21世纪 管理信息化前沿
IT治理经典丛书

信息安全管理

全球最佳实务与实施指南

孙强 陈伟 王东红 著

清华大学出版社

21世纪 管理信息化前沿
IT治理经典丛书

信息安全管理

全球最佳实务与实施指南

孙强 陈伟 王东红 著

清华大学出版社
北 京

内 容 简 介

本书是我国信息安全管理领域的重要专著，为我国各类组织管理信息安全风险提供了最佳实践。它从标准释疑、实施和案例分析三方面入手，全面阐述了信息安全管理体系的全生命周期。

文中全面介绍了 ISO/IEC 17799(BS7799)这一全球公认的信息安全管理标准的产生、发展历程及其主要内容；深入阐述了实施信息安全管理的方法、步骤及应用软件；并首次批露我国企业实施 BS7799 的经验和教训；同时，“BS7799 实施案例”重点从客户、咨询公司、厂商三个方面介绍了四个典型案例。

本书不仅适用于 CEO、CIO、IT 战略规划主管、CSO、政府和企业管理人员、IT 咨询顾问，而且也是信息系统审计师和信息安全管理体系审核员的必备参考佳作，更可作为高等院校从事信息安全管理教学研究的师生的参考文献。

图书在版编目(CIP)数据

信息安全管理：全球最佳实务与实施指南/孙强，陈伟，王东红著.—北京：清华大学出版社，2004.10
(21 世纪管理信息化前沿/IT 治理经典丛书)
ISBN 7-302-09654-6

Ⅰ.信…　Ⅱ.①孙…　②陈…　③王…　Ⅲ.信息系统—安全管理—国际标准　Ⅳ.TP309-65
中国版本图书馆 CIP 数据核字(2004)第 099412 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
策划编辑：张立红
文稿编辑：王晓娜
封面设计：王　岚
版式设计：孔祥丰
印 刷 者：北京季蜂印刷有限公司
装 订 者：北京国马印刷厂
发 行 者：新华书店总店北京发行所
开　　本：185×230　**印张**：23.75　**字数**：451 千字
版　　次：2004 年 10 月第 1 版　2004 年 10 月第1 次印刷
书　　号：ISBN 7-302-09654-6/F・955
印　　数：1～5000
定　　价：40.00 元

编 委 会 名 单

主　　任：张旭明

副 主 任：罗文

编　　委：陈拂晓　杨天行　刘献军　黄涌　李峻
郝亚斌　辛鹏骏　刘复利　孙强　孟庆麟
郭晓英　孟秀转　邓永基　王鹏　李莞菁
曲玉阁　赵晓光

总 策 划：郝亚斌

主　　编：孙强　陈伟　王东红

副 主 编：郝晓玲　孟秀燕　李长征　郭宏杰

引论

信息安全治理

信息安全治理产生的背景

在当今的全球商业环境中，信息的重要性被广泛接受，信息系统在各类组织中得到了广泛应用。许多组织对其信息系统不断增长的依赖性，加上在信息系统上运作业务的风险、收益和机会，使IT治理成为公司治理越来越关键的一部分。最高管理层(董事会)和执行管理层需要确保 IT 适应企业战略，同时企业战略也恰当利用IT的优势。

现实世界的任何系统都是一串复杂的环节，安全措施必须渗透到系统的所有地方，其中一些甚至连系统的设计者、实现者和使用者都不知道。因此，不安全因素总是存在。没有一个系统是完美的，没有一项技术是灵丹妙药。

事实上针对系统安全的攻击越来越普遍。早在 1996 年，美国会计总署(GAO)报告指出，美国国防部一年有 15 000 个系统遭到高达 250 000 次攻击，其中 65%攻击成功，防范和弥补损失的费用高达数亿美元。更值得注意的是，这些攻击中只有400 个被查明，20 个被报告。如果说 1996 年受到攻击很大程度上是一种系统的弱点，那么今天，它已成为一种威胁，正如美国联邦调查局对 100 个针对电子商务网站的敲诈案件调查表明，攻击者不仅威胁公开客户信息，并且实际上在要求得不到满足时实现这种威胁。许多国家的政府已经认识到安全的重要性，并积极采取措施提高信息安全，如根据敏感度隔开信息基础设施，投资于更好的认证方法，以及使信息基础设施使用者对其行为负责等。以美国政府为例，“9·11 事件”后美国信息基

