是报文和服务的定义，对每个使用它们的业务服务，它们必须分别地被保护。然而，当前它们没有规定为 Web 服务应用提供数据完整性、源鉴别或机密性服务的完整方法。预期将有新的要求，SOAP 具有扩展框架，允许在标准化方法中加入安全要素和协议。本条给出了一些关于 Web 服务的标准的概述。

安全声明标记语言(SAML)规定了可交换安全信息的基于 XML 的框架，可解释为某个安全域内具有一个标识的实体的声明。这些声明通过 SAML 请求和响应报文传送。交换的安全信息以 SAML 声明的形式传送，这些声明可传送关于先前鉴别事件、人或计算机主体的属性和授权决定(允许或不允许主体对资源的访问)的详情。业界注视 SAML 的发展，业界希望它成为传送基于 SOAP 的 Web 服务的登录信息的标准方法。SAML 现在具有用于 SOAP 的绑定的描述。

Web 服务安全(WS-Seurity)是 SOAP 的建议扩展集,它可使 Web 服务交易具有完整性和机密性。WS-Security 试图通过安全令牌传播、报文完整性和报文机密性提供完整性和机密性。Microsoft 和 IBM 建议的 WS-Security 和职责已提交 OASIS(Organization for the Advancement of Structured Information Standards)。

XML 加密是一个 W3C 规范,规定如何通过标准化加密方式传送 XML 信息。XML 加密允许对数字化内容进行加密和解密,这些内容包括在元素级别而非属性级别的 XML 文档中。该规范也允许对 XML 文档接收者用于解密内容的密钥信息进行安全传输。

XML 签名是一个 IETF 和 W3C 联合工作组的建议草案,该工作组致力于如何在 XML 文档中描述数字签名信息。对任何类型的数据,无论是否驻留在包括签名的 XML 中,"XML"签名提供了完整性、报文鉴别和/或签名人鉴别服务。"XML"签名是为其他安全标准(包括 XML 加密、SAML 和 WS-Security 在内)所引用的基础标准。

"自由联盟计划"是一个行业社团,由主要的业界机构领导,这些业界机构愿意共同使用开放的、统一的身份识别技术。统一的身份识别可以使消费者在多个机构中使用单一的、经过验证的身份。该消费者可以在一群机构中,采用同样的可信的身份信息,而不必提交新的身份、所有者身份证明。

XML 密钥管理(XKMS)是一个 W3C 规范,用于描述和注册可与 XML 签名和 XML 加密规范一起使用的公钥。XKMS 目前的版本号是 2。密钥管理工具包可以从许多供货商处得到。

B.2 Web 服务标准

B.2.1 概述

Web 服务标准正在迅速发展。为实现基本 SOAP 交易标准,需要补充三个关键领域的工作:服务发现、安全和业务过程。关键的服务发现标准是 UDDI,该标准描述 WSDL 文件的中央库(公有或私有设置)如何允许用户发现和调用服务。一大批安全标准正在用于在用户和报文级别上提供真实性、加密、签名和声明服务。业务过程标准主要致力于回答:"我如何把许多服务聚合起来,生成一个完全有用的过程,而非一个单个的功能。"

B.2.2 实现

一般来说,实现 Web 服务至少需要考虑 Web 服务面临哪些风险或威胁、降低安全威胁所采取的措施等方面的内容。对于这个分析,参见图 B.1,图中相对简单的 Web 服务(WS1)用于处理整个机构的网络中的其他位置的客户。在本图中,四个客户可能向 WS1 请求服务。注意这些客户从他们自身来说可能也是 Web 服务,从而为一个客户提供功能的 Web 服务本身可能扮演一个为完成其自身功能而向其他服务请求服务的客户。例如,为了提供一个月度付款计算服务,一个提供抵押计算的 Web 服务可能依赖于一个费率确定 Web 服务。

客户 S2 配置在一个相邻的网络,可能与 WS1 在同一个数据中心。客户 S3 也在公司的内部网络中,但可能相隔非常远,可能在另一个州或国家。客户 S4 在一个与互联网相连的非军事区(DMZ)中,与互联网和公司内部网络都有某种程度的连接。内部服务(如 WS1)可能对于在互联网上的客户(如 S5)是可用的。

B.2.3 安全

针对一般威胁,WS1 的安全要求可概括为几类。首先,请求服务的输入数据要求机密性,返回客户的输出数据也要求机密性。机密数据的完整性也是一个隐含的要求。第二,为确认客户身份,防止未授权客户使用服务,需要身份鉴别和客户请求的授权。最后,常常有一些登录请求,允许重构交易和、跟踪动作。对于某些 Web 服务,可能只需要数据完整性要求而无需机密性要求。

当直接要求 WS1 的安全时，考虑构建一个解决方案可能是复杂的。例如，在 WS 客户端和 WS 服务器间的安全鉴别可使用口令、证书或其他可能的方法。证书可提供极高的安全性，但是考虑性能、负载均衡、失效等，实现证书可能会遇到问题。口令在某些环境下安全性较低，但在某些情形下已经足够。例如，对于一个与同一硬件上运行的 WS 对话的 WS 客户，需通过机器的内存的口令提供足够的安全性。如果 WS 客户位于与服务不同的机器上，则可能需要加密口令。口令可在应用级别上用 WS-Security 标准加密，或在传输层用 SSL 加密，或在网络层用 IPSEC(IP 安全协议)加密。在应用层、传输层或网络层可能同样要求输入和输出数据的机密性。

注意身份鉴别要求特别是针对客户(也是软件)的，而非最终用户。Web 服务可以假定客户已鉴别了最终用户的身份，或者 Web 服务可通过 Web 服务请求鉴别最终用户。

