Microsoft SQL Server

2008 安全

Microsoft SQL Server 2008 安全

虽然改进的过程很艰辛，但是 Microsoft SQL Server 2008 比 2005 和 2000 更安全了。保护业务的关键是数据库安全。组织、企业、互联网、以及应用程序对数据库的依赖程度从来没有如此之高。毕竟，现在有什么数据不是存储在你的后端数据库中呢！微软的 SQL Server 2008 是在八月六日发行的，由于对其它性能、功能和安全特性的高需求，2008 上市的速度比继 2000 版之后的 SQL Server 2005 快得多。而且，微软在三个方面面临着强大的竞争：传统的数据库技术、网络应用程序平台、和开源社区。

SQL Server 2008 的安全总述

但是 Microsoft SQL Server 2008 比 2005 和 2000 更安全了。Microsoft SQL Server 2008 保护业务的关键是数据库安全。组织、企业、互联网、以及应用程序对数据库的依赖程度从来没有如此之高。毕竟，现在有什么数据不是存储在你的后端数据库中呢！与其先前的产品相比，Microsoft SQL Server 2008 最显著的变化是其精密的数据安全性能：加密、密钥管理和增强元数据的安全性。

- Microsoft SQL Server 2008 安全性提高（一）

SQL Server 2008 的认证机制和功能

SQL Server 2008 支持五中认证机制：基本认证（Basic Auth）、NTLM、分类认证（Digest Auth）、Kerberos 和综合认证，综合认证实际上就是 Kerberos 和 NTLM. 的结合。此外，SQL Server 2008 支持五中认证机制：基本认证（Basic Auth）、NTLM、分类认证（Digest Auth）、Kerberos 和综合认证，综合认证实际上就是 Kerberos 和 NTLM. 的结合。

- Microsoft SQL Server 2008 安全性提高（二）

- Microsoft SQL Server 2008 安全性提高（三）

SQL Server 2008 的加密和简化

SQL Server 2008 为全文数据库、矩阵和以职能为基础的加密提供本地支持。密钥管理也已经完全更新。SQL Server 2008 提供了不同形式的加密技术，这是密钥管理的一个内部系统。SQL Server 2008 为数据库的审核等功能，使数据库管理员和安全管理员的工作更轻松。

- Microsoft SQL Server 2008 安全性提高（四）
- Microsoft SQL Server 2008 安全性提高（五）

SQL Server 2008 与法规

SQL Server 2008 较之前的 2005 和 2000，在加密和认证机制等方面有了重大的提高，但是在企业中，各种法规对 SQL Server 2008 提出了怎么的要求？SQL Server 2008 如何遵从法规的要求呢？

- Microsoft SQL Server 2008 安全性提高（六）
- Microsoft SQL Server 2008 安全性提高（七）
- Microsoft SQL Server 2008 安全性提高（八）

Microsoft SQL Server 2008 安全性提高（一）

虽然改进的过程很艰辛，但是 Microsoft SQL Server 2008 比 2005 和 2000 更安全了。

保护业务的关键是数据库安全。组织、企业、互联网、以及应用程序对数据库的依赖程度从来没有如此之高。毕竟，现在有什么数据不是存储在你的后端数据库中呢！

微软的 SQL Server 2008 是在八月六日发行的，由于对其它性能、功能和安全特性的高需求，2008 上市的速度比继 2000 版之后的 SQL Server 2005 快得多。而且，微软在三个方面面临着强大的竞争：传统的数据库技术、网络应用程序平台、和开源社区。

Oracle 公司一直几乎每年都发行新版本的数据库，专门为小型行业、企业、联机、以及政府而设计的。Sun Microsystems 公司收购了 MySQL，已经一跃成为数据库市场的一个新的竞争者。MySQL 收购后的可靠性已经成指数形式增长。这与加强的支持、文件证明、许可、以及服务选项相结合，将不可避免地为大公司带来更多的问题。

人们对数据库技术的新误解是，认为那些新的成功的网络公司正在开发平台，采用主机和应用程序逻辑来支持这些平台，比如数据库。Salesforce.com(应用程序交换)、Amazon（EC2）、Google（应用程序接口）和印度发电站 Zoho 在分布式平台市场都有相应的产品。

对微软社区来说，好消息是：SQL Server 2008 中的安全特性是经过深思熟虑设计，并且是合理实施的。到目前为止，与其先前的产品相比，最显著的变化是其精密的数据安全性能：加密、密钥管理和增强元数据的安全性。尽管基于功能的权限并不是新产生的，但是增强的灵活性却提供了对数据库更多方面更紧密的控制。在过去，发行的访问量多于必需的访问量，这样的时代已经一去不复返了。