础设施保护委员会(PCIPB)列出了53个信息安全重点问题，把信息安全列入国家战略。在这个战略中，信息安全被分成5个等级：第1级是家庭用户和小型商业机构，第2级是大型企业，第3级是高等教育、联邦政府、州与地方政府等关键部门，第4级是国家优先任务，第5级是全球性合作网络。但是，在2002年Gartner举办的研讨会上，与会人士普遍认为“9·11”后企业依然没有提高警惕，这一点从Gartner研究主管 Donna Scott 进行的调查中就可以明显地反映出来，这次调查是 Scott 在2002 年关于保持业务持续性发展问题的陈述报告的一部分。该报告显示全球 2000强企业中只有不到25%的企业在全面的业务持续性计划上进行了投资，而就在这些进行了投资的企业当中，只有 50%对自己的持续性计划进行了全面的测试。 针对严峻的现状，Scott 警告说：“随着实时企业观念的推进，即使是最小的中断——关键业务系统几分钟或是几小时的储运损耗、关键供应商或是外部服务供应商服务的中断对整个经济形势可能引发的潜在业务冲击及对客户或供应商所产生的影响——都可能带来极为严重的商业后果。”

美国政府在2003年投资500多亿美元，用于改造IT基础设施及其性能。其中政府机构用于网络安全的支出将增长64%，达到约 30 亿美元。看到上面的数字，你一定会认为，随着网络安全支出的增长，政府部门的计算机安全环境将会得到极大的改善，能够抵御任何形式的网络威胁。然而事实可能并非如此。Gartner 的副总裁 John Pescatore 预言，政府网络安全的显著改善至少需要花费3年的时间。他认为，与个人网络安全相比，政府网络安全现在还处于远远落后的状态，要想解决一些比较大的问题，必须先要建立网络安全的基础和机制。

目前业界普遍认为，信息安全是政府和企业必须携手面对的问题。政府和企业管理执行层(董事会)有责任确保为所有使用者提供一个安全的信息系统环境，而且，政府部门和企业在认识到安全的信息系统好处的同时，应该自我保护以避免信息系统的固有风险。

中国工程院院长徐匡迪曾指出：“没有安全的工程就是豆腐渣工程”。2003年我国接连不断地出现程度不同的信息系统安全事故，这些事故不仅仅是简单的信息系统瘫痪的问题，其直接后果是导致巨大的经济损失，还造成了不良的社会影响。如果说经济损失还能弥补，那么，由于信息网络的脆弱性而引起的公众对网络社会的诚信危机则不是短时期内可能恢复的。

我国政府主管部门以及各行各业已经认识到了信息安全的重要性。2004年1月

9日至10日，全国信息安全保障工作会议在北京召开。中共中央政治局常委、国务院副总理黄菊出席会议并作重要讲话。他指出，必须充分认识做好信息安全保障工作的极端重要性，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化健康发展。

为了切实加强金融信息安全保障工作，认真学习和贯彻落实全国信息安全保障工作会议精神，人民银行、银监会、证监会、保监会联合组织的全国金融信息安全保障工作会议在于2004年4月21日在京召开。会议结合当前金融信息安全保障工作实际，研究部署了新时期金融信息安全保障工作。

我们回头来看，政府和各行各业对信息安全的重要性有了认识，相关的标准规范正在形成，投资力度在加大，安全技术、产品、市场在发展，多数企业机构正在制定符合不同业务系统和网络安全等级需要的综合性安全策略和计划。那么，我们为什么依然没有安全感呢？到底需要什么样的方法或机制来治理或管理信息安全呢？经过近一年对国内外信息安全和最佳实务的研究，我们认为关键是要建立一套能够涵盖组织信息安全的制度安排机制，它包括治理机制和治理结构，这种制度安排通过建立和维护一个框架来保证信息安全战略和组织的业务目标精确校准，并且和相关的法律和规范一致。从后面的分析阐述中，我们可以看到有效的信息安全治理是非常必要的。