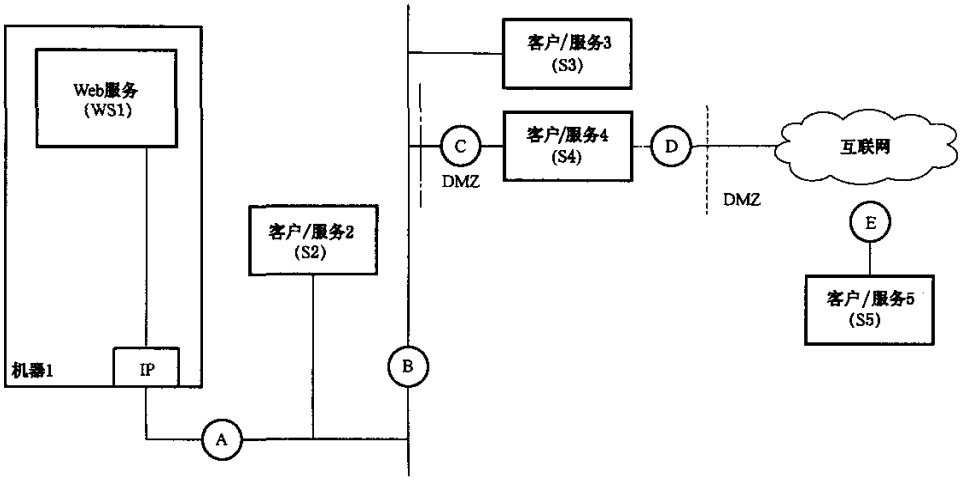


图 B.1 Web 服务通用模型

B.2.4 威胁分析

对 WS1 的威胁包括滥用服务、拒绝服务和未授权使用服务。在多数情况下，滥用服务宜被服务本身阻止。WS1 宜检查所有输入和输出的有效性，当 I/O 落在预期范围之外时，WS1 生成错误报文。拒绝服务能通过在不同机器上生成服务的多个实例，通过在实例间的负载均衡请求，通过其他广为人知的确保 IT 服务可用性的方法处理。未授权使用可通过安全鉴别客户请求的服务来阻止。某个 Web 服务可能不需要鉴别客户请求，也可能需要很严格地鉴别客户请求，取决于 WS 的属性。请求在账户间转移资金的 WS 宜非常安全；否则会引起欺诈客户请求转移钱的服务。基于输入贷款值和抵押费率的计算贷款支付的 WS 不需要安全性，因为这仅仅是个计算。

B.2.5 解决方案

根据客户请求服务的不同，WS1 安全要求的解决方案可能不同。考虑如果 WS1 仅仅支持如 S2 那样物理上距离 WS1 很近的客户。在这些情况下，在 S2 上，客户和服务距离很近，可通过路由表、虚拟 LAN、网段间的内部防火墙或其他技术来降低未授权服务请求的机会。假定 WS1 和 S2 与外界的通信被适当地保护，由于它们与外部世界隔离，有理由相信，可以很容易地实现数据机密性和口令验证。

当我们移动到远离 WS1 时，复杂性就增加了。在客户 S3 和 WS1 之间，服务请求沿着一个更大的网络传送，这就为网络嗅探开放了更多的机会，使得可能在更多的地点产生和注入未授权请求。因此，需要在 WS1 和 S3 之间增加安全措施。如前所述，这可能是基于证书的鉴别，也可能是 S3 硬件和 WS1 硬件间的 IPSEC 协议。

对于客户 S4，机构的 DMZ 的位置涉及更多的安全考量。非军事区用于把互联网和内网的连接分隔开来。DMZ 内的系统面临更大的风险，因此可能需要增加安全措施。对于 S4，应用层和传输层或网络层的结合是满足机构的安全策略的恰当的途径。

最后，对于机构外部的 S5 的 Web 服务请求，这个进入的请求将可能需要一个复杂的解决方案。鉴别信息可能在应用层被保护，安全地穿过互联网，通过 DMZ，进入 WS1，因此 WS1 可决定是否向 S5 授权请求服务。同样地，请求的输入数据可在应用层加密，但应用层数据加密可能在 DMZ 中终止（或解密）、校验以确保数据具有合适的参数，可向 WS1 传输时重新加密，以使其可在 WS1 解密。类似地，在可重新生成对 WS1 的请求（可能以不同形式）的 DMZ 中，完整的 WS 请求可能在传输层或网络层进行额外的加密，然后传输给位于 DMZ 的中间服务（可能是 S4），在该 DMZ 中可重新生成对 WS1 的请求（可能以不同形式），这样，WS1 的接口就决不会暴露给机构之外。

概括一下，WS-Security 包括有许多可能的鉴别机制的组合，针对身份验证和机密性，有满足不同需求的口令加密和数据加密。在典型的机构的网络中有许多可能使用 Web 服务的位置。威胁和需要的对策依赖于 WS 客户、WS 服务器的位置，以及这两个系统之间的网络路径。

还有许多其他因素应被考虑。客户和服务器之间的性能常常非常关键。对失效切换、备份、恢复和类似的偶然事件的关心使得一些对策变得更有吸引力。不同公司的 WS 开发工具为 SSL 和 WS-Security 标准提供不同种类的支持；你的工具可能不支持基于证书的 SSL 会话重用。由于应用服务器可能具有和标准工具相关的不同能力，结果可能不同。