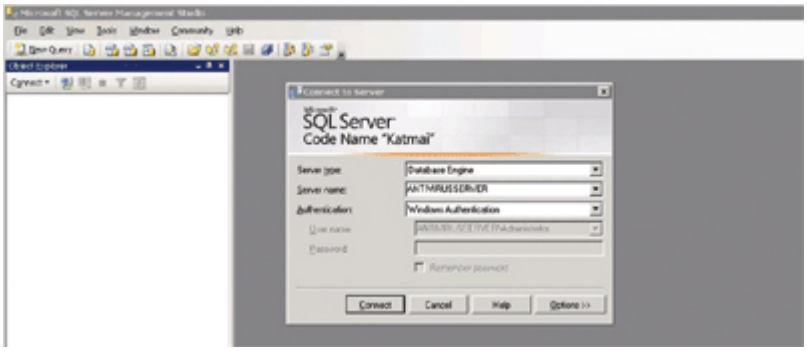
（作者：James C. Foster 译者：李娜娜 来源：TechTarget 中国）

Microsoft SQL Server 2008 安全性提高（二）

你是谁？

SQL Server 2008 提高了认证模块的安全性，以此为战略和实施标准，微软公司顺应了市场的需求，取得了巨大的成功。在这样一个时代，基于网络的蛮力攻击是常有的事，微软公司意识到这个时候应该对 SQL Server 2000 中的基本性能进行更新，而这些更新在 2005 中又没有得到完全解决。（见下面所示的截图）

登录



SQL Server 2008 支持多种认证机制。

你仍然可以利用 LDAP 和 Active Directory 的投资，进而以一种安全的方式登录到 SQL Server，但是，现在与非 Windows 客户端的结合支持全信道加密技术。在默认的情况下，全信道加密采用 SQL 生成的 SSL 证书，几乎可以防止所有的即开即用的中间人攻击。

全信道加密也可以确保 SQL 语句所传输的用户名的安全，以及其它任何有效载荷详细信息的安全。

与 2005 版中所默认的用户名和密码哈希相比，这是一个重大的成就。

对于微软群组原则（Microsoft Group Policy）工作室而言，事情也可以变得更容易一些。现在，你可以通过群组原则物件（GPO），来为所有 SQL Server 2008 的数据库管理并且加强密码的对象属性：比如终止日期、锁定时间、使用年限和锁定目的。虽然你可以通过本地基本的 Windows 操作系统来管理 SQL Server 2005 的基本组件，但是，现在你既有能力管理操作系统，也有能力管理所覆盖的 SQL 服务器。

虽然这些性能会有助于与蛮力攻击问题进行作战，但是编码来为一个账户解锁是相当简单的。在这个一体化之前，大多数数据库管理员并没有合理地设置密码策略，来提醒、或者甚至锁定系统管理员或者数据库管理员账户，即使多年以来，这是一种系统管理员常见的做法。GPO 密码策略的一体化也关闭了这个循环。

在因特网上受到了很大影响的服务或者 SOA 认证，现在得到了显著的改善。SQL Server 2008 支持五中认证机制：基本认证（Basic Auth）、NTLM、分类认证（Digest Auth）、Kerberos 和综合认证，综合认证实际上就是 Kerberos 和 NTLM. 的结合。

SQL Server 2008 也提供了这样的性能：能够用数字证书来标记编码模块。通过提供对表格和其它对象的精细访问，这个性能也适用于存储的程序、函数、触发器，以及甚至是事件通知、简化的权限管理。其实，你可以分配权限来对模块进行编码，并且仅允许用户访问外露的登录点，但不能访问基础的系统配置。

标记编码模块为防止未经授权的变更带来了更多的便利。这两个用例都增加了一个深度防御的设计，用以提高整体的安全性。

（作者：James C. Foster 译者：李娜娜 来源：TechTarget 中国）

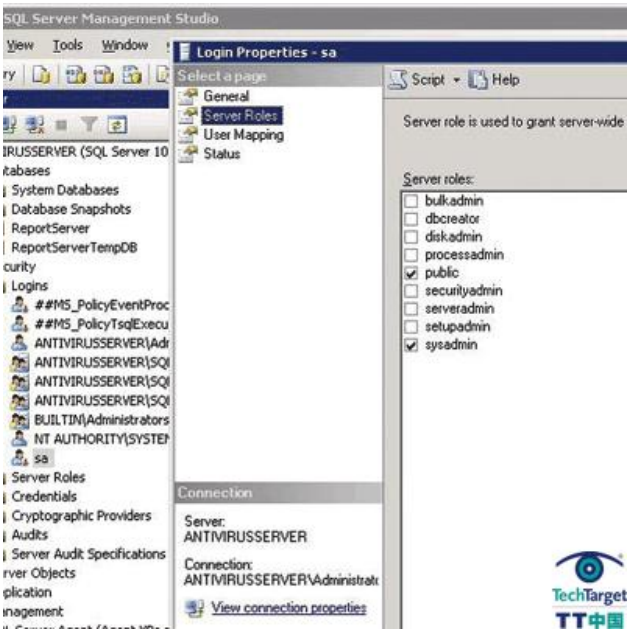
Microsoft SQL Server 2008 安全性提高（三）

有特权的实体

SQL Server 2008 引进了许多全新的、精细的控制机制，以确保合理地创建、分配、执行这些权限，而且比前几个版本的误差更小。

公共职能。虽然大部分以核心职能为基础的访问性能都与 SQL 2005 保持相似，但是同时也包含附加的功能来帮助以网络为基础的应用程序软件盒，并且防止匿名的因特网攻击。创建一个新的公共职能，微软已经有了很大的提高。通过 SQL 2008 服务器的默认值，每一个数据库用户被自动添加到该组（职能与组的类似，但是还拥有以数据库和应用程序逻辑与功能为基础的相关特权和访问权限）。创建这个公共职能，可以约束因特网用户，并限制所有类型的访问（见下面的屏幕截图）。

