IBM安全性

Tivoli software

企业风险和合规管理

IBM安全解决方案支持新业务模型，有助于管理整个企业的合规性

目录

执行概要

在日趋物联化、互联化和智能化的智慧地球上，安全性对于企业至关重要。组织面向受众提供的数据和信息越多，存在的风险就越大。结果，出现了一系列新的需求。安全性必须是智慧的安全性，使组织能够与他们的客户、合作伙伴、员工以及其他实体之间建立信任，保护关键的信息、应用、系统和服务。但这仅仅是开始。

组织必须具备智慧的安全性，以利用新的具有前景的营业模型。举例而言，联邦关系使组织能够更加自由地共享信息，在高度互联的环境中与其他组织相互协作。组建联邦可能是一个充满挑战的过程，因为一个组织互联程度越高，它的系统就会越容易受到攻击。新的业务模型也需要智慧安全性来支持，比如云计算，其中资源是在传统组织及其安全性基础架构的边界外部进行管理的。要充分利用智慧地球上的新机会，组织必须保证他们的关键资源安全并受到保护，无论谁访问它们或它们位于何处都是如此。

开展业务的新方式使组织更加需要管理整个环境中的风险。如今的监管部门要求符合越来越多的标准，以保护敏感数据的隐私和完整性，组织必须具备正确的安全机制来尽可能高效地完成这一任务。然而，符合这些标准并不能保证系统是安全的:组织还必须主动评估和管理各个系统中的风险。

在组织努力降低复杂性、削减成本和确保合规的过程中，恰当的安全控制和最佳实践扮演着重要角色。因此，要加强安全性，风险和合规解决方案应该作为整合服务管理(Integrated Service Management)办法的一部分来实现。此方法有助于使安全性成为业务流程不可分割的一部分，而不是一个附加部分，有助于组织在业务和IT资产之间实现可视化、可控化和自动化。

将更多资源用于满足不断增长的合规需求

如今，在美国有数千种对各种组织进行监管的法规，并且仍在不断推出更多法规，尤其是在受到严格管制的行业中，比如银行和金融服务。2010年美国政府投入558亿美元预算用于该财年的监管活动，高于上一个财年的536亿美元，实际支出可能比估计的预算更高。与上一年相比，2010年的监管开支预计增长4.2%，联邦监管机构的员工安置预算将增长2.3%。[1]

和联邦政府在监管活动上花费更多资金一样，私有企业也在增加资金投入来遵守法规。一项报告预计，美国公司2010年在监管、风险和合规方面投入的资金将增长至298亿美元，比上一年增加了近4%，几乎是企业在2005年预计花费的两倍。而这还没有考虑用于遵从美国监管要求在全球的花费。公司迄今为止已花费了数年的时间致力于监管合规预算，每年遵从不断增加的法规和行业要求所需的资源持续增长。这些监管要求针对的是企业面临的实际而严重的威胁，以及恶意的个人和组织可能滥用的个人私有数据。

而且追求合规性永无止境:这是一种持续的、周期性的过程，要求不断的付出和关注。不幸的是，保持合规并不总是能确保系统的安全。组织必须明智地选择遵守法规的方法，以免-浪费时间和金钱。主动评估和管理环境中的风险不仅能满足合规需要，而且使组织能够追求旨在削减成本和改善服务的新业务模型。一项研究显示，超越基本的临时流程实现最高级优化的公司能够获得更多的收入、利润和客户维系水平，每年合规性的花费比早期阶段更少。

寻找智慧的风险解决方案来应对挑战

在瞬息万变的监管和运营环境中，要成功管理风险非常困难。这要求智慧的风险解决方案，能展示出对风险相关信息的新颖和独创性的度量、建模和应用方法。智慧的风险管理在于收集更好的信息，更快速有效地加以利用，并将日常事件中对人为干预的需求降至最低。因此，智能化和互联化不仅让风险和合规管理充满了挑战，同时也为迎接这些挑战提供了绝佳的机遇:

- 智慧企业是物联化的，实现细粒度的信息管理和控制，使组织能够感知威胁并迅速、准确地做出反应。
- 智慧企业的系统建立在支持创新的互联数据之上，能够直接推进数据处理和提供单一的事实来源。
- 智慧企业支持对广泛的结构化和非结构化数据进行快速、智能的分析，以提高洞察力，做出明智的判断。

