



一个关键的循规问题：数据传输的 安全程度如何？



2 执行摘要

4 对未能遵从的惩罚

4 来自公司的响应

5 数据分散，风险随处可见

6 超越 FTP：应用程序集成

7 Section 409 现已出台

8 一个令人畏缩的任务，一个可行的解决方案

9 保护灵敏度

10 将不同的系统链接到一起

11 事件探测和警告

12 从 FTP 进行简单的升级

13 一个关键的循规工具

执行摘要

“循规性”。就在几年前，这个术语还只是企业结构内一项深层次的业务职能。这些都已成为过去。

在今天的美国，循规性不再是一个任由公司私下里靠自觉意识实现的次要刺激因素。Sarbanes-Oxley 和其他政府规章纷纷出台，确保公司遵从性已经成为一项关键的任务。

当然，人们之所以越来越关注循规性词干，是由于近年来种类多变的企业犯罪所引起的——包括不清楚、不准确或完全不合理的公司财政状况报告，这些行为会给股东带来风险。

例如，为了恢复投资者、股东和大众对美国公司的信心，联邦和州的监管机构得到了大力发展，从而能够定义、利用和增强众多政府发起的公司循规性法案来保护公众利益。

当前的循规计划已经遍布许多地区和行业，集中在美国和欧洲的银行、保险和投资领域。当今所采纳的这一系列规章的雏形是 Sarbanes-Oxley Act of 2002，目标是美国证券交易所中的上市公司。

遵从性的其他主导因素

美国的政府监管不力并不是当今遵从性的惟一驱动力。全世界普遍存在将公司的财务报告实践标准化的迫切需求——特别是在欧盟内部，但在美国和欧洲之间也存在这种需求。这些是标准化公司报告财务状况的方式的主导因素，使公司能够彼此共享和沟通财务状况。另一个主导因素属于宏观经济级因素：渴望保证经济的稳定性和投资者对经济状况的信心。

但它也影响着美国以外的公司。例如，在英国，就有一家领先的银行正在投入大量资源确保自己遵守 Sarbanes-Oxley 法规。

同时，其他遵从性法案依然在不断涌现。影响欧洲银行的 Basel I 和 Basel II 将于 2007 年正式出台。Solvency Acts I 及 Solvency Acts II 主要面向保险业公司，将从现在起到 2007 年分阶段实施。2001 年后逐步发展起来的 CAD 3 对银行和投资公司管理资金和偿付能力的方式提出了要求。在欧洲，今年出台的 ISRS 是一项财务报告遵从性标准。

这些法规有一个共同点：它们都是用来追踪、管理和减少企业行为的各方面的风险元素的。

近十年来，企业面临的循规性问题浪潮产生了空前的影响——原因仅仅是政府监管机构拥有了前所未有的权力。当前的许多遵从性法案都是着眼于整体、意义深远的，涉及一系列跨企业方方面面的审查。

当今的循规性法案不仅对公司施加了一连串必需清除的障碍，还要求公司能够使用正当的措施快速扫除这些障碍。近来得到授权的政府机构正在提出强制性的最终期限——多数情况下为六个月。

对未能循规的惩罚

被推上法庭的可能性或许并不是管理层越来越关注遵从性问题的充分理由，还有另一个理由：未能循规可能对公司的股票价格产生负面影响。在循规性计划方面落后的公司将付出投资者信心降低、市场占有率减少的代价。为什么呢？当今，人们对公司的行为不当非常敏感——无论这样的行为是真实的还是想像的，市场将公司未能循规的现象视为一个信号，表示公司没有能力管理风险，也没有能力组织适当的资源来处理这些风险。

来自公司的响应

政府机构的强制要求、遵从性计划的广泛影响和潜在惩罚的严重性综合在一起，自然而然就促使公司前瞻性地实现遵从性。即使那些没有被法案直接作为目标的公司也意识到需要向顾客、提供商和股东证明他们拥有某些类似的实践，能够管理风险。

为遵从新法规，公司需要论证用于记录和管理为股东带来潜在风险的公司活动——以及影响公司财政状况的信息——的规程。

那通常需要在整个企业内实现新的或替代的流程。并且愈发要求对公司进行更彻底的改变，必须在企业内进行从上到下的、广泛的变革。

数据分散，风险随处可见

将您自己放到将要经受政府监管机构循规性审计考验的公司 CEO 或 CFO 的位置。政府团队需要审查您的业务和财政记录，以确保其准确性和完整性。

如果所有这些记录都驻留在中心位置的一台服务器上，那么这只是一次简单的演习。但实际情况并非如此，几乎所有大企业都趋向于成为分散的组织——投资于多年来分别构建的多个 IT 系统。这些异构系统在设计时并未考虑无缝协作，但其中都包含彼此关联的业务和财政信息。