公共职能



在 SQL Server 2008 中，默认指派所有的用户为公共职能，这是一个限制因特网用户访问权限的好方法。

元数据保护。数据库或者表格的元数据和其本来的数据同样重要。比如，如果我可以接到这样的证明：某个数据库中存在一个表格或者特定的矩阵，那么我就可以得出结论：这是 SQL 攻击的一个很好目标。SQL Server 2008 允许你通过以用户分配的职能为基础的错误响应来保护这个元数据。因此，举例来说，如果所有的因特网用户都处在公共角色之中，并且其中一个用户在没有正当权限的情况下，试图访问或者甚至删除一个名为“SecretSauce”的表格，那么就会返回下面的响应：

不能删除表格“SecretSauce”，因为不存在这个表格，或者是由于你没有这个权限。

更精细的 schema。SQL Server 2008 中的突出之处是实施了以 schema 为基础的数据库安全及其文本。2008 版之前，SQL Server 通过采用某个用户进行逻辑配对，进而处理了一个 schema。当你在 SQL 2000/ 2005 中创建一个新的用户时，其间也创建了一个 schema。然后，这个用户得到了许可，这些许可就好像他自己的一样。现在，你必须创建一个用户，然后再创建或者分配给他一个特定的 schema。这个用户获得了一个或者几个 schema 的拥有权，而且，然后这个 schema 分配不同的权限到数据库得基本元素中。这个额外的数据库层允许你为用户和数据库元素设置更精细的许可和控制。

对象的分离允许某个单一用户创建并实施几个与 2005 版相对的 schema，在 2005 版中，需要用到多个用户帐号。因此，可以潜在地减轻安全管理的负担。

可获得的对象。2005 中引进了可获得的对象，SQL Server 2008 就是建立在这个理念的基础上的。被认为是主要功能的登录和服务可以划分为多个组分，将更精细的许可授予数据库中、表格中的几乎每个对象。这个以职能为基础的或者许可的精细度是数据安全性方面一个大的提高，这个很好地对公共职能进行了补充。在服务器的终端，提供了控制，进而限制通过网络信道、命名的传输管道以及其它通信信道的通信。

通过许可设置，可获得的对象就可以连接到主要功能之中。虽然许可继续使用 GRANT、DENY 和 REVOKE，来定义某个功能的许可，但是现在，你可以再向前走一步，允许主要功能对其它功能授权，使这些功能可以访问受到控制的信息。

代理服务器。SQL Server 的代理服务器连接到用户证书和工作许可。这就提供了一种精细的方法来为任务中每个单独的步骤授予许可。这是与先前的版本形成鲜明的对比：先前的版本使用一个单一的，通常是全面的功能强大的代理器账户。每个子系统可以拥有任意数量的相关代理器。

这里有一个特例：只有经过模块主人的许可，Transact-SQL 子系统才可以运行。比如，如果拥有者是“Foster”，那么只有在 Foster 设置的特权下，才能执行所有的 Transact-SQL 语句。

重要的是要注意到，当从 SQL Serve2005 升级到 SQL Server 2008 时，单一的代理器帐户将会继续保留到新的版本中。应当做出仔细的考虑，决定如何分割帐户，以及如何合理地限制权限。

（作者：James C. Foster 译者：李娜娜 来源：TechTarget 中国）

Microsoft SQL Server 2008 安全性提高（四）

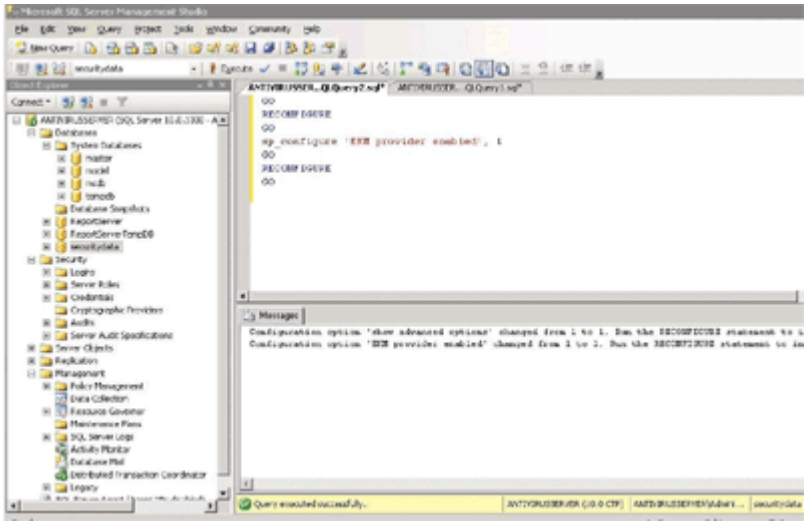
加密是关键

好消息：几年前，你购买了另外一些补充的数据库加密产品，停止为这些产品的维护支付费用，回到原来遵守 PCI 规定的产品，会让你倍感轻松——如果你在一个微软数据库的工作室的话。不幸的是，所有这些新的技术和管理性能仅适用于微软的数据库（没有 MySQL 和 Oracle 的综合管理性能）。SQL Server 2008 为全文数据库、矩阵和以职能为基础的加密提供本地支持。密钥管理也已经完全更新。