附 录 C
（资料性附录）
风险评估说明

C.1 风险评估矩阵表

表 C.1 为风险评估矩阵表。

表 C.1 风险评估矩阵表

脆弱性区域：人员 确认以下威胁产生的风险的级别	资金损失风险			生产率损失风险			名誉风险		
信息的未授权泄漏、篡改或者破坏	H	M	L	H	M	L	H	M	L
信息的无意修改或破坏	H	M	L	H	M	L	H	M	L
信息的未能传递或错误传递	H	M	L	H	M	L	H	M	L
服务的拒绝或降级	H	M	L	H	M	L	H	M	L
脆弱性区域：设施和设备 确认以下威胁产生的风险的级别	资金损失风险			生产率损失风险			名誉风险		
信息的未授权泄漏、篡改或者破坏	H	M	L	H	M	L	H	M	L
信息的无意修改或破坏	H	M	L	H	M	L	H	M	L
信息的未能传递或错误传递	H	M	L	H	M	L	H	M	L
服务的拒绝或降级	H	M	L	H	M	L	H	M	L
脆弱性区域：应用 确认以下威胁产生的风险的级别	资金损失风险			生产率损失风险			名誉风险		
信息的未授权泄漏、篡改或者破坏	H	M	L	H	M	L	H	M	L
信息的无意修改或破坏	H	M	L	H	M	L	H	M	L
信息的未能传递或错误传递	H	M	L	H	M	L	H	M	L
服务的拒绝或降级	H	M	L	H	M	L	H	M	L
脆弱性区域：通信 确认以下威胁产生的风险的级别	资金损失风险			生产率损失风险			名誉风险		
信息的未授权泄漏、篡改或者破坏	H	M	L	H	M	L	H	M	L
信息的无意修改或破坏	H	M	L	H	M	L	H	M	L
信息的未能传递或错误传递	H	M	L	H	M	L	H	M	L
服务的拒绝或降级	H	M	L	H	M	L	H	M	L
脆弱性区域：环境软件和操作系统 确认以下威胁产生的风险的级别	资金损失风险			生产率损失风险			名誉风险		
信息的未授权泄漏、篡改或者破坏	H	M	L	H	M	L	H	M	L
信息的无意修改或破坏	H	M	L	H	M	L	H	M	L
信息的未能传递或错误传递	H	M	L	H	M	L	H	M	L
服务的拒绝或降级	H	M	L	H	M	L	H	M	L

C.2 风险评估描述

C.2.1 脆弱性区域

风险评估矩阵是一个一页的表格，用来帮助评估业务功能风险。它可分为5个脆弱性区域：

1) 人员；
2) 设施和设备；
3) 应用；
4) 通信；
5) 环境软件和操作系统。

C.2.2 潜在威胁

风险矩阵表格中的每个脆弱性区域中，4个要被评估的潜在威胁如下所示：

1) 未授权的信息泄漏、修改或破坏；
2) 信息的无意修改或破坏；
3) 不传递或错误传递信息；
4) 服务拒绝或降级。

C.2.3 风险级别和类别

在每个威胁的右边是三个风险类别：资金损失、生产率损失和名誉损失的风险级别。信息安全策略、程序和过程是机构用来评估和降低业务风险的风险管理工具。服务、信息系统或产品递送方面的问题可导致收入或资产的资金损失风险。风险级别是内部控制、信息系统、雇员诚实和操作过程的函数。

由于公众的负面看法导致的收入、资产和商业名誉的风险可对金融机构创建新的关系、服务或维持现存的关系、服务的能力产生影响。风险可能导致机构面临起诉、财务损失或对其声誉的进一步损失。由于侵犯或不遵守法律、规章、规定、预先的惯例或伦理标准所造成的更大风险可能使金融机构面临罚款、民事财务赔偿、损失补偿和合同失效。

本导则中使用的风险级别是：

——高(H)：由于相应的脆弱性造成的威胁而产生的巨大的资金损失、生产率损失或名誉损失；

——中(M)：少量资金损失、生产率损失或名誉损失；

——低(L)：最小的资金损失、生产率损失或名誉损失或没有损失。

C.2.4 风险评估说明

在五类脆弱性中按照不同业务功能，矩阵在最后一列以风险级别高(H)、中(M)或低(L)表示威胁的影响。要评估企业的风险，需要

——对于要评估的业务功能，分析矩阵中每个潜在威胁的意义；

——询问谁、如何面临风险，每个脆弱性中发生的潜在威胁导致何种级别的风险。

没有决定风险级别的绝对标准。在作出决定时，确定货币变化范围、员工工作时间范围和最坏情形的事件是有益的。当怀疑所分析的潜在的威胁时，假定最坏的情形将发生并选择最高风险级别。

当完成风险评估矩阵时，关键的假设应是不存在保护措施。

作为一个例子，矩阵中“设施和设备”的第一个威胁可作如下分析：

——如果具有普通访问权限的个人泄漏了关于你的设施和设备的信息(即一个部门雇员泄漏了包含有价值或机密的信息部门的安全信息)，该机构会有资金损失、生产率损失或机构名誉损失么？

——损失级别和/或名誉损失是高、中还是低?

被识别的威胁(即一个部门雇员泄漏了包含有价值或机密信息的部门的安全信息)应该记录。对于一个通过一个脆弱性或完整的一类脆弱性的特定的威胁,“不适用”(N/A)的响应可能对某些业务功能是合适的。当这种情况发生时,应记录所作出决定的根本原因,所有文档应以一个完整的矩阵形式保留。

一旦威胁被识别,则须作出选择:假定有权人士决定接受风险或降低风险。风险可以通过以下手段降低:风险分担(保险)、使用安全控制选定风险或变更业务目标来排除威胁源头。

C.3 风险评估表

表 C.2 为风险类别表。对于每个风险类别,填入与每个脆弱性相关的风险级别,高(H)、中(M)或低(L)。对每类风险作出评估后,要给出该脆弱性的整体风险。当该表完成时,选择合适的控制措施。

对每个风险类别,填入与每个脆弱性相关的风险级别。风险级别宜分级为高、中或者低。在对风险种类分级之后,为每个脆弱性指定一个整体风险。

表 C.2 风险类别表

	风险种类			
脆弱性	资金损失	生产率损失	名誉损失	整体风险
人员				
设施和设备				
应用				
通信				
环境软件和操作系统				

C.4 风险评估表描述

C.4.1 概述

风险评估表用于展示每个脆弱性的综合风险级别。三个风险类别列在表格的顶端和左面脆弱性的五个区域之间。

通过给定五个脆弱性区域中每个区域的综合风险级别完成风险评估表格。综合风险级别宜通过 C.2.2 中风险评估矩阵的先前识别过的四类威胁获得。

C.4.2 风险表格指导

要综合每类风险,检查风险评估矩阵上的每个脆弱性所圈定的风险级别(见 C.1)。单独考虑每个风险类别,决定四类威胁将导致何种综合风险级别(见 C.2.2)。在风险评估表写下该风险级别。