为实现业务目标，这些单独的系统要交换数据，从而导致大量数据频繁在系统中移动。并且为了满足循规审计人员的需求，需要提供所有涉及业务和财政数据的财政方面数据交换的相关记录，且必须能够在这些数据交换发生和成功完成时进行检验。但是，当信息在系统间传输时，它们可能会被破坏或丢失、或者重定向到错误的系统。它可能会被不准确地复制或再现出来，从而导致冗余事件、活动等。



由于许多公司主要使用的依然是传统文件传输协议（FTP）数据传输技术，因此这些危害的影响被进一步放大。尽管 FTP 有着自身的优势，但是对于移动信息来说，它并不是最安全的方法。为填补其安全性缺口，许多组织已经创建了工作区，工作区带来的问题往往像组织意欲通过其解决的问题一样多。组织要使用内部编写的修复程序解了 FTP 技术的缺点。并且往往要采用不同程度的手工干预——指派专人打电话、发传真和电子邮件——以确保信息已传递。尽管这些权宜之计或许能使公司持续正常运转，但无法达到新循规性标准所提出的严格要求。

超越 FTP：应用程序集成

因为 FTP 文件传输技术对敏感财政数据来说不够安全，所以一种用来扩展或替代简单文件传输方式的全新、高度安全、逐渐普及的方法引起了人们的注意。这就是“应用程序集成”。

应用程序集成诞生于金融市场领域，原用做在金融机构、银行间传输和价值 10 亿或更多的高价值交易之间发布信息的方法。发展应用程序集成是为了保持传输中信息的安全性和完整性，确保信息在未被破坏、重复或丢失的情况下抵达预期目的地。

今天，应用程序集成是一个已经证明和广泛传播的机制，用于确保在信息在移动过程中的完整性。并且有越来越多的公司使用它来帮助满足循规性要求。



今天, 有越来越多的公司使用应用程序集成来满足循规性要求。

Section 409 现已出台

正在使用的应用程序集成是如何正确地促进遵从性呢? 例如, 即将出台的Sarbanes-Oxley 新法案——称为 Section 409——将是公司至今为止面临的最具挑战性的 Sarbanes-Oxley 要求。Section 409 要求组织透露可能影响公司财政表现的任何事件。这意味着公司必须证明数据的完整性, 并向股东承认和报告——实时地——公司内发生的任何财政实践或问题。遵从 Sarbanes-Oxley Section 409 要求改进整个企业内的数据流。他们必需证明系统到系统的通信是健壮的, 并且通信能够保证信息的准确性。他们必需能够显示紧密地控制了对传输中信息的审计追踪。当可能影响公司财务健康的异常事件发生时, 他们必需实时发出警告。

Section 409 要求企业分析其集成基础设施和文件传输机制，并修复这些系统来确保数据的完整性和准确性。许多公司已在积极筹备将高达三分之一的 IT 部门资源投入构建计划，来满足 Section 409 要求。

Section 409 只是一个单独的佐证。由于越来越多的循规性法案开始实施，对公司来说，应用程序集成是促使数据传输方法顺利通过遵从性审计的方式。

一个使人畏缩的任务，一个可行的解决方案

毫无疑问，对许多公司来说，满足循规性项目有关的全部规模和技能是使人畏缩的。许多已在早期开展此项目的企业也低估了这项工作所需的时间和工作量。这样的失误导致企业普遍将循规性理解为 CFO 和负责财政报告的员工应该处理的问题。它影响到公司内创建财政报告所用信息的每个领域。

为了使用应用程序集成技术更新自己的 IT 系统，从而应对遵从性问题，许多公司正在寻求外界的帮助。大部分公司都找到了 IBM。

当前最有效的应用程序集成解决方案之一是被称为 IBM Web Sphere[®] MQ Version 6 的中间件产品。使用比 FTP 更可靠、更安全的技术来交换文件和数据，这个 IBM WebSphere 中间件产品组合中的一员能够帮助公司树立信心，使他们有能力在企业内外完整地传输敏感信息。

保护敏感的信息

用于可靠、完整地连接应用程序的事实标准是 WebSphere MQ Version 6。它能够使不同的系统以一种能够维护数据完整性的方式互相通信。它也担当了一条可靠的和健壮的总线，可以将公司数据放在上面，然后灵活地定位到需要接收数据的公司部门。

WebSphere MQ Version 6 使用数据传输层提供了一个组织——不同于普通的、自主开发的 FTP 方法——当数据在企业内流动时帮助保存其完整性和准确性。公司不必担心消息在应用程序间交换时会丢失数据，因为数据是安全地和精确地进行交付的。进而帮助减少数据可能被破坏的风险。在诸如财政声明、循规性报告和其他至关重要的公司信息等文档中，这是非常有价值的收益。