信息安全治理的含义

1. 信息安全治理的含义

所谓信息安全治理是指最高管理层(董事会)用来监督管理层在信息安全战略上的过程、架构及与业务的关系，以确保信息安全战略与组织的业务目标一致。它不同于信息安全管理。

信息安全管理提供管理程序、技术和保证措施，使业务管理者确信业务交易的可信性；确保信息技术服务的可用性，能适当地防御不正当操作、蓄意攻击或者自然灾害，并从这些故障中尽快恢复；确保拒绝未经授权的访问。信息安全管理的目标是公司的信息及信息系统的安全运营，确定IT目标以及实现此目标所采取的行动。

信息安全治理是一种基础制度安排，如果缺乏健全的制度安排，不可能有很好的信息安全管理；同样，没有有效的信息安全管理，单纯的治理机制也只能是一个

美好的蓝图，而缺乏实际的内容。就目前我国信息化建设的现状而言，无论是信息安全治理，还是信息安全管理都是我们所迫切需要健全的。

安全是一种“买不到”的东西。打开包装箱后即插即用并提供足够安全水平的安全防护体系是不存在的。建立一个有效的信息安全体系首先需要在好的信息安全治理的基础上，其次要制定出相关的管理策略和规章制度，然后才是在安全产品的帮助下搭建起整个架构。相反，就不可能得到一个真正意义上的安全防护体系。所以，尽管有些单位安装了一些安全产品，但这不能称其为实现了信息安全治理。

2. 善治的信息安全治理

善治的信息安全治理应该能做到：

(1) 安全战略与业务战略的一致

- 业务需求驱动安全需求；
- 安全架构适应业务流程；
- 信息安全投资与企业战略和最大风险状况密切相关。

(2) 交付价值

- 一系列安全实务标准，如最佳安全实务基准；
- 正确排序，将资源优先分配给具有大影响和商业利益的地方；
- 规范的、商业化解决方案；
- 完整的解决方案，包括组织、流程和技术等；
- 持续改进的文化。

(3) 风险管理

- 资产识别与估价；
- 脆弱性、威胁的识别与评价；
- 风险评估；
- 风险控制与管理。

(4) 绩效评估

- 定义评估准则；
- 反馈评估程序的进展；
- 保证独立性。

实现善治的信息安全治理

1. 实现善治的信息安全治理的方法

实现善治的信息安全治理，需要最高管理层(董事会)、管理执行层采用一种正确的方法。

(1) 清晰的职责分工

- 最高管理层(董事会)层职责：
  - 将信息安全及其持续性改进计划落实到业务管理者；
  - 建立审计委员会。该委员会清楚理解其信息安全任务，知道怎样与管理层和审计师合作；
  - 确保内部和外部审计师同意，审计中包括信息安全审计委员会和管理执行层要求的信息安全审计内容；
  - 要求信息安全负责人向审计委员会报告信息安全治理的进展和问题；
  - 建立危机处理机制，该机制要求执行管理层和最高管理层(董事会)最初就开始参与。
- 执行管理层职责：
  - 建立安全职责，协助管理者制定战略，并帮助组织实现这些策略；
  - 建立可测量的和易于管理的安全战略。该战略以标杆、成熟度模型、差距分析和持续报告绩效为基础；
  - 由安全和审计专家(内部的和外部的)筹办，进行年度的业务风险头脑风暴法会议；
  - 得出风险现状评估结论，提出行动建议，并用持续的行动强化执行效果；
  - 综合运用专家的知识，制定信息安全与风险应急方案；
  - 建立适用于企业的实施方案，不断评估和更新该方案；
  - 根据既定的程序进行信息安全审计，管理层有责任跟踪审计执行情况；
  - 制定清晰的方针策略和详细的指南，多和员工就该计划进行沟通，使每个人认可该计划，这就是善治的安全治理；
  - 经常性地监控评估所发现的系统弱点(CERT)，评估非法入侵造成的影响；