为了提前预防如今的风险和合规管理挑战，智慧企业正在努力提高在全球的业务范围内实时了解和管理风险的能力。

使用IBM安全性框架解决风险和合规问题

随着组织努力创建既安全又动态的基础架构，他们面临着跨安全域端到端管理风险的新的迫切要求。在动态基础架构中管理风险的关键在于建立一组基本的安全控制，使其能够灵敏、快速地提供服务，同时削减管理和运行安全基础架构的成本。

为此，IBM创建了一个综合安全性框架，它基于：

- 信息及相关技术的控制目标(COBIT)，这是全球公认的基于行业标准和最佳实践的管理框架。[6]
- 信息安全管理实用规则(ISO/IEC 27002:2005)是一个国际标准，制定了企业发起、实施、维护和改进信息安全管理的指导方针和一般原则。该标准包括11个信息安全管理领域的控制对象和控制的最佳实践。
- IT Infrastructure Library® (ITIL®)，为IT服务管理和相关流程提供了一个综合、一致且连贯的最佳实践框架。[8]

从安全的角度来看，对这些流程和最佳实践进行集成使组织能够确保它们在固定的控制限制下正常运行，在日益互联和复杂的环境中提供期望或要求的服务。

IBM安全性框架的总体基础包括安全性治理、风险管理和合规、支持常见策略、事件处理和报告。IBM安全性框架的关键组成部分包括：

- 人员和身份–确保合适的人和系统能够在合适的时间访问合适的资产。
- 数据和信息–保护正在传输的和静态的关键数据。
- 应用和流程–确保应用和业务服务的可用性和安全性。
- 网络、服务器和端点–提前预防所有IT系统组件中的即将出现的威胁。
- 物理基础架构–利用数字控制保护物理世界中的事件。

图1:IBM开发的安全性框架为跨企业安全域端到端地管理风险提供了基础。

IBM通过结合硬件、软件和服务帮助企业完整或部分地应用此安全性框架。IBM在此框架中提供的企业风险和合规管理解决方案既全面又灵活，它们可以针对独特的企业要求而调整，从而适当地管理风险和帮助向监管者证明合规性。

面向企业风险和合规管理的IBM安全解决方案

IBM针对企业风险和合规管理提供了一个完善的安全解决方案组合，它有助于应对越来越物联化、互联化和智能化的企业中的系统安全挑战。这些产品提供了全面的功能来解决企业环境中的人员、流程和信息风险问题。为了确保环境在固定的控制限制下跨各种业务和IT资产，适度的可视化、可控化和自动化妥善运营是必要的。在整合服务管理(Integrated Service Management)方法中实现风险和合规管理解决方案可以加强安全性，方法是将它作为业务流程的一个不可或缺的部分来构建，而不是附加部分。IBM安全解决方案使用一种整合服务管理方法实现，可以提供在智慧地球上推动成功的业务增长所必需的可视化、可控化和自动化水平。

IBM针对企业风险和合规管理的解决方案跨身份、数据和信息、应用、流程和基础架构端到端地保护企业。每项产品中都包含自动化的风险管理功能，可形成一个从控制、管理到审计、合规的闭合循环。IBM解决方案通过在所有这些产品上建立集成的合规管理机制，帮助确保各个平台上一致的合规性。

本文介绍用于帮助您评估和管理整个企业中的风险的具体的IBM软件解决方案。

IBM Tivoli Security Management for z/OS:下一代大型机安全

大型机操作的日趋复杂和范围的日趋扩大，再加上熟练的大型机操作人员的有限，这为管理组织最安全的平台带来了挑战。不断增长的数据量，共享大型机上的信息的必要性，以及监视访问控制(甚至对于系统的特权用户)的任务，都可能产生巨额开支和复杂的安全性问题。组织需要一个大型机解决方案，可以安全地自动进行审计、警报和监视，同时提高大型机成为企业安全性中心的能力。

在如今的大型企业中，许多任务关键型应用可能位于IBM System z®大型机计算机上。IBM使用端到端大型机安全解决方案帮助使大型机能够作为企业安全性中心而运行，该解决方案提供安全策略实施、有效的用户管理、威胁监视以及其他与风险和合规管理相关的功能。

IBM根据具体的企业安全要求来建立和实施安全策略，加强了风险管理和合规性。组织可以在Resource Access Control Facility (RACF®)上前瞻性地实施安全策略合规，预防内部安全错误，识别不合规的安全命令，发出警报来响应高风险的安全命令。