SQL Server 2008 提供了不同形式的加密技术，这是密钥管理的一个内部系统。过去，加密密钥管理基本上是由外部的第三方产品处理的，这是因为 SQL Server 缺少适用的用户管理。

外部密钥管理（EKM）可以保护来自存储在任何现有网络服务中一切数据，以及访问数据库本身的数据。此外，KEM 使得外部和第三方产品能够结合在一起，并且在 SQL 服务器中注册设备。这些设备可以使纯软件产品，也可以是“硬件设备”，比如以硬件为基础的 SSL 加速器。在 SQL 服务器中注册过的设备允许应用程序和用户访问，并允许使用其加密密钥（如下面的截图所示）。

外部密钥管理（EKM）

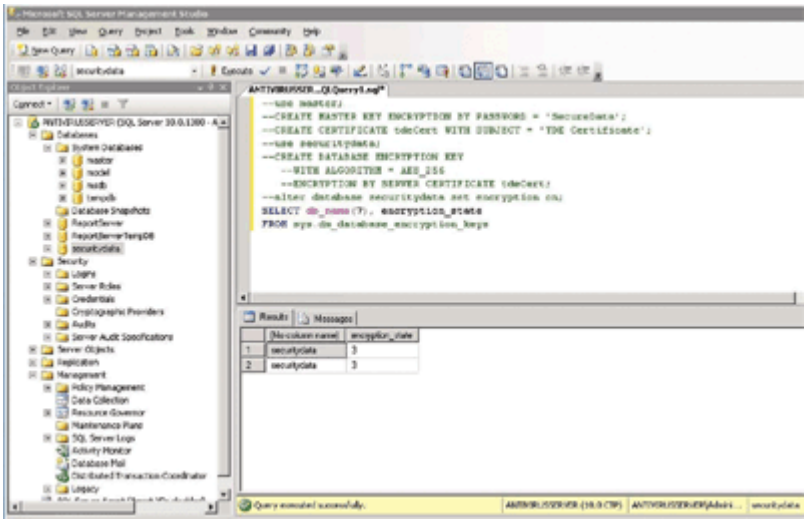


（SQL Server 2008 改善了加密、保护数据和网络服务、以及与第三方密钥管理产品的合作，可扩展的密钥管理（EKM）是所有这些性能的核心。）

通常情况下，联邦政府和大型的电子商务组织使用这些服务，比如那些来自 nCipher 和 SafeNet 的服务，这些服务使用先进的密码术特性，对密码替换时间表和密码年限方面的策略进行设置。当这些产品自动操作旋转密码时，即使在很小的几率下，某个特定的密码受到威胁，旋转密码也可以确保数据受到保护。SQL Server 2008 也完全支持硬件安全模块（HSM）。

最近的产品也引进了透明数据加密技术（TDE）（见下面的截图）。首先，插件程序是唯一的真正加密选择。SQL Server 2005 为加密矩阵引进了一些本地支持，而且 2008 版也已经显著的提高了这一性能。

透明数据加密技术（TDE）



（透明数据加密(TDE)技术可以对整个数据可进行加密，同时也能对日志进行加密。）

透明数据加密技术（TDE）是一种完全的、可控制的数据库加密技术。透明数据加密技术（TDE）可以加密整个数据库，以及所有相互影响的数据和日志数据。对管理员而言，TDE 是的一个轻松的选择，可以确保数据受到保护，而不会影响数据库的结构。使用先前的版本时，应用程序开发者频繁地创建了自定义的编码来对数据进行加密和解密。然而，有了透明数据加密技术（TDE），当把数据写到磁盘，或者从磁盘读出的时候，这些功能可以自动起作用。这就消除了开发者多余的工作，并且加强了所有数据的安全性。

透明数据加密技术（TDE）的灵活性和保持优点可谓来之不易。在使用率较高的系统中，CPU 性能对服务器和数据库的影响程度可以达到两位数的百分点。

筹备数据库很简单。改变数据库的指令必须由数据库管理员来运行，具体内容与下面的指令类似：

```
alter database is_mag_db

set encryption on
```

```
go
```

SQL Server 2008 拥有即开即用的功能，可以进行对称加密、不对称加密、以及以证书为基础的加密，满足任何包含在微软密码库中的标准。

（作者：James C. Foster 译者：李娜娜 来源：TechTarget 中国）

Microsoft SQL Server 2008 安全性提高（五）

简单的审核

传统上，管理员所面对的最大挑战之一一直都是审核数据库。问题的核心在于数据库的目标。为一个控制的应用程序或者出于特殊目的而处理并存储大量的数据，这样的工作需要一个熟练的工程师来完成。问题是你如何验证那个数据就是用于实现其本来的目的，而不是出于一些带有恶意的意图。