- 使支持业务流程的信息系统基础设施能够在故障发生后立即恢复，特别是遇到一般的故障时；
- 建立安全基准线，并严格监控其不被违反；
- 实施安全事故响应机制，减少重要数据的丢失和破坏；
- 通过高标准的控制流程来强化所有安全设施、重要的服务器和通信平台等；
- 基于业务管理规则授权，授权方式与业务风险管理相配合；
- 工作绩效评估包含安全绩效评估，并对此采取适当的奖罚措施。

(2) 分析关键成功因素

这一环节要确保：

- 认识到好的安全方案需要持续完善；
- 组织安全责任人直接向高层领导报告并负责安全方案的执行；
- 管理层和员工共同理解安全的重要性、必要性、弱点和威胁，理解并接受他们自己的安全责任；
- 定期由第三方来评估安全策略和安全体系结构；
- 安全负责人有管理安全的方法和能力，特别是在通过采取入侵测试和主动监控措施时，将发生事故的可能性降至最低，但事故不可避免发生时，应具备对事故侦查、记录，分析其严重性，编写报告和采取行动的能力；
- 清楚定义风险管理责任人的任务和职责及管理层的责任；
- 定义可接受风险的界限及风险转移、减少的策略；
- 定义风险管理改善行动的职责和程序；
- 每隔一段时期由第三方进行更客观的安全战略审查；
- 识别并持续监控关键的基础设施；
- 使用服务水平协议，增加与安全服务商、业务持续计划服务商之间的合作；
- 在制定策略时就考虑和确定策略的执行强度；
- 对员工进行策略认识、程序理解、是否遵循方面的测试；
- 保证部署前的应用软件的安全；
- 信息安全控制策略与业务整体战略规划相一致；
- 管理层确信和认可信息安全、控制策略，强调沟通、理解和遵循这些策略的必要性；
- 采用一致的策略制定框架，指导策略的构思、制定、实施和遵循；

- 意识到虽然“内部人”是绝大部分安全风险的根源，但有组织犯罪的攻击和其他没有专业知识人员的攻击也不容忽视；
- 适当关注数据机密性、版权及其他相关法律的遵循；
- 确保员工以符合道德、安全的方式履行责任；
- 榜样的力量是无穷的。管理层必须明白信息安全对于组织成功的关键意义，带头遵守有关规章制度，为所有员工树立起安全意识的榜样。

(3) 绩效评估标准

从以下方面判断在信息安全是否成功：

- 没有引起公众不满的事故；
- 减少因为安全问题而推迟新行动计划的数量；
- 有没有基于信息技术的业务持续性计划；
- 是否对重要的信息基础设施进行自动监控；
- 对员工从信息安全意识程度与信息安全操作实务两方面进行检查评估。

通过以下方面确定信息安全治理是否成功：

- 全面遵循最低安全要求，或者记录违背最低安全要求的行为；
- 制定和确认与 IT 有关的规划和策略，其内容包含信息安全的任务、远景、目标、价值和行为准则；
- 所有相关方都了解信息安全战略规划和策略。

2. 信息安全治理成熟度模型

最高管理层(董事会)和管理执行层可以运用信息安全治理成熟度模型建立组织的安全级别，见图 0 和表 0。该模型被认为是：

- 一种自我评估等级的方法，确定组织处于哪个级别；
- 一种使用自我评估结果设定将来发展目标的方法，这个目标是根据组织希望处于等级表的哪个级别；
- 一种达到项目目标的计划方法。这个计划是通过对当前状况和目标差距分析来实施的；
- 一种确定项目优先次序的方法。这种次序确定的依据是项目类别及其投资收益率。