Tivoli Security Management for z/OS® 提供了更加有效的用户管理和简化的安全管理，帮助提高与风险和合规管理相关的任务的效率并减少其中的错误。例如，管理员可以在不影响生产的前提下测试安全配置变更，主动识别多个RACF数据库之间潜在的冲突，以及从单一界面管理用户、组、角色、权限和策略。

通过全面、连续地监视威胁事件，Tivoli Security Management for z/OS可以检测对已有基准的变更，找到滥用特权的证据，减轻内部威胁风险。IBM的解决方案还包含跨平台日志收集、复杂的数据分析以及跨操作系统、应用和数据库的预封装报告等功能，帮助促进对政府和行业法规及标准的合规性。

Tivoli Security Management for z/OS支持目前所有受支持的IBM z/OS操作系统版本，以及企业所依赖的CICS®等子系统。这减少了与升级到z/OS新版本相关的工作，使得以非停机方式管理风险和合规性更加容易。

通过IBM提供的合并的安全功能，如RACF、System z大型机安全性和其它IBM企业安全性解决方案，组织能够建立企业安全性中心，在该中心实现整个企业的安全性管理和安全策略的集中化和标准化。该中心可以提供风险和合规管理功能，比如生命周期身份管理、访问控制策略、联邦身份管理以及合规性监视和报告功能。

Tivoli Security Management for z/OS是zSecure产品系列的一部分，其中包括向CA TopSecret和CA ACF/2以及RACF添加其它审计和风险管理功能的产品。

IBM特权身份管理解决方案:防御内部威胁

尽管保护IT系统免受外部危害至关重要，特别是当因为与其它组织共享信息和进行协作的需要而模糊了传统界限时尤为如此，但是请谨记对系统的威胁也可能以特权用户的形式来自企业内部。他们使用IT系统、应用和数据来进行日常工作，能够访问敏感信息和资产，并且往往掌握了高超的技术。因为他们被授予了对IT系统的众多的访问权限，所以这些内部用户可能对组织内的数据完整性和隐私构成了最大威胁。事实上，2007年的一项研究表明大约69%的安全性事件来自员工和前雇员。[9]无论是这些安全性事件是故意、恶意的还是无意、偶然的，它们都可能造成严重的危害，企业必须对此严加防范。

显然，管理与特权用户相关的风险的答案不是为了限制访问，对管理员、LOB经理和其他一些用户而言，广泛的访问权限是必要的。其目的是确保他们的操作具有适当的可见性，同时配备策略和流程来迅速响应问题和潜在问题。IBM安全性解决方案可通过这种方式帮助保护企业，它们提供了如下功能:

通过规定用户权限来管理对系统和应用的访问，使用实时行为跟踪来发现问题，以及提供实时警报来迅速解决威胁。

IBM特权身份管理解决方案的另一个重要优势是能够在虚拟机不断增加、数据中心整合不断推进和云计算不断成熟的过程中保持特权身份的可控性和问责性。

IBM Tivoli Access Manager系列解决方案使组织能够建立有效、自动化的系统来管理特权用户对操作系统、电子商务应用和其他关键系统的用户访问。一旦部署了这些解决方案，Tivoli Security Information和Event Manager等解决方案便可用来自动监视用户行为，识别问题和报告用户活动。这使收集的用户活动监控信息变得可操作，尤其是在论证与特权用户问题相关联的内部策略和监管要求的合规性时。Tivoli Security Information and Event Manager也提供了近乎实时的警报功能。关于可疑活动的信息可以传送到一个关联引擎以供进一步分析和处理。

IBM Tivoli Security Information and Event Manager: 优化合规工作

安全性信息和事件管理(SIEM)通过将实时管理与监视和报告相结合，可帮助优化安全和合规工作。IBM Tivoli Security Information and Event Manager汇集了SIEM的两个主要方面，即用于事件管理的实时管理仪表板和评估策略合规性的信息分析仪表板，为风险和合规性管理提供了综合的基础。结合运用这两项功能，组织可以在整个企业中集中进行日志收集和事件关联，并利用先进的合规性仪表板将事件和用户行为链接到企业策略。

Tivoli Security Information and Event Manager提供了强大的企业审计仪表板，使首席信息安全官和审计人员能够获得企业中所有相关活动的单一视图。他们可以迅速了解记录了多少活动并将用户配置文件与被访问的信息相比较。企业审计仪表板还有助于查看随时间变化的策略违犯情况，利用日志数据库满足不同的报告和合规要求。