测算每个风险类别之后，要得出一个整体风险，应分析每个脆弱性的风险级别背后的根本原因，给每个脆弱性指定一个整体风险级别，为高(H)、中(M)或者低(L)。

决定每个脆弱性的综合风险级别没有绝对的规则。然而，以下内容宜加以考虑：

——威胁发生的可能性。出现可能性更高的威胁应该对给定风险级别有更重大的影响。出现可能性更低的那些威胁宜具有更轻微的影响；

——对于和正在评估的业务功能具有最大相关性的威胁，在给定风险级别时宜更加着重对待；

——评估风险级别时宜保守，存在怀疑的时候，宜选择更高的风险。

作为整体风险级别的例子，在选择整体风险级别时，信息的未能传递和错误传递可能更加被重视，因为未能传递对正在接受分析的业务功能来说，比信息的未授权泄漏更为严重。

C.4.3 控制措施选择

安全防护措施的选择可提供机构对它所接受的风险的直接控制。机构需要评估计划的和现存的保护措施怎样降低风险分析中识别出的风险，识别出可用或可开发出来的额外保护措施，开发出 IT 安全架构并确定不同种类的限制(见 9.3～9.7)。应选择适当的、经过证实的保护措施把评估的风险降低到可以接受的级别。选择保护措施的额外的详情可在 ISO/IEC 13335 中找到。

C.4.4 影响和可能性排序

数字 1～9 用于表示可能性和影响。通过为可能性大小给定一个通用的评价，并在企业风险框架(Enterprise Risk Framework)的六个主要的类别中分别定义影响，本条描述了在实践中这些数字的意义。尽管这给出了量化的指标，这些值宜被看作给出了数量级的相对顺序而非绝对值。

以下数值给出了所采用的可能性的量值：

1) 可忽略——每 1000 年左右发生 1 次；
2) 极端不可能——每 200 年发生 1 次；
3) 非常不可能——每 50 年发生 1 次；
4) 不太可能——每 20 年发生 1 次；
5) 可能——每 5 年发生 1 次；
6) 很可能——每年发生 1 次；
7) 非常可能——每季度发生 1 次；
8) 预计会发生——每月发生 1 次；
9) 确信会发生——每周发生 1 次。

可以近似地认为每一种情况的可能性是前一种情况的可能性的 4 倍。

以下表 C.3 是框架中六个主要标题中每一个对应的影响。不是所有的格都填写了，但是它给出了一个范围。一些风险评估可能需要不同的词汇，但是使用的级别宜大致类似。

表 C.3 风险评估

级别		描述	名誉	运行	安全	法律/规章	资金损失	策略
低	1	可忽略			非敏感数据的本地密码泄漏但未被使用		＜$100	
	2	非常小	在当地广播或出版物中对银行系统的负面报道	低级别的运行问题，不对客户产生影响	敏感数据的本地密码泄漏但不被使用	在法律规定的时间内没有收到规定的清算者应答	$100～$1 000	

表 C.3（续）

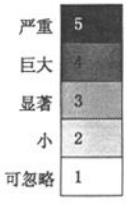
级别		描述	名誉	运行	安全	法律/规章	资金损失	策略
低	3	小	登载在国内新闻媒体或张贴在互联网上的关于银行系统的“日常性的”抱怨，例如，读者来信	对某个系统成员的服务临时失效（约1小时），对客户产生有限的影响	企图访问运行的系统；运行的信息的微小泄漏或损失	识别出可纠正的潜在的不兼容	$1 000～$5 000	策略或标准未能维护
中	4	值得注意	引起国内新闻媒体或广播的关注	对清算产生广泛影响的运行问题	合法的访问权利的滥用	不能提供法律所要求的数据，如萨班斯·奥克斯利法案	$5 000～$20 000	
	5	严重	出现在新闻媒体、广播、电视中的严厉的、批评性的文章或消息，这些文章或消息易于认为是来源可靠的	对多个系统成员的服务临时失效或对一个系统成员的服务长时间失效（最多1天），对客户产生严重的影响	对一个或多个系统成员的运行的系统的逻辑或物理渗透；例如，产生一定损害的恶意病毒	法规干涉，投诉未获支持	$2 0000～$100 000	策略或标准不存在
	6	很严重	来自监管部门或业界的公开批评	系统成员不能清算	中低额的欺诈得逞	启动警方或司法调查；司法干涉，投诉被支持	$100 000～$1 000 000	
高	7	巨大	广播和电视上的头条新闻	在一天中的关键时期（星期五下午3点以后）对多个系统成员的服务失效	高额欺诈得逞；业务数据或控制系统损坏	对清算中心的起诉（不成功）	$1 000 000～$10 000 000	管理控制损坏
	8	非常巨大	政府干预或相当的政治反应	整个工作日的无法完成清算	清算系统被攻击并严重损坏	对清算中心的起诉（成功）	$10 000 000～$100 000 000	
	9	灾难性的	新闻媒体和电视通篇报道，公众和系统成员完全丧失信任	几天或几周无法提供服务	清算中心或其密码系统完全被破坏；无法修复的高额欺诈	高管层有计划的、故意的违法	$100 000 000～$1 000 000 000	未来将对清算中心的存在产生疑问；支付行业遭到破坏

注意评估是基于“净”风险而非“总”风险。换句话说，应考虑现存的控制手段对风险的影响。通常预防性控制措施的存在将减少事件发生的可能但不影响其后果；致力于减缓影响的控制措施通常并不影响可能性。

暴露程度或“严重性”