使用 Web Sphere MQ Version 6，应用程序可以有效、间接地进行通信。作用类似于“用于应用程序的语音邮件系统”，它管制信息流、在队列中保留信息，直到有适当的应用程序可以用来交付。借助无与伦比的可伸缩性、群集和模块化，它使无人职守操作变得可靠和可审计。

由于数据安全和保密是任何循规计划都极为关注的内容，Web Sphere MQ Version 6 包括了 SSL (Secure Socket Layer) 加密，这使信息能够被加密到一个极为安全的程度。（对于那些需要更加复杂的安全性的公司，IBM Web Sphere MQ Extended Security Edition 提供了对保密和不可否认性的额外支持。）



WebSphere MQ Version 6 一个最有价值的好处是，它能够确保信息到达它的目的地。此外还提供了“精确地一次性交付”——确保了文件已经向接收者交付了一次且仅交付了一次。这个安全措施帮助防止过度分配和滥用信息。精确地一次性交付减少了协调那些在系统间被破坏的或复制的公司信息的需要。它也使不同的系统能够在这些系统不可用的时候进行通信。

WebSphere MQ Version 6 对遍及企业的信息移动提供了全面的日志和追踪支持。它还有一些特性可用于平衡那些贯穿公司的信息移动，来确保信息尽快到达。这对于诸如 Sarbanes-Oxley Section 409 这样的循规性所提出的实时信息报告要求是特别重要的。

将不同的系统链接在一起

收集财政信息来实现循规性目的的一个通常的阻碍是，大量的信息驻留在不同操作系统的众多服务器上。这种多样性给协调这些机器在创建和存储系统数据时所采取的不同方法带来了很大困难。

WebSphere MQ Version 6 通过集成这些不同的平台和操作系统克服了这些系统差异。它使公司能够集中精力弄明白需要发送哪条信息，而不是以哪种机制来发送信息。支持超过 85 种不同的平台配置



——包括对 Java Message Service (JMS) Application Programming Interface (API) for Java™ 和 Message Queue Interface (MQI) API 的集成的支持——它提供了应用服务器和其他应用程序之间的无缝集成。由于这个原因，它可能正是典型组织一直需要的那种唯一的安全消息传递解决方案。

Web Sphere MQ Version 6 使用大量现有和新兴的技术对人们连接应用程序提供了 IT 级别上的支持。这包括诸如 C 和 Java 等语言，以及一种称为 Web 服务的灵活技术。

事件检测和警告

Web Sphere MQ Version 6 保证了数据的完整性和安全性，同时另一种 WebSphere 产品可检测那些能够对公司产生实质性影响的事件——从而相应地向各主要方面发出警告。

IBM WebSphere Business Integration (BI) Message Broker 使您能够预定义业务规则，来检测发生在企业内的重要事件，并且在事件发生时触发自动警告。这种能力可帮助公司减少财政和资产风险。例如，如果潜在的顾客有坏账，可以使用业务规则来配置 WebSphere BI Message Broker，以检测这种情况并自动判断通知哪个人。

另一个例子是：在金融行业，通过分析特定的交易模式可以发现欺诈性交易。可以预定义公司规则来确定这些模式，然后在检测到欺诈性模式时向 CFO 发出红色标记以示警告。然后公司即可采取一些措施来保护自己免于受到可能的欺诈。

WebSphere BI Message Broker 可以帮助公司克服在将信息交付到所有公司系统时，转换或改造信息所遇到的信息格式方面的困难。这就提供了一种连接系统的灵活方法，制定技术和投资决策的时候无需担心会给链接这些系统增加困难。

WebSphere BI Message Broker 继承了 WebSphere MQ Version 6 的所有特性，可保证整个企业范围内移动的数据的完整性和安全性。

从 FTP 进行简单的升级

对于那些当前使用传统 FTP 连接的公司，WebSphere MQ Version 6 提供了一种快速的、简单的方式来迁移到更高级、更安全的传输方法——那就是系统集成。它提供了一个简单的界面，使 FTP 驱动的 IT 部门能够使用文件传输图形化界面来随意地移动信息。所以，如果 IT 人员习惯使用 FTP，他们也能够使用类似的文件传输工具和观念，经由可靠的 MQ 基础设施来交换文件。结果，IT 组织可以以一种渐进的方式构建一个 MQ 基础设施或网络，从而根据公司需求升级或取代 FTP 及其他连接应用程序。WebSphere MQ Version 6 创建了一个分布式——但完全集成的环境，用来移动信息。此外，通过使用 WebSphere MQ Version 6 FTP 脚本命令，可以使已自动化的文件传输系统轻松地得到增强。这就使 FTP 命令能够被自动发送和接收，并能够经由 WebSphere MQ 网络自动传输文件。