为了推动对特定法规的遵从性，IBM解决方案还包含了丰富的管理模块，每个模块都提供了极其详细的帮助，包括:

- 资产分类模板，使用法规所使用的术语显示受影响的信息、人员和资产。
- 策略模板，根据监管谁应该访问被监管信息以及能够访问多少信息的自定义策略衡量事件数据。
- 报告中心，利用资产分类和策略模板提供针对具体法规或最佳实践的数十个相关合规报告。

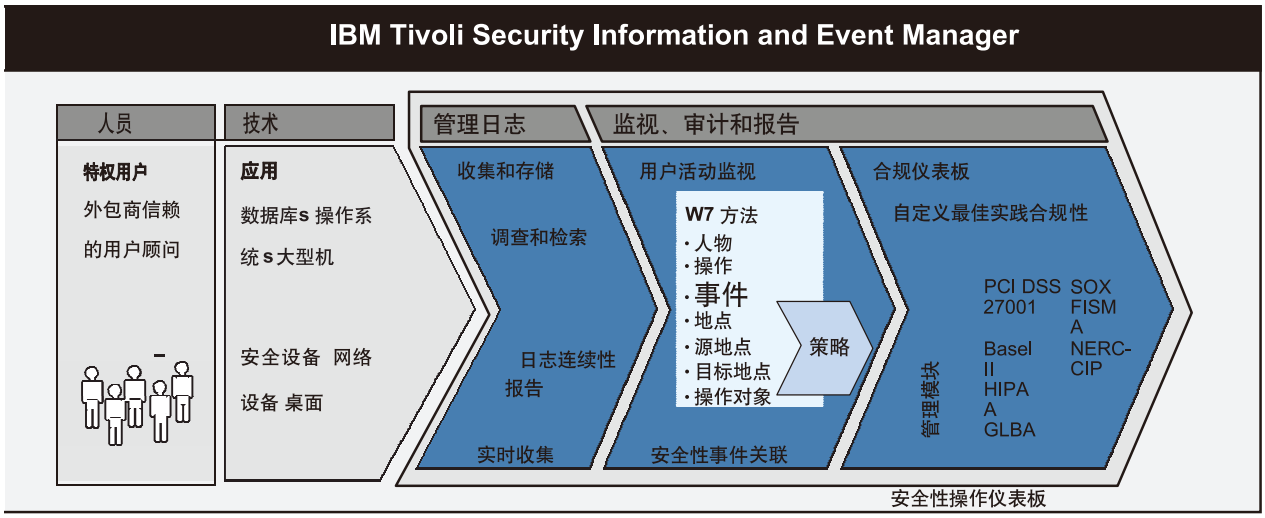

图2: IBM Tivoli Security Information and Event Manager为解决SIEM要求提供了完善的基础。

IBM Guardium软件: 数据库风险和合规管理

对同时提供了实时安全性和细粒度审计的经济有效的企业风险和合规解决方案的探索，已延伸到了数据库环境，在这个环境中，独立的应用可用来在不显著影响性能的前提下实施策略。

Guardium实时数据库监视和企业应用安全性使组织能够通过主动识别未经授权的数据库活动保护其关键企业数据的安全。它还包含审计和合规功能，以简化合规和数据隐私流程。并且与许多数据库审计解决方案不同，Guardium涵盖z/OS操作系统平台，提供了完整的数据库覆盖。它创建了细粒度的审计线索，而不会影响性能或稳定性，统一了对多个平台的监控，并作为独立网络设备在数据库外进行操作，确保了职责分离。

Guardium数据库监控和安全功能具有工作流自动化应用，该应用简化了合规工作流程，把数据库安全性生命周期管理从容易出错的、耗时的定期执行的活动转变为有效地支持风险和合规目标的连续的、自动化流程。该软件:

- 提供一组在整个企业基础架构实施的策略和报告，无需配置每个数据库服务器或安装新软件。
- 同时将审计线索和督查结果存储在一个甚至特权用户都无法修改的信息库中。
- 跟踪电子签发和逐级上报的结果。
- 管理合规报告在整个企业中的定期分发。
- 实现对安全事件和策略违反进行主动、实时响应，而不是只提供对静态日志数据的事后分析。
- 提供自动化的合规报告和工作流自动化功能，减少IT工作负载。

Guardium也可用于自动化任何重复性任务。例如，可以安排定期扫描以自动发现可能添加到或从以前的位置移开的敏感对象，产生的结果可用来自动更新这些对象的所有适当的策略组。