一旦对影响和可能性“记分”，以下图 C.3 中的模型将作为定义暴露程度或“重要性”的手段。这包括五级；在实践中，任何评分为 1 的东西不值得进一步分析，任何评分为 5 的东西应立即被处置而不再进行风险评估！因此实际上我们最后只有 3 个分数。

暴露程度/重要性



影响										
	9	3	3	4	4	4	5	5	5	5
	8	3	3	3	4	4	4	5	5	5
	7	2	3	3	3	4	4	4	5	5
	6	2	2	3	3	3	4	4	4	5
	5	2	2	2	3	3	3	4	4	4
	4	1	2	2	2	3	3	3	4	4
	3	1	1	2	2	2	3	3	3	4
	2	1	1	1	2	2	2	3	3	3
	1	1	1	1	1	2	2	2	3	3
		1	2	3	4	5	6	7	8	9
		可能性								

图 C.1　可能性与影响

很明显，重要性越高，越应在分析和控制风险方面加大力度。在这一阶段，不要紧跟“打分”系统，因为“打分”系统已经完成了识别对管理所需要处置的关键的风险问题，而应该基于所有可用的信息来分析和控制风险，这些信息包括但不限于风险暴露程度（不管它们的得分）。本阶段要考虑的因素都是通常的业务管理的决策性因素：资源可用性、预算、目前的公司战略和目标，政治影响，等等。

后续措施

为了处置识别出来的风险，通常可选择四种典型的措施：

——规避：如同名称所建议的一样，这仅仅意味着移除威胁源或变更业务目标，使风险不再发生作用。尽管听起来这是一个处置风险的理想方法，但它仅适用于少数情况。“没有风险，没有业务”！例如，你可以从不离开家，避免被汽车撞倒，但是你的生活中将失去很多。再举一个和业务操作更近的例子，我们可以通过不使用第三方来避免第三方故障造成的影响——这样我们可能会丢失很多可以运作的业务！然而，当风险可以真正规避时，这通常是廉价和持久的解决方案。

——处理：处理风险往往是我们所做的最多的，在某种意义上是我们可接受的通常做法，通常称为“制定一个行动计划”。它意味着采取某种措施来降低风险的可能性，或控制事件的结果从而

降低影响的措施。这方面例子很多且显而易见——通过使用备份机制来处理数据丢失的风险，通过限制密钥生命周期等，可以控制密钥损坏的影响。

——转移：转移风险意味着让第三方承担主要影响。实现这一方法的典型手段是通过保险。不付出一些费用几乎不能实现明确的转移！例如，我们可能通过需一定费用的专业赔偿策略，把给出错误建议的责任转移出去。风险有时能通过合同安排（作为责任）分担给第三方，尽管他们处理后果的能力本身就是风险！

——接受：最后的选择就是简单的接受风险；风险可能发生，然而，可以评估可接受的代价和其他三种选择的代价，然后决定：接受风险的潜在益处超过风险的破坏程度。例如，我们可以决定接受手持轻武器的犯罪分子强行进入驻地的风险，因为物理保护措施的费用很高，而且物理保护措施会影响对客户的友好性。

当然，有可能使用混合方法处理特定的风险——这不是精确的技术——我们可能接受一定的风险，搜寻犯罪分子武装闯入的例子，通过使用非武装保护处理较小的威胁（如人们在街上随便走走），选择在关键区域加上 PIN 输入键盘或减少关键系统的功能以控制其影响，也许把一部分风险通过给我们的雇员购买人寿保险分担出去。

残余风险

要确定采取什么措施和监控活动来管理残余风险，并把所有行动的责任分派出去。

附 录 D
（资料性附录）
技 术 控 制

D.1 硬件

D.1.1 终端系统控制

如今，多数机构用一些台式机和笔记本电脑作为主要的面向用户的系统。这些终端系统使用各种操作系统，尽管其中大量的操作系统来自一个供货商。另外，这些机器的使用正在逐渐扩大，而在某些场合，更多地使用更小的个人数字助理(PDA)。蜂窝电话越来越普及，也越来越广泛地用作终端系统。文档、讲稿和表格及类似的信息的制作人员经常使用基于 PC 的解决方案。其他企业用户也经常使用基于 Web 的技术来处理应用——这样就需要授予用户使用 PDA 和蜂窝电话访问的权限。

对于任何终端系统，首先要考虑的是操作系统的安全设置。未使用和不必要的子系统，如数据库和操作系统的某些功能，应该被禁止并移除。其他功能应限于最少必要用户的正确的操作。另外，如果供货商可以为终端系统上运行的操作系统和应用程序提供系统补丁和分发更新功能，企业应有某种机制实现这些功能。例如，在 Office 套件中，已经发现一些与 Microsoft 的宏的性能有关的功能问题。

除了操作系统，企业应考虑这些终端系统的任务，以及额外的功能，如防病毒、入侵检测、入侵阻止、防火墙和虚拟专网，是否应提供给企业用户。许多情况下，机构的外围系统(如 10.5 中所指出的那样)将提供诸如防病毒、防火墙和入侵检测与阻止。然而，对于移动系统，随着企业的业务合作伙伴的扩展，在移动系统、PDA 及台式机上复制这些特性对于传统的分层防御是非常有意义的。例如，一个移动 PC 用户，位于家中，用 VPN 通过宽带连接进入企业，这样的用户可能成为一个攻击的渠道，临时的外围设备需要与其他外围设备具有同样的安全性。

D.1.2 服务器系统控制

如同终端系统一样，服务器系统需要内部操作系统的级别控制和外部应用控制。服务器常常需要一些终端系统不需要的功能和子系统。由于服务器可能会运行一个数据库、一个 Web 服务器、一个 FTP 服务和/或其他功能，这些服务器可能具有更大的潜在易受攻击点。服务器需要向其他可能不总是值得信赖的设备授权访问这些服务。另外，如同终端系统一样，当新版本和补丁发布时，必须制定测试、更新和管理系统的条款。适当的处理包括：为生产系统打补丁前，在非生产环境中测试新补丁。