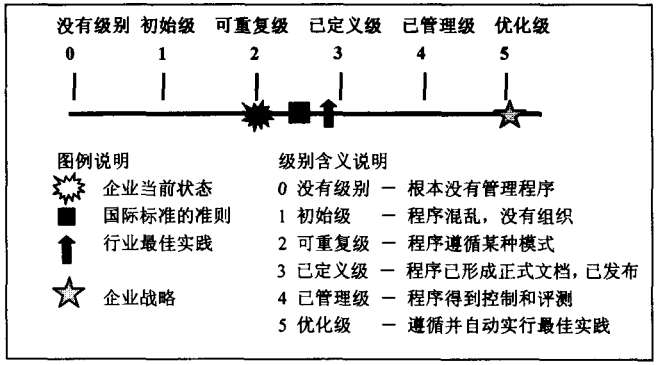

图 0　信息安全治理成熟度模型

表 0　信息安全治理成熟度级别

成熟度级别说明	说　明
0	没有级别 ● 没有业务评价流程；组织没有考虑安全隐患和项目开发不确定性对业务的影响；没有认识到风险管理关系到 IT 解决方案的获得和 IT 服务的交付。 ● 组织没有认识到信息安全的必要性；没有确定保证安全的责任和义务；没有实行支持信息安全管理的措施；没有对信息安全问题及时响应的程序；完全没有系统安全管理流程。 ● 不理解 IT 运作的风险、弱点和威胁，不理解 IT 服务中断对业务的影响；不认为服务的持续性是管理层应关心的问题。
1	初始级 ● 组织以一种混乱的方式考虑 IT 风险，没有遵循定义的流程和策略；每个项目都是采取非正式的项目风险评估。 ● 组织认识到信息安全的必要性，但是安全意识只依靠个人；被动考虑信息安全，没有对信息安全进行审计；由于职责不清，没有人对发现的信息安全问题负责；无法预知信息安全问题的后续反应。 ● 持续提供服务的职责不是正式的，且只有限地授权；管理层知道有关风险和持续服务的必要性。

(续表)

成熟度级别说明	说　明
2	可重复级 ● 开始认识到信息系统风险的重要性和必要性；有某种风险评估方法，但这个过程虽然仍然不成熟，但在完善中。 ● 信息安全职责被赋予一个了解信息安全，但没管理权的人；员工具有不完整的和有限的安全意识，但无法分析信息安全的信息；没有确定组织特定的信息安全需求，只是被动对信息安全事故做出反应，请第三方处理这些事故；开始制定安全策略，但没有足够的技巧和工具；信息安全报告不完整，易于使人误解，或不能切中要害。 ● 分配了持续服务的职责，但提供的服务不完整；系统可用性比较差，没有考虑其对业务的影响。
3	已定义级 ● 组织范围内的风险管理策略定义了怎样进行风险评估；风险评估遵循一个已定义的流程；该流程已形成规范，适用于所有接受过相应培训的员工。 ● 安全意识存在并得到管理层的促进；安全简报已标准化和正式化；定义信息安全程序并使其适合安全策略和程序结构；确定信息安全职责但没有始终如一地得到执行；信息安全报告面向 IT 而不是面向管理；执行了初步的入侵测试。 ● 管理层不断交流持续服务的必要性；局部采用了高可靠设备和冗余系统；严格维护重要的系统和设备。
4	已管理级 ● 根据标准程序评估风险，不遵守此程序的将被 IT 管理者通报；IT 风险管理可能成为具有很高责任的管理职能；管理执行层和 IT 管理者已确定组织容忍的最大风险级别，并已有测量风险/投资回报率的测量标准。 ● 清晰赋予、管理和执行信息安全职责；持续分析信息安全风险及其影响；完整的基于特定安全基准线的安全策略和实践；标准化、流程化的用户识别、验证和授权程序；建立员工安全知识考试制度；入侵测试是标准的和正式的预防程序；越来越多利用成本/收益分析，支持安全评测；信息安全流程与组织总体的安全战略保持一致；信息安全报告与管理目标相联系。 ● 强制执行持续服务的职责和标准；关键系统使用冗余系统，包括使用高可靠设备。

(续表)