为了审核前面版本中的数据库，管理员不得不在不同的数据点，启动多个触发器和警报，以记入日志，并稍后进行结果分析进而确定不规则的数据点。SQL Server 2008 简化了这一程过程。某个审计员或者管理员需要对审核的数据点进行定义（比如，用户的行为、数据的要素、用户或者职能），然后在服务器上创建服务器审核或者数据库审核的技术说明。从那里可以采用 SQL Server 2008 Management Studio 中的 Windows 事件观察器或者日志观察器来检查事件。

虽然，完成审核与日志性能的配置需要几天的时间，但是，灵活性允许你将详细的、适用的日志结合到第三方的解决方案中。

对 比

SQL BY THE NUMBERS

Each version of SQL Server has become more secure through improvements in key features.

Feature	2000	2005	2008
Default install–secure by default	2	4	4
Reduced attack surface (options installed, but disabled)	2	3	3
Automated system configuration analysis	1	1	5
Automated updates and patches	3	3	3
Enterprise database management	3	3	4
User authentication	2	3	4
Password policy enforcement	2	3	4
Endpoint authentication	2	3	3
Role-based permissions	2	3	4
Custom permission sets	2	4	4
Quantity of securable objects	2	3	4
Meta data security	2	2	5
Agent proxy control/flexibility/permission	2	2	4
Execute context and/or ownership chain	2	3	4
User/schema separation	1	3	3
Data encryption	2	2	5
Key management	2	3	5
Code module signing	2	3	4

SCALE

1 Not Supported
2 Partially Supported
3 Full Support
4 Highly Competitive
5 Best of Breed

生活更轻松

构建了顶端产品，而且包含微软可信赖计算计划（Microsoft Trustworthy Computing initiative）在内，经过默认设置和设计的 SQL Server 2008 更安全可靠。与 2005 相似，SQL 2008 中的几乎所有的组件和模块虽然都可以安装，但是，都被默认关闭

了。仅运行需要的组件和模块，这一方法有效地减少了攻击层面——层面越大，受到威胁和攻击的机率就越大。

为了帮助数据库管理员和安全管理员，微软已经更新了 Surface Area Configuration Tool。有了小而简单的 Win32 GUI，你可以轻松地中止使用过的 SQL Server 服务、协议、连接和端口。Win32 GUI 已经经过升级，可以支持新版 SQL 的所有性能。

虽然这是一种实现安全的坚固方法，但它同时也给数据库管理员（DBA）在安装过程中带来了额外的工作。声明管理框架-工作（DMF）是一个新的工具，它对此会有所帮助。这是一种通过一个安全的通信信道来管理初始配置 SQL 服务器的一个或几个步骤的方法。可以配置几个策略、组件和模块。对于管理诸如 clusters 系统和 failover 系统之类的极其相似的系统而言，这是一个相当不错的机制。

在每次叠代过程中，SQL 服务器已经显著地获得了更高的安全性。2005 版的发行就是一个必备的升级，SQL Server 2008 也不例外。

如果你为全球制药分销商、大型数据的提供商、或者一个小城市负责安全、风险管理，和/或规则遵守方面的工作，那么你就既要遵守联邦规则，又要遵守行业规则。

规则从每个方向都在攻击你。无法达到诸如萨班斯？奥克斯利法案（Sarbanes-Oxley）和国家数据破坏通知法案之类的联邦和国家的要求，就会威胁到公司品牌的声誉和执行官的个人自由。达不到诸如健康保险可携带和责任法案（HIPAA）、PCI、公平信用报告法案（Fair Credit Reporting Act）之类的行业要求，或者得不到国家执法资格认证，这会导致你所在公司进行业务的能力和客户的个人身份信息处于危险之中。

作为一个信息安全和风险的专家，在过去五年中，你的视野之内已经是一个日益规范的商业环境。框架、审计、自动化和 GRC，这些都是你所处的环境。

此处不再赘述。

Forrester Research 公司安全与风险管理实践的资深分析师 Marc Othersen 说：“你不想从事的工作就是执行或者测试相同的三、四、五倍的控制。

因此，如果没有大规模重复的努力，企业该如何管理多项规章制度呢？是否能有一个包罗一切的框架，可以满足所有的重叠部分？

服务于三个不同市场的三家企业正在建立其遵守“简单按钮”的版本，利用大量的资源来创建一个可重复的流程，以满足脾气极其暴躁的审计员的需求。

（作者：James C. Foster 译者：李娜娜 来源：TechTarget 中国）

Microsoft SQL Server 2008 安全性提高（六）

改进的萨班斯法案（SOX）引导的方式

John Sapp 是 McKesson 公司的高级管理员，主要从事 IT 管理、风险与规则遵守，同时也是国家最大的制药分销商。他说：“我们创建战略的方法绝对会是包罗万象的，要么遵守规则，要么遵守我们的内部策略。基本上，首先建立大的图像，然后，决定我们将如何实现它，并确保我们从事这项工作的方式允许我们能真正的做到跨企业的综合，同时又要脱离我们通常所见到的分散的做法。