内部控制方面，服务器必须充分利用操作系统的控制措施，限制服务器关键部位的功能和访问权限。例如，用于支持 Web 页面的服务器不必开通 FTP 服务，或为通用服务器队列开放端口。同样地，FTP 服务器不宜开放 HTTP 的端口和协议。

除操作系统外，还需要考虑服务器内外的防病毒、入侵检测和防火墙。这可能是把服务器放置在防火墙后的安全区内，使用基于硬件的网络入侵检测系统，或使用服务器自身所有的三层安全服务。大量的机构、网络和安全问题推动了评估和决定什么样的控制对什么样的服务器是合适的。

D.1.3 大型机系统控制

大型机系统仅由少数制造商制造，可以完成高负载处理。作为结果，大型机总是被看作比其他 IT 处理系统更安全、更强大。不过，大型机系统需要使用同其他系统一样的安全准则来管理。核心的操作系统需要保护或“加固”，在操作系统之外，还需要考虑其他的方法。典型地，大型机系统需要装载一个

机构最有价值的信息和业务规则，因此大型机系统需放置在分层网络安全体系的核心部位。每个用户被分配一个适当的、具有有限功能的ID；只有很少数的人员具有对大型机的管理控制权限。和其他系统一样，应仔细考虑职责分离，将其作为大型机安全控制的一部分。

D.1.4 其他硬件系统控制

其他硬件设备和系统会涉及类似的方面，这些应于生产系统在机构内部署前予以评估。这些设备可以是专门的加密系统(这是一个为许多防火墙和入侵检测系统提供商所推崇的新的硬件类型)，或网络硬件如路由器和交换机。在所有情况下，应了解产品所基于的操作系统，宜加固操作系统以防止简单攻击。另外，合理部署这些和内部网络连接、防病毒扫描、防火墙和入侵检测相关的设备很重要。

D.2 软件

D.2.1 Web服务器

Web服务器是非常普通和常用的软件应用，它主要用于向用户分发Web页面。其应用可以从非常简单——仅仅提供信息的封装页面，到非常复杂——多页面形式的文档，支持脚本、活动的计算机软件指令和其他。机构必须确定他们能承受何种程度的复杂性，以何种恰当的方式在互联网、Web服务器和内部数据之间建立连接。典型地，金融机构应建设一个带有防火墙的三层体系结构，在互联网和Web服务器间、在Web服务器和内部数据间都提供边界。在系统中分出应用逻辑或业务逻辑的多层体系结构，常常用于提供对数据流的严格控制。

D.2.2 应用服务器和Web服务

专门的Web服务器发展成为应用服务器——运行某个应用的功能片的服务器，这些功能片作为可由许多应用所访问的可重用组件。例如，在账户间转移金钱的功能可以作为一个应用服务器的组件运行，可以由为用户提供在线银行体验的应用所使用，也可以由为客户提供银行服务的呼叫中心接线员使用。这些应用组件功能片具有接口，这些接口允许这些应用作为服务通过Web访问。这些Web服务的行为非常像早先的远程过程调用，但是它们具有Web友好的特性，因为它们使用可用于任何设备，甚至那些不支持传统的Web浏览器的设备上的可扩展标记语言(XML)。许多供货商提供支持Web服务的应用服务器。更多关于Web服务和Web服务安全的信息可在附录B中找到。

许多供货商分发应用服务器和Web服务软件，每个版本有其自身必须被管理的重点、设置和更新。供货商和第三方常常会分发在互联网上使用的推荐安全设置。这些宜针对特定机构的策略、实践和需求考虑并评估。

D.2.3 软件应用开发过程

许多机构使用大或小的供货商提供的开发工具来定制软件，或者说生成特定的应用。这些软件开发工具很少指导操作者将信息安全整合进来考虑。因此，在软件开发过程中就考虑信息安全是很重要的。当在软件开发时就考虑信息安全要求，而不是在系统完成时增加安全软件模块，有助于安全人员维护最有效的信息安全结果。

软件开发开始前，必须告知开发公司信息安全策略、这些策略如何与开发过程关联，以及理解机构面对的威胁。宜告知他们信息安全方案和开发进行时他们在哪里可以获得指导。机构策略、实践和与信息安全官持续对话是确保软件提供有效的信息安全的坚实基础。

整合了安全要求的应用软件的开发中需要考虑两个方面。首先，软件开发过程应遵循结构化、文档化的步骤。目的是生产仅满足其自身要求的软件，不允许执行不希望的操作，无论是偶然还是恶意。要

达到这个目的，机构宜遵循 ISO 21827[13]提供的指导。其他关于软件能力成熟度模型的信息可以在 http://www.sei.cmu.edu/cmmi/上获得。带有关键安全要求的应用软件宜使用成熟度模型中级别 3 或更高级别的过程来开发，这要求用于管理和工程活动的软件过程文档化、标准化并集成到一个用于机构的标准的软件过程中。所有计划使用机构的标准软件过程的经批准的、裁剪的版本，该软件过程用于开发和维护软件。

第二个方面是确保在应用软件中整合进适当的安全要求。公司信息安全策略、安全体系结构和风险评估将产生这些要求。在开发过程中，所有的要求需要被文档化，整合和测试。安全要求也应规定：需要多大数量的证据才能表明这些要求完全满足了安全策略和任何控制规章。

因为对安全软件运行方式的了解可能对应用造成危害，文档（如测试结果和操作员指南）宜为受控文件，使之不会因不经意而被非授权人员得知。可免费得到大型开发项目问题的完整描述：NIST SP 800-64“系统开发生命周期中的安全考虑”可在 http://csrc.nist.gov/publications/nistpubs/index.html 下载。