成熟度级别说明	说　明
5	优化级 ● 开始有规律地、有效地执行一个结构化的、组织范围内的风险评估流程。 ● 信息安全是业务管理者和 IT 管理者的共同责任，它被统一到公司安全管理目标中；信息安全需求被清晰定义，优化并包括于经核实的安全计划中；安全职责在应用软件的设计阶段就被考虑，终端用户负有更多管理安全的责任；信息安全审计报告提供变化的和风险早期预警告；自动监控关键的系统；利用由自动化的工具支持的正式的事故响应程序以快速处理事故；定期的安全评估，以评价安全计划执行效果；系统地收集和分析新的威胁和隐患信息，及时通知并实施恰当的补救措施；入侵测试、安全事故的深层原因分析和预先发现风险是持续改进的基础；在组织范围内构成人、制度和技术三维一体的安防体系。 ● 持续服务计划和业务持续性计划被集成，优化，并得到日常的维护；购买的持续服务必须得到厂商和主要提供商的安全保证。

概述起来，信息安全治理成熟度模型方法和其他成熟度模型一样，具有以下几个方面的优点或作用。

- 信息安全治理成熟度模型涉及信息安全和组织业务的各个方面，是一种进行实用性比较的等级制，能以简单方式测定差异，有助于确定有关信息技术管理安全性方面的相对水平；
- 使管理部门相对容易地依据等级制对自己定位，并找出需要改善安全管理的地方。组织对自身进行差距分析以确定需要做哪些工作来达到所选级别。0～5 等级是基于一个简单的成熟性量度，体现出一个处理如何从不存在级发展到优化级的管理过程，增加成熟度意味着增强风险管理与提高管理效率；
- 信息安全治理成熟度是测量信息安全管理等级的一种方法，这些等级正是一个给定的信息安全管理处理的惯例，体现各个成熟层次的典型模式，有助于组织将主要精力投入到关键的管理方面；

- 信息安全治理成熟度模型等级有助于专业人员向管理层解释信息安全管理存在的缺陷，并把他们组织的控制惯例与最佳惯例对照起来，从而确定组织的未来发展目标。

信息安全治理成熟度模型将有助于解决在 IT 部门中普遍存在的以下问题。

- ➢ 在竞争如此激烈的市场环境中，你的公司或部门在信息安全上处于什么水平？
- ➢ 如果你认为有差距，究竟差在哪里？如何去改进？
- ➢ 如果你觉得运作善治，那么你能说出好在哪里？好到何种程度？
- ➢ 如何对信息安全管理进行绩效评估？

信息安全治理的规范

目前已有的信息安全治理规范包括：

1. 经济合作和发展组织，《信息系统安全指南》(1992)

经济合作和发展组织的《信息系统安全指南》用于协助国家和企业构建信息系统安全框架。美国、OECD 的其他 23 个成员国，以及十几个非 OECD 成员国家都批准了这一指南。该指南旨在：

- 提高信息系统风险意识和安全措施；
- 提供一个一般性的框架以辅助信息系统安全度量方法、操作流程和实践的制定和实施，鼓励关心信息系统安全的公共和私有部门间的合作；
- 促进人们对信息系统的信心，促进人们应用和使用信息系统；
- 方便国家间和国际间信息系统的开发、使用和安全防护。

这个框架包括法律、行动准则、技术评估、管理和用户实践，及公众教育或宣传活动。该指南的最终目的是作为政府、公众和私有部门的标杆，社会能通过此标杆测量进展。

2. 国际会计师联合会，《信息安全管理》(1998)

信息安全的目标是“保护依靠信息、信息系统和传送信息的人、通信设施的利益不因为信息机密性、完整性和可用性的故障而遭受损失”。任何组织在满足下面 3 条准则时可以认为达到信息安全目标：数据和信息只透露给有权知道该数据和信

息的人(机密性)；数据和信息保护不受未经授权的修改(完整性)；信息系统在需要时可用和有用(可用性)。

机密性、完整性和可用性之间的相对优先级和重要性根据信息系统中的信息和使用信息的商业环境而不同。

信息安全因急速增长的事故和风险种类而日益重要。对信息系统的威胁既有可能来自有意或无意的行动，也可能来自内部或外部。信息安全事故的发生可能是因为技术方面的因素、自然灾害、环境方面、人的因素、非法访问或病毒。另外，业务依赖性(依靠第三方通信设施传送信息，外包业务等等)也可能潜在地导致管理控制的失效和监督不力。