McKesson 公司 2008 年的财政年度收入是 1071 亿美元，关于遵守萨班斯-奥克斯莱法案，该公司有一个成熟的程序，并且这是 Sapp 模型和其团队正在遵循的程序，用以构建一个一站式企业范围内的遵守程序。

Sapp 具有开发和项目管理的背景，他称财富 500 强中有很多企业想要制定一套可重复的流程来处理规则遵守问题，而他的组织与大部分这些企业不同。他已经采取措施来确定并了解 McKesson 公司的 IT 环境，制订对控件的测试，并使之自动化，评估并报告风险，提高组织风险和规则遵守程序的整体成熟性。他说，现在，McKesson 处于一个特定的状态，向着可重复性迈进，并最终实现进程的标准化，同时优化进程。

Sapp 说：“在三年内，我期望我们能处于一个标准化的状态，这对我而言，就是让我们达到这样的状况：我们拥有一套标准、进程和控件，可以始终如一地普遍适用于不同的企业，并能够进行优化，我们能够真正地获得即插即用的环境，即：无论我们获得了什么产品，我们都可以插上电源使用，或者如果我们选择卖掉某个企业，这个环境可以使我们轻松的处理这个过程。

作为 McKesson 公司以前风险服务方面的高级顾问，Sapp 是 SOX 企业部门的协调管理人员，主要负责 SOX 法案项目的 IT 控制。接触到了更广泛的职能以后，他很快发现了

McKesson 公司的众多收购是如何创造了这样一种环境的，在这个环境里，公司是分散操作的，根本没有采用标准化的程序或者生命周期的方法来处理规则管理的工作。他的目标很快便很明确：克服分散的做法，建立一个项目，可以允许他通过这些活动来促进公司的运行。

McKesson 公司的 SOX 项目利用了 ISO27001 标准，来进行信息安全管理；并且采用了 COBIT 框架来进行 IT 管理和计量。

Sapp 说，虽然他的组织已经配置了 Brabeion GRC 套件，但是他相信不同工具的结合将最终满足 McKesson 公司的需要。他正在评估几种其它类型的 IT GRC 工具，会帮助将多个规则（比如 PCI 和 HIPAA）添加到这些框架之中。SOX、PCI 和 HIPAA 是 McKesson 公司的三个最大的规则遵守问题。此外，该公司用于财政方面的 SAP 环境，是人们关注的主要领域。

Sapp 说：“我们发现许多类似的规则，ISO 中的一条规定可以满足每条这些规则中一些部分。”比如，访问控制就是每条规则的补充。“只要满足其中一项 ISO 的条款，ISO 就允许我们在不同的规则中使用同一项条款，并且确保是正确的。我可以测试一次，并且可以进行多次确认。如果我正在每项规则中使用相同的访问控制程序，那么接下来，我就可以减少测试的次数。这就是采用我们的 SOX 项目，我所能做到的。由于我们已经大大地改善了我们的程序，因此我可以彻底的减少在审计上所花费的时间。我们已经完成了审计，这个时间我称之为创纪录的时间，也在我们的预算之内。”

Sapp 希望，他现在所评估的 GRC 工具会进一步脱离繁琐、费力的手工过程，来从企业部门中收集数据、测试、并将控件与特定的规则相对应。随着 200 多个控件可适用于 SOX 项目，Sapp 说，这是采用 Brabeion 工具实现自动化的第一个目标。

他说：“我们期待有一个自动化的工具，能够帮助我们测试这些控件，指认证据，并防止用户跳转到下一步。我有一个用户告诉我，我们已经改善了这里的生活质量。虽然，在自动化之前，我确实使用了 SharePoint，但是，你获得了这些工具，工作量并不在于此。”

Sapp 指出，他说看到的 GRC 工具在界定某个组织的资产和法人方面，做得相当出色。他说，他们一致赞成对工作流程进行分析，并创建附属的流程；这种信息也可以用于 GRC 以外的工具。他补充到，这个工具可以正确的收集资产的信息（比如，确认不受支持或者过期的软件版本），这在风险评估过程中有帮助。最后，他指出仪表板设施是一种强有力的方法，所提供的风险图片，可以达到 C 级。

他说，与此相反，一些工具虽然试图做很多工作，但是做得并不是很好。这些产品被宣传为一切齐全、即可使用。由于工作重点被误导了，因此，整个企业的 GRC 项目有时会遭受运行不好的工作流程。Sapp 说：“厂商主要是出售工具，而不是让你退回去，查看进程和策略。他们最先考虑的不是进程和策略，他们把这项工具调整的任务丢给你，并且声称这可以解决你所与的问题。”

Forrester 公司的 Othersen 说，在这些处于其核心地位的工具很好地遵守了规则，指出来源，自动进行人工测试，并提供可靠的报告。它们的失败之处在于没有将 IT 风险与行业风险挂钩。