D.2.4 安全软件获取

一个机构可以与其他机构签约，开发安全软件或带有安全考虑的应用软件。这个问题在 D.2.3 中有相关描述，但是有两点不同。第一个不同是：开发过程受纸面合同限制。要求的变更将导致合同变更，可能导致费用增加、进度拖延。第二个不同是：订立合同的人通常并不清楚机构的结构和文化。对机构的假想和误解将同样导致合同的变更。因此，在指定要求、选择开发者和执行接受度测试时，机构会非常严格。

机构可能也会购买现成的安全软件来满足安全体系结构的一些要求。必须清楚地理解软件的能力和局限。这些知识是必要的，这样可以识别剩余的要求，这些要求可被体系结构的其他元素满足。

新的软件需要与现存软件兼容，这样它就不会危害或使得现存的安全过程无效。ISO 15408[7]中定义的一套安全要求和规范：通用准则（CC）是普遍使用的安全软件基准。CC 描述了功能和保证要求；它对于审查要求和从多个来源中比对产品是非常有用的。

通用准则可免费下载，网址是：http://niap.nist.gov/cc-scheme/index.html。

D.3 网络

D.3.1 广域网

D.3.1.1 概述

广域网（WAN）系统覆盖了广阔的地区；通过通信协议，WAN 可以在一个校园内的一些建筑物内或一个建筑物内运行。互联网是由许多 WAN 构成的，每个 WAN 有其自己的路由器、交换机和与其他 WAN 相连的网关。所谓普通老式电话系统（POTS）是另一种 WAN。在所有情况中，这些网络允许数据到处流动。另外，它们提供很多信息易于受到攻击的接入点。

在机构内，尤其是地理上分散的大的机构内，机构的网络包括到更大的 WAN 如互联网的连接、校园内或一个建筑物内的几个局域网和一些把 WAN 与机构连接的专用连接。通常，这些专用的 WAN 连接被作为机构内部的连接，这些连接缺乏用于连接其他业务的或外部 WAN 如互联网的边界控制。作为常规风险评估的一部分，机构必须考虑专用的 WAN 连接可能被监控，因此具有高价值的信息应被加密。另外，对机构网络外部的用户授权的访问必须被严格控制。

D.3.1.2 有线 WAN 系统

多数 WAN 系统是有线网络，使用光纤或铜缆连接交换机和路由器。如上面所述，有线 WAN 系统

中很少考虑加密，除非是在最关键的网络链路上。多数 WAN 线缆由墙、柜橱、几乎无人能进入的窄小空间所保护。这些物理保护的形式和对连接的周期性检查，就是多数 WAN 的所有安全措施。当公司购买了专线时，可能进行一些测试，但是基于合同的对电信服务提供商的信任别无选择。有时，甚至会出现假设的有线 WAN 连接，它们实际包括微波、激光或 RF(射频)链路(包括卫星)，这些都会产生另外的机会，使得在 WAN 商监测信息流成为可能。

D.3.1.3 无线 WAN 系统

蜂窝电话网络正在迅速扩张，新的数据传输系统正在出现。尽管多数这类网络仍然相当慢(约 20kbs)，基于网络协议，未来会出现 Mb 级(兆级)的通过基于蜂窝电话网络协议的传输能力。因为这些系统具备了蜂窝电话网络的移动特性，但是又支持高带宽，它们常常被称为无线 WAN 系统。这些系统也限制了提供加密和类似的安全能力的机会。然而，正在增加的许多机构用户对 WAN 安全问题的敏感性，尤其是针对蜂窝电话的，导致了更有计划的安全策略，包括至少达到电话级别的加密数据——见 9.3.2.2。

D.3.2 局域网

D.3.2.1 概述

在一个校园区域内，或者一个建筑物的一层上，或一个家庭办公室内，局域网(LAN)系统也在兴起。这些网络常常使用与其“堂兄”广域网同样的协议和路由系统，但是通过在 LAN 和 WAN 间使用某种类型的网关，可提供更安全的环境。网关可能是一个简单的流量带宽和路由集线器，或者它可能包含防火墙、防病毒扫描软件，入侵检测和其他边界安全控制(如 10.5 中所指出的)。在所有情况下，保持对网络连接的理解和对网关设备的控制是保护 LAN 的关键所在。其他的细节在下面讨论。

D.3.2.2 有线 LAN 系统

有线 LAN 通常通过对路由器、交换机和线缆连接的管理实现物理保护。某些情况下，IP 地址的分配和其他管理功能可以限制新设备进入 LAN，尽管如此严格地管理网络可能对企业内用户造成困难，打击他们的信心。

D.3.2.3 无线 LAN 系统

D.3.2.3.1 概述

无线 LAN 系统，特别是 Wi-Fi，或 802.1 lx 系统通常提供可用于网络连接和数据发送的短距离[<300 ft(~100 m)]RF(射频)信号。有许多和无线 LAN 系统相关的安全问题，最明显的是故意广播潜在的敏感的公司信息。很多复杂的攻击：如夺取连接，通信和信任重定向都是可能的。在局部的安全解决方案(有线设备隐私 Wired Equivalent Privacy)公开之后几年，802.1 lx 系统的可互操作和安全的标准出现了。在各种无线系统中，可以使用思科专利的安全模块化标准，轻量级可扩展代理平台(LEAP)，开放保护可扩展认证协议(PEAP)。在企业内扩建无线 LAN 系统时，PEAP 的使用或相似的安全机制宜认真考虑。

扩建无线环境时，有两种主要的结构变化。一种变化是使用 PEAP，确保仅仅是授权系统和用户可以通过无线访问网络，并且在企业网络内部建立 LAN，把所有无线用户作为公司的可信成员。另一个变化是把外部 LAN 与公司网络连接，使用虚拟专网，SSL 站点或类似的安全技术保护对公司资源的访问。这些内容详见 D.3.2.3.2～D.3.2.3.4。