3. 国际标准化组织，《ISO 17799 国际标准》(2000)

ISO/IEC17799(根据 BS7799 第一部分制定)作为确定控制范围的单一参考点，在大多数情况下，

这些控制是使用业务信息系统所必须的。该标准适应任何规模的组织。它把信息作为一种资产，像其他重要商业资产一样，这种资产对组织有价值，因此需要恰当保护它。

ISO/IEC17799 认为信息安全有下列特征。

- 机密性—— 确保信息只被相应的授权用户访问；
- 完整性——保护信息和处理信息程序的准确性和完整性；
- 可用性——确保授权用户在需要时能够访问信息和相关资产。

信息安全保护信息不受广泛威胁的损毁，确保业务连续性，将商业损失降至最小，使投资收益最大并抓住各种商业机遇。安全是通过实施一套恰当的控制措施实现的。该控制措施由策略、实践、程序、组织结构和软件组成。

4. 美国注册会计师协会(加拿大特许会计师协会)，《SysTrustTM 系统可靠性原理和准则 V20》(2001)

SysTrust 服务是一种保证服务，用于增强管理者、客户和商业伙伴对支持业务或某种特别活动的系统的信任。SysTrust 服务授权注册会计师承担如下保证服务：注册会计师从可用性、安全性、完整性和可维护性 4 个基本方面评估和测试系统是否可靠。

- 可用性—— 系统在服务水平声明或协议规定的时间内可以运行和使用；

- 安全性—— 确保系统拒绝未经授权的物理的或逻辑的访问；
- 完整性—— 系统的数据处理是完整的、准确的、及时的和被授权的；
- 可维护性—— 必要时能够升级系统而不影响系统或者与系统的可用性、安全性和完整性相冲突。

SysTrust 定义在特定环境下及特定时期内，没有重大错误、缺陷或故障地运行的系统为可靠系统。系统的界限由系统所有者确定，但必须包括以下几个关键部分：基础设施、软件、人、程序和数据。

SysTrust 的框架是可升级的，因此，企业能够灵活选择 SysTrust 标准的任何部分或全部来验证系统的可靠性。对系统四个标准的判断组成对系统整体可靠性的判断。注册会计师也能单独判断某一标准如可用性或安全性的可靠性状况。但是这种判断仅仅对特定标准的可靠性做出判断，不是对系统整体可靠性的判断。

5. 信息系统审计和控制协会(IT 治理研究院)，《信息和相关技术的控制目标》(COBIT)

COBIT 的第一版由信息系统审计和控制协会(ISACF)于 1996 年发行。在 1998 年，第二版在增加了控制目标和实施工具集后出版。现在得到的第三版由 IT 治理研究院在 2000 年发行，增加了管理方针和其他详细的控制目标。CoBIT 起源于 IT 需要传递组织为达到业务目标所需的信息这个前提。除了鼓励以业务流程为中心，实行业务流程负责制外，COBIT 还考虑到组织对信用、质量和安全的需要，它提供了组织用于定义其对 IT 业务要求的几条信息准则：效率、效果、可用性、完整性、机密性、可靠性和一致性。

COBIT 进一步把 IT 分成 4 个领域(计划和组织，获取和实施，交付和支持，监控)，共计 34 个 IT 业务流程。其中 3 个与信息安全直接密切相关的业务流程是：

- 计划和组织流程——评估风险；
- 交付和支持流程—— 确保持续的服务；
- 监控流程—— 保证系统安全。

每个流程定义了一个高级别的目标：

- ➢ 识别 IT 流程中最重要的信息准则；
- ➢ 列出需要经常调整的资源；
- ➢ 考虑控制 IT 流程的重要方面。

COBIT 为正在寻求控制实施最佳实践的管理者和 IT 实施人员提供了超过 300