IBM Tivoli Data and Application Security:企业数据的端到端保护

随着数据量不断增加，并且数据共享仍然是运营业务的重要部分，如今的企业面临着不断增加的数据丢失风险。目前，数据量每18到24个月就会翻一番，使提供安全的企业数据存储变得更加复杂，[10] 并且应用程序已成为了数据安全威胁的一个主要的攻击点。随着如今的复合应用越来越复杂，再加上企业长期致力于让它们更容易被需要共享信息的用户访问，组织的数据变得比以往更加脆弱。数据丢失事故可能对企业造成巨大影响，导致的后果包括对底线的易于量化的影响，以及难以量化但同样具有破坏性的影响(如公共声誉的损失)。

Tivoli Data and Application Security通过提供可审计的访问控制，支持对用户特权的细粒度控制，以及集中进行对数据加密密钥的管理，帮助组织保护数据和应用。它为企业存储系统、数据库和关键应用中的敏感数据提供了端到端的保护，有助于支持合规计划及提高数据和应用的可靠性。

IBM Tivoli Data and Application Security提供了以下重要特性:

- 对用户特权的细粒度管理，从应用级别到操作系统级别。
- 集中的授权和安全策略管理和实施，用于细粒度的授权和数据级访问控制。
- 对加密密钥的集中管理，用于磁带和磁盘存储。
- 完善和自动化的用户活动监视和报告。
- 为应对各种法规和行业标准而定制的集中的、自动化合规报告和日志管理，这些法规和标准包括支付卡行业数据安全标准(PCI DSS)、Basel II、Sarbanes-Oxley (SOX)和ISO 27002等。

数据和应用安全解决方案通过防止对敏感数据的可能导致数据破坏或合规性违规的未授权访问或使用，可帮助组织管理风险。与此同时，它还可以帮助促进内部和外部协作者之间的数据共享，包括通过基于Web的服务。

IBM Rational AppScan Enterprise Edition:测试Web应用漏洞

对任何参与电子商务的企业而言，测试和报告Web应用的安全性都是风险和合规管理的一个愈加重要的部分。在这方面，许多组织面临的挑战在于将应用扫描扩展到整个企业，同时仍然维持对漏洞数据的集中控制。为了应对此挑战，IBM提供了IBM Rational® AppScan? Enterprise Edition，这是一个基于Web的多用户应用安全解决方案，适合需要以集中方式执行漏洞评估的测试团队使用。该软件的功能包括先进的应用扫描、修正功能、管理性安全度量指标和仪表板，以及重要的合规报告。

IBM Rational AppScan Enterprise Edition包含一个可扩展的企业架构，支持同时集中扫描多个应用。它遍历一个Web应用，分析和测试它的安全性和合规问题，然后生成实用的报告。

该软件可以检测Web应用中嵌入的恶意软件以及恶意或不良的站点，减少企业网站感染访问者的系统或将它们重定向到危险的在线目标的风险。一旦扫描进程识别出安全漏洞，该软件将提供智能修复建议，简化修正过程。它还执行对指标的连续监视和汇聚，确保随着时间的推移修正和趋势改善。复杂的仪表板和灵活的报告视图提供了风险和修正过程的企业级可视化。与质量保证(QA)测试工具和代码扫描设备的无缝集成，进一步简化了QA和开发团队执行的安全测试和修正。

为了论证对监管企业系统安全性的法规的符合性，该软件附带了40多个开箱即用的安全合规报告，包括针对PCI DSS、ISO 27001和ISO 27002安全性标准，以及Health Insurance Portability and Accountability Act (HIPAA)、Gramm-Leach-Bliley Act (GLBA)和Basel II记录等行业特定法规的报告。

IBM安全性服务:一种综合的端到端的风险管理方法

IBM安全性服务提供了业界最丰富和最富创意的安全性服务组合，使客户能够有效地管理风险，同时优化安全性投资。通过提供跨IBM安全性框架所有域的各种服务，风险合规管理、数据和信息、应用和流程、网络、服务器和端点以及物理基础架构，IBM安全性服务推动提高企业的集成度，缩短上市时间和创收时间。

IBM安全性服务组合包括帮助评估和实现安全性解决方案的专业的安全性服务、托管防火墙服务等托管安全性服务，其中IBM从云中管理企业的安全性；和Web URL过滤或安全性事件日志管理等云安全性服务。