D.3.2.3.2 企业边界内部的无线 LAN

使用 PEAP 公司可确保只有授权用户可以访问无线 LAN 并使用公司资源。这类解决方案仍然易于受到拒绝服务攻击，但是如果无线服务是在一个由公司控制的建筑物或一个园区内管理和维护，这类解决方案还是很合理的。这类方案考虑了机构内的移动用户，在不同的会议室中参加多个会议的情形，或者经常往来于公司的各分部之间的管理人员。更进一步，这种类型的解决方案把对网络带宽的使用、互联网的接入和对其他的公司资源的访问限制到授权用户。这里有过多的关于 PEAP 的安全实现的细节需要在内部体系结构模型中深入讨论。供货商和互联网可提供很多资源。

D.3.2.3.3 企业边界外部无线 LAN

另一种为授权用户使用无线网络的方法是在企业网络外部提供带有互联网连接的无线连接。在这种情况下，无线用户可能是任何行走的路人，或者任何预订了服务的人。他们不能直接访问公司资源。需要访问公司资源的用户可使用 VPN(见 11.2.1)安全地接入公司网络。

这种解决方案在网络管理方面有缺点；但是有许多用户方面的优势。金融机构一般不希望外部用户使用无线 LAN 资源，但是大学可能会希望无线 LAN 对校园内的所有访问者开放。另外，资产管理公司可能希望一个建筑内的所有租赁人可以使用无线 LAN。

D.3.2.3.4 其他关于无线 LAN 的考虑

如同家中的宽带连接把介于互联网和公司网络与资源间的终端系统转变为边界设备一样，无线 LAN 也把终端系统(如笔记本电脑)转变为边界设备。因此使用无线连接的终端系统应考虑安装防病毒的软件、防火墙和入侵检测软件。

带有无线 LAN 连接的移动笔记本电脑将产生额外的需求。无论公司无线 LAN 是在企业网络内部还是外部，这些移动的用户都会需要通过 VPN(IPSEC 或 SSL)访问公司资源，因为无线“热点”越来越流行。这些热点位于机场、公园、大学、咖啡店、餐馆、饭店和其他商务旅行者频繁出现的地方。带有无线访问设备的经理人会希望互联网连接无时无处不在。VPN 为旅行中的用户提供访问公司资源的能力。

管理在“热点”的移动用户的一个主要的问题是对普通的互联网 IP 地址的信任。许多公司使用 10.(网段)和 168.(网段)。IP 地址是为文件和打印服务在公司内共享而设置的，这些不可路由的地址经常被重新使用，以至家庭网络、咖啡店和多重公司网络可能使用同样的地址(如，10.1.1.100)，即在每个网络中，不同的设备和资源具有同样的地址。因为 VPN 配置文件经常基于地址作加密和路由的决策，通过具有潜在的新的威胁的移动的笔记本，这些“10.”和“168.”地址可能会被错误的信任。类似 VPN、防火墙，IDS 系统也根据 IP 地址作连接和信任决定。因此，移动的笔记本信任一个工作环境中的打印机，甚至是家中的打印机可能是恰当的，然而信任咖啡店中的文件服务器就需要完全不同的考虑。对这些关切的策略、软件和其他对策宜基于公司的整体策略来评价和应用。

D.3.3 其他通信问题

这里还有一些其他通信问题。例如，在同一个网络上语音和数据不断整合，虽然这些问题刚刚开始产生，但它们开辟了通信问题和应对措施的新领域。最近，基于数据/语音整合的语音防火墙、中继 VPN 和多媒体入侵检测系统(IDS)解决方案的产品已出现，引起了主要供货商的关注。这些解决方案已被公司采用，提升了公司内部语音通信的管理质量，节省了成本。

参 考 文 献

[1] ITU-T Recommendation X.509 (2001) | ISO/IEC 9594-8, Information technology—Open Systems Interconnection—The Directory: Public-key and attribute certificate frameworks—Part 8

[2] ISO 7498-2, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture

[3] ISO/IEC 10181-1, Information technology—Open Systems Interconnection—Security frameworks for open systems: Overview

[4] ISO/IEC 13335 (All parts), Information technology—Security techniques—Management of information and communications technology security

[5] ISO 13491-1, Banking—Secure cryptographic devices (retail)—Part 1: Concepts, requirements and evaluation methods

[6] ISO/IEC 13888 (All parts), Information Technology—Security Techniques—Non-Repudiation

[7] ISO/IEC 15408 (All parts), Information Technology—Security Techniques—Evaluation criteria for IT security

[8] ISO/IEC 18043, Information technology—Deployment and operation of Intrusion Detection Systems

[9] ISO/IEC TR 18044, Information Technology—Security techniques—Information security incident management

[10] ISO TR 19038, Banking and related financial services—Triple DEA—Modes of operation—Implementation guidelines

[11] ISO 19092 (All parts), Financial Services—Biometrics

[12] ISO/IEC 19790, Information technology—Security techniques—Security requirements for cryptographic modules

[13] ISO/IEC 21827, Information Technology—Systems Security Engineering—Capability Maturity Model (SSE-CMM®)

[14] ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation

[15] ANSI X9.79-2001, Financial Services Public Key Infrastructure (PKI) Policy and Practices Framework

[16] ANSI X9.84-2003, Biometric Information Management and Security for the Financial Services Industry

[17] FIPS 140-2, Security Requirements for Cryptographic Modules, National Institute for Standards and Technology (USA.). http://csrc.nist.gov/cryptval/140-2.htm

[18] FIPS 197, Advanced Encryption Standard (AES), National Institute for Standards and Technology (USA.). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[19] Security Of Electronic Money, published by the Bank of International Settlement, Basle, August 1996

[20] W3C Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation, Copyright©[6 October 2000] World Wide Web Consortium, (Massachusetts Institute of Technology,

Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2000/REC-xml-20001006/

[21] Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing

[22] Gramm-Leach-Bliley (GLB) Act of 1999, http://www.senate.gov/~banking/conf/