Othersen 说：“在风险引擎方面，它们没有商业前景。这些工具都集中处理 IT 方面的问题，但是大部分风险都是与业务一起发生的。如果你遗失了信用卡号码，相关的行业将支付损失，而不是 IT 行业支付。将 IT 控制失误转化为行业风险，这是这些产品的最大弱点。

他补充到，他们也不需要解决治理。“作为一个首席信息官（CIO）或者安全经理，应该由你自己来决定使用这种工具进行收集和分析数据”。

（作者：James C. Foster 译者：李娜娜 来源：TechTarget 中国）

Microsoft SQL Server 2008 安全性提高（七）

FERM（First Advantage 企业风险管理）方式

变幻莫测的法规遵从使得许多信息安全专家处于孤岛上。为了满足某项联邦法律或者行业标准和精准度，需要执行一些控件，通常情况下，对规则的理解同样重要。

Isabelle Theisen 是 First Advantage 公司的首席安全官。他将建立好的框架、进程和自动工具进行了自治的连接，以此来处理这些变幻莫测的法规遵从问题。这些连接不仅可以执行一个可靠的规则遵从程序，而且可以执行良好的商业惯例。

Theisen 说：“企业将任何与规则遵从有关的东西，都看成是一个无可避免的灾祸；他们需要这一点，因为他们被告知他们需要。我正在试图改变这个观点，告诉他们：‘不，你们也可以使用 IT 治理、自我约束、行业操作规则遵守和安全性，从而真正成为与竞争对手不同的市场占有者。’你可以换个方向，用比竞争对手做得更好的方式来使用它。”

First Advantage 是一家数据供应商，服务对象为：汽车经销商、债权服务和拥有信用报告、背景核查、技能评估以及更多的雇主。该公司的总部设在加利福尼亚州，受到萨班斯-奥克斯利法案（Sarbanes-Oxley）、联邦信用报告法案、金融服务现代化法案（Gramm-Leach-Bliley，也称格雷姆-里奇-比利雷法案）、PCI 和国家数据破坏通知法案和隐私法的约束。这些规则中的一些要求是重叠的，并且指令性的意见很少。

作为回应，Theisen 设计了她所谓的 FERM（First Advantage 的企业风险管理）项目，来确定控件覆盖了尽可能多的法规。该框架融合了 COBIT、ISO 和 NIST 的建议，也是人工操作流程的综合，可以确定风险和控件，并最终将其从 ControlPath 转化为 GRC 工具。ControlPath 是该公司 18 个月以前购买的工具。

她说：“我们在不同的企业部门都实施这个工具，从而进行评估、鉴定、测试以及修复工作，确保我们达到了所有企业部门的要求。”

在典型的审计工作方面，Theisen 恰当地比较了以前的人工操作流程和自动化操作——前者采用许多面对面的采访、调查、和问卷调查，进而确定是什么处在不同的企业部门之中、以及目录安全、风险管理、IT 治理和其管理程序。这一信息保存在一个电子表格中——Theisen 说，这不太实际。现在，已经升级为 ControlPath 工具。

Theisen 说：“我始终建议使用自动化工具。必须要拥有一个有关这方面信息的贮存库，即建立一个简单的 Access 数据库。否则，每年都询问相同的问题。又怎么能够建立一个基线呢？对规则遵守级别进行人工管理，这将是一场噩梦。”

自动化也可以帮助跟踪并确定控制对象的进程的发展趋势。

鉴定是 FERM 程序四个配置过程的第一步。诸如服务提供和企业部门评估之类的目录都集中并且上传在该工具中。

下一步是评估。一些威胁、漏洞和风险会影响到特定的服务提供，应该对这些威胁、漏洞和风险进行评估。应用于某个企业部门中的服务提供的每个应用程序可以进行行业影响分析、数据分类、以及威胁模拟。Theisen 说：“由于我们进行数据分层，我们可以仅仅关注服务提供方面的高风险应用程序。企业管理部门一直都极其支持，由于他们知道我们正在关注的对他们来说非常关键——他们服务提供中的高风险应用程序——并且，我们不需要做任何事情。

她说，虽然这两个阶段是最耗时的，但却是完全有必要的。

第三阶段是测试。已经确定了高风险问题是什么，Theisen 的研究小组就可以集中精力确定对于一个业务部门而言什么是关键的。在控件分析问卷调查之前，对应用程序和基础设施进行评估。Theisen 说，这个问卷调查针对的是正在讨论的服务提供。

ControlPath 构建了一个主控制库，与 First Advantage 相关的所有控件相对应，使其能够为每个业务部门建立定制的调查问卷。

她说：“这就是自动化作用的所在之处。”

修复是最后的阶段。根据测试的结果，Theisen 有一列修复的项目，是按风险的优先顺序来排列的——所有来自该组织业务影响分析和数据分类中的风险。

Theisen 指出，主要的挑战涉及法规中的不固定变化，在前端几乎很少有自动化程序来收集数据。通常情况下，组织不得不等待厂商更新他们的控制库，或者自己进行人工更新。