在风险和合规性管理领域，来自IBM安全性服务的产品可以帮助企业应对3种重要的业务挑战:满足合规要求，理解和管理风险，以及实现合适的策略和控制。解决这3大挑战的服务产品包括:

- 安全策略规划和制定。
- 安全风险评估。
- 安全健康状况检查。
- 安全研讨会。
- 信息安全框架开发。
- 企业安全架构开发。
- 隐私服务。
- PC安全性评估。

这些产品能够通过多种方式为企业提供帮助，例如通过评估对主要法规和行业标准的合规状态来设置合规基准，开发合适且有效的框架来实施风险和合规管理。IBM安全性服务同时利用了来自IBM和作为IBM精选合作伙伴的其他领先安全性供应商的同类最佳产品。

为何选择IBM?

作为领先的安全公司，IBM以可信赖的合作伙伴身份与我们的客户合作交付安全产品和服务，其中我们的研究成果、尖端的技术、专业咨询经验、实施体验和对IT安全解决方案的世界级支持进行了整合与互联了，而安全性成为了

IT服务环境的内在要素。我们帮助客户解决确保智慧地球安全的复杂性、成本和合规性问题。在评估客户的安全需要、提供解决方案和确保这些解决方案成功实施方面，IBM是您的理想选择:

- 我们拥有技术-IBM拥有能够理解和修复威胁的X-Force®，以及数千个专注于安全计划的研究人员、开发人员、顾问和主题专家。
- 我们知道方法-我们已指导和实现了数千个安全项目，所以我们在最佳实践、流程和ROI方面拥有实践专长，并且我们关心客户的成功。
- 我们了解全局-IBM提供端到端解决方案，从安全策略和监管到跨大型机、台式机、网络、普适计算等。
- 我们了解客户的行业-IBM拥有广泛的行业专业技能并针对行业垂直挑战(包括保护业务流程)量身订造了安全解决方案。
- 我们一直在实践-我们管理着全球400,000名员工的安全和隐私，我们的服务团队每天为客户管理着超过70亿件安全“事件”。
- 我们用事实证明-IBM已提供IT安全超过30年。我们拥有200多个安全成功案例和50多个已发布的案例研究。
- 我们拥有生态系统-IBM拥有一个大型的业务合作伙伴社区，它实现我们的解决方案并为其提供补充。
- 我们可帮助您选择-IBM安全性服务评估人员可提供一个IBM和非IBM产品列表，帮助客户为您的环境创建最佳的解决方案。

更多信息

要进一步了解IBM如何帮助组织有效地管理风险和合规问题，完善安全状态，从而更好地实现业务目标，请联系您的IBM销售代表或IBM业务合作伙伴，或者访问:**ibm.com**/security。

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

在中国印刷
2011年11月

[1] deRugy, Veronique和Melinda Warren, "监管者预算报告:新内阁中的立法预算和员工安置费用继续膨胀，"
Mercatus Center, George Mason University, 2009年10月。
http://mercatus.org/publication/regulators-budget-report

[2] Tucci, Linda, "2010年治理、风险和合规开支继续增长，" SearchCompliance.com, 2010年12月1日。
http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html

[3] D´Antoni, Helen, "符合法规的安全，" Information Week, 2005年8月29日。
www.informationweek.com/news/securityshowArticles.jhtml?articleID=170100825

[4] "META Group Study 表示64%的公司拥有专门的合规性预算，" Business Wire, 2004 年7月26日。
www.thefreelibrary.com/64%25+of+Companies+Have+Dedicated+Regulatory+Compliance+Budgets,...-a0119745130

[5] Greiner, Lynn, "除安全性外，合规开支还提供了其他收益，" Network World, 2008年8月12日。
www.networkworld.com/news/2008/081108-compliance-spending-offers-benefits-besides.html

[6] 关于COBIT的更多信息，请访问
www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

[7] 关于ISO/IEC 27002:2005的更多信息，请访问
www.iso.org/iso/catalogue_detail.htm?csnumber=50297

[8] 关于ITIL的更多信息，请访问www.itil-officialsite.com/home/home.asp

[9] 2007年全球信息安全状态，与PricewaterhouseCoopers合作展开的一项CIO和CSO联合研究项目。
www.pwc.com/en_BE/be/publications/state-of-infsecurity-pwc-07.pdf

[10] "高管们表示数据量正在变得难以管理，" Government Technology News Report, 2008年8月5日。
www.govtech.com/gt/articles/385068

TIW14052-USEN-00