WebSphere MQ Version 6 更新提供了可与其他 WebSphere 产品无缝交互的开箱即用消息传递。因此，在 J2EE 技术上进行了投资的公司，已经准备访问同 WebSphere MQ 进行互操作的集成的消息传输。这意味着您可以创建一个通用的总线机制，在 Java 和非 Java 环境中安全地传输数据。

此外，IBM 转售一种称为 PM4Data 的产品，它来自 IBM 宝贵的业务合作伙伴 CommerceQuest。该产品能够为公司触发文件系统在 WebSphere MQ 内的移动提供更高级、完善的帮助。

一个关键的循规性工具

由于企业竭尽全力来遵从法规的要求，处理来自企业高层的压力，来确保达到并保持了循规性，并认识到未能循规的处罚的严厉性，因此或许企业不会认为循规性是一件好事。但这它可以是一件好事，因为有了遵从性的 IT 计划可以增加公司的灵活性和 IT 基础设施的弹性。它也能帮助公司更好地利用公司信息并增加在市场中的竞争优势。

应用程序集成不仅给公司提供了利用新的和现有投资的好处，还创建了一个更加实时的、面向事件的和集成的企业。可以帮助公司以一种按需应变的形式来应对压力、威胁和机会。



若想了解应用程序集成如何帮助您解决循规性问题的更多信息，请联系我们的某位专家，专家可与您共同探讨降低和管理数据移动风险的实际方法，比如：

- 使用 *JMS* 标准化消息传输
- 使用 *SSL* 来加密并安全地监控数据以确保完整性和保密性
- 准确地审计和报告流程和单个消息

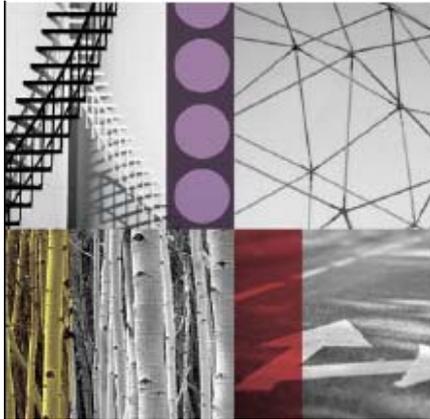
请咨询您的 IBM 代表，获得关于 **Information Risk** 和 **Readiness Assessment** 的信息，了解您的信息是否存在风险。此评估将帮助您理解业务流程所处的状态，您的数据是否存在风险和哪些附加流程可降低风险。您将了解：

- 数据存储在哪里
- 谁有权访问这些数据
- 现有哪些规程用于处理数据丢失
- 数据如何移动
- 如何在流程间共享信息

如需了解更多信息，请访问

ibm.com/websphere/applicationintegration/compliance。

为符合当今政府的循规性要求，组织需要证明其拥有健壮、准确、系统到系统的通信，并保证其数据能够在整个企业内流动。许多企业已意识到，**FTP** 技术不足以完成这些任务，它们正在转移到应用程序集成所提供的增强的可靠性和安全性。在此过程中，它们发现了用于高度安全信息传输的事实标准：**IBM WebSphere MQ Version 6**。



每个用户都负责确保自己遵从特定于它的公司和从事领域的法律和法规，包括 (但不限于) Sarbanes-Oxley、Basel II 和其他循规性法律和法规。

产品用户的唯一职责是寻求并获得优秀法律顾问的建议，来鉴定和解释任何相关的法律和法规。而这些法律和法规可能影响用户的公司和用户为遵守这些法律和法规所需的任何行为。

IBM 不在任何法律、审计或会计方面建议、表示或担保其产品或服务将确保任何获得许可的产品用户能够遵从任何特定法律或规范。



© Copyright IBM Corporation 2005

IBM Corporation

Software Group

Route 100, Building 1 Somers, NY

10589 U.S.A.

Produced in the United

States of America

06-05

版权所有。

, IBM、IBM 徽标、
WebSphere 和 zSeries Business
Machines Corporation 在美国或其他
国家的商标或注册商标。

Java 和所有基于 Java 的商标是
Sun Microsystems, Inc. 在美国和
其他国家的商标。

其他公司产品和服务名称可能是
其他公司的商标和服务标志。

本文所提到的 IBM 产品或服务
不代表 IBM 将在所有设有 IBM
分支的国家内推出。 .

可以通过 Internet 浏览 IBM 主页

ibm.com.

G507-1318-00