一些企业执行良好的商业惯例来管理数据，另一个挑战就是，严密的关注适合于这些企业的规则遵守。

Theisen 说：“我尽力不讨论这些法规。这是在讨论良好的商业惯例。”。

（作者：James C. Foster 译者：李娜娜 来源：TechTarget 中国）

Microsoft SQL Server 2008 安全性提高（八）

信息技术基础设施库（ITIL）所引导的方式

虽然公共机构可以免于受到华尔街的冲击，但是，这并不能消除约束他们的规则要求。他们遵守规则的压力仅仅来自于不同的来源。比如，迈阿密滩（Miami Beach）市一定要获得佛罗里达州执法部门的许可，这是该城市的公安部门可以申请联邦基金的晴雨表。此外，还有 PCI。随着市民支付自己的税款，驾驶执照费用和停车罚单用信用卡交付，这个城市和其它大部分城市一样，必将会遵守行业的支付卡安全标准。

Nelson Martinez 是这个城市的系统支持经理，他通过集中城市的 IT 基础设施，并将作为服务管理平台的 ITIL，以及 NIST 标准用来处理安全问题，进而处理这些需求的交叉问题。随着这个城市开始执行电子政务的倡议，这种集中化在未来几个月中会变得越来越重要，电子政务基本上在网上创造了一个虚拟的市政厅。

Martinez 说：“由于是公共资助的资金，因此这里存在一个道德问题。我们坚决负有一定程度的责任。我们希望能够符合一定的行业范围内的安全政策。很大程度上，我们就是一个 ITIL 工作室，我们像私营行业一样，采用变更控制从事一切工作。我们追踪一切，我们遵循服务水平协议（SLAs）。”

Martinez 的组织负责这个城市的基础设施——网络、服务器、台式机、网关、此外还有灾难恢复。它主要采用移动的工作人员来支撑各个部门。比如公众安全必须安全地连接到国家和联邦的数据库，这样可以在信息传输发生阻塞时，进行背景核查。

Martinez 的系统必须坚持遵守严格的 FDLE 配置方针，否则，事故不仅仅会危害到敏感的公众信息的安全，而且也会危及到这个部门获得资金的能力，导致其得不到认可。

Martinez 指出，ITIL 的标准化是至关重要的。在迈阿密滩市有一个 IT 部门专门负责该市所有的办事机关。Martinez 说：“这是我想要开一家 IT 工作室的真正的唯一途径。已经有了合适的标准。有一个统一的安全策略可以指示如何进行工作。这是唯一的途径，能够使我们在不同环境中拥有充分的控制。”

变更控制是最大的胜利，因为 ITIL 为 Martinez 的工作室提供了安全。

Martinez 说：“你还必须采取主动，进行你的扫描和电笔测试，察看问题出在哪里并解决这些问题。只要你已经建立了一个基准，你可以说：‘我是要大部分都处于安全状态’。ITIL 称，你需要具备合适的变更控制流程，这样你就可以追踪所在环境中的变更。”

Martinez 说，迈阿密滩市配置了 Symantec Enterprise Security Manager(简称 ESM)，用来处理其漏洞扫描并且监测政策偏差。比如，该工具就配备了 NIST 和 NSA 标准的模板。Martinez 用这些安全模板来制定规则，以遵守诸如 PCI 和用于移动连接的内部政策之类的行业规定。这个城市也使用 eEye 的 Blink 来实时监测入侵防御系统（IPS）和入侵监测系统（IDS）。

Martinez 说：“Symantec ESM 尤其擅长于为服务器创建模块，并告诉我们：我们是否遵守这些规则。这个工具是一个很好的方式，可以显示出正在进行季度规则审核的审计员是否违背了我们的机器，并能够进行补救。

Martinez 指出，如果某个安全问题威胁到了数据安全（法规遵从），可以检查问题的根源，并解决这个问题。比如，使用 ITIL，可以确定是服务器的变更还是防火墙设置中的变更导致了这个问题的发生。

他说：“这个工具可以帮助你进行排查并且重新回到起点，指出是什么原因导致了这个问题。如果你已经具备了服务水平协议（SLA），那么我怎么能向我的客户保证我将满足该服务的 5 9s 呢？

我需要确定我正在主动控制环境中的变更，或者确定这些变更在实施之前已经经过了核查。”

Martinez 指出，在实施变更之前，对与任何变更领域相关的风险进行评估，这一点是至关重要的。

他提到：“变更必须经过深思熟虑。我相信这对于产品环境的安全和性能来说都是非常关键的。如果你没有合适的充足的变更控制策略，发生重大的事故，是迟早的问题。”

Forrester 公司的 Othersen 指出，大多数组织都处在与这三种情况相类似的困境之中：选定框架的过程中、以及向遵守规则的规范化环境发展的道路上。

Othersen 说：“大约 10%的组织已经达到了圆满的状态：实现了规范化，其框架也是合理化和自动化。其余的组织正在选定框架，获得财政预算。虽然还没有采购或者进行工程实施，但是每家组织都在朝着那个方向发展。只是它们现在的运行方式效率比较低下。”

（作者：James C. Foster 译者：李娜娜 来源：TechTarget 中国）