IBM全球企业咨询服务部
IBM Security Systems

Tivoli. software

管理身份和访问，实现持续合规性并降低风险

管理、控制并监视用户对资源、应用程序和信息的访问

要点

- 验证访问资源的所有用户的真实性
- 监视用户访问是否遵循相应的使用策略并且与法规一致
- 在违规的地方采取纠正措施
- 在整个用户生命周期为用户授权提供问责性和透明度
- 支持用户活动的持续审计，以执行策略并协助实现合规性。

随着企业尽力安全地向其用户社区交付高品质、高可用性的服务，它们要设法应对成本控制和不断变化的用户群体、访问点以及应用程序。但是，这只是与身份和访问管理(IAM)相关的更大挑战中的一部分。服务必须单独交付给拥有正确权限的正确的人——无论是员工、供应商、合作伙伴还是客户。这已经变得越来越重要，但更难以实现。

Sarbanes-Oxley、Basel II、Federal Information Security Management Act (FISMA)、Health Insurance Portability and Accountability Act (HIPAA)、Model Audit Rule (MAR)和Payment Card Industry Data Security Standard (PCI/DSS)等合规性法规强调对个人授权和访问权限的可见性和控制能力的重要性。同时，计算方面的发展使其变得更难，包括:

- 结构化和非结构化数据的爆炸式增长
- 无处不在的信息访问
- 更丰富的、基于Internet的协作和云计算的增长

IAM的复杂性以及风险与合规性的压力要求使用一种新的方法，以及使这种方法成为现实的解决方案。企业需要的是策略驱动的IAM治理，提高可见性、控制力和自动化，在不降低生产力的情况下保护资产免受未经授权的访问。

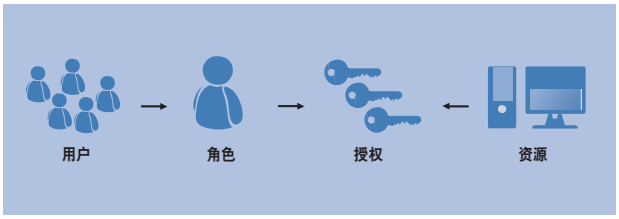

图1:IAM治理有助于将正确的资源提供给拥有正确权限的正确的人。

利用IAM治理建立企业的防御前线

IAM治理是企业安全前线的一部分。它是一项基础技术，可以确定已授权谁访问哪些资源，目的是什么，访问多长时间。除了授予、更新和删除访问权限的技术和策略之外，IAM治理还包括一些工具，可以监视、审计和报告用户利用其访问权限执行了哪些操作。如果没有IAM治理，授权管理、数据泄漏防护和欺诈检测等安全策略可能只有很少或根本没有执行访问策略的参考点。IAM治理是利用安全智能优化企业数据保护的驱动因素的基本组成部分。

大多数组织都在安全工具和技术方面进行了投资。但是，分层防御与在您的环境中构建安全智能并不一样。采用主动的安全方法，把风险控制集成到每个结构中会怎么样呢？IBM身份和访问管理治理可以有助于解决问题，并且提供的价值超出风险控制 — 还有整个用户生命周期中用户授权的问责性和透明度。

如果身份管理更直接地集成业务目标和优先事项，那么 IT 就可以向个人提供更加精细调优的服务，使业务能够把握各种机会。IAM治理解决方案还可以改进其他安全和策略控制技术，并为全面的安全管理作出贡献。IAM治理描述了组织如何管理、保护和监视应用程序、信息和系统的身份识别和访问权限。它进一步扩展了通过用户配置、Web访问管理和目录基础架构等核心身份和访问管理功能所提供的价值。

IAM治理解决方案发现、分析并建立用户访问、工作流、报表工具和分析。这将为用户访问治理创建一个流程，其中的授权约束将有助于管理业务冲突。IAM治理包括以下实践:

- 用户生命周期管理（用户配置和取消配置）
- 密码管理和单点登录(SSO)到多个应用程序（包括自助服务选项，以减少帮助台呼叫量）
- 角色管理（根据工作职能和业务需求为用户分配不同的角色，并管理职责冲突的分离）
- 认证策略建立一个定期审查流程，并验证用户访问权限是否合适
- 访问管理（对内部用户以及包括业务合作伙伴和第三方服务提供商的外部用户执行基于策略的访问）
- 授权管理（执行细粒度的、基于角色、规则和属性的应用程序和服务访问）
- 持续审计和报告，以监视用户活动、执行政策并协助实现合规性

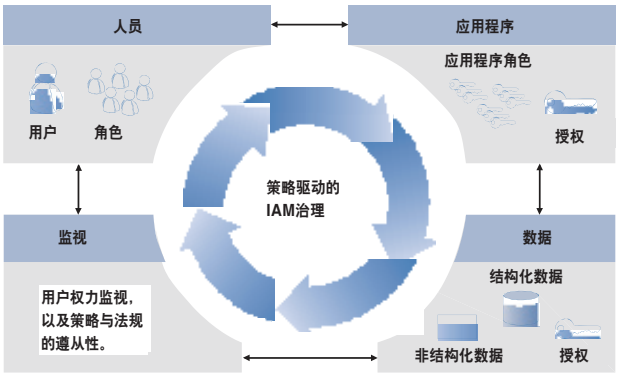

图2:IBM提供一个由策略驱动的IAM治理方法。

利用策略驱动的IAM方法促进一致性与合规性

考虑到对安全和隐私的关注在不断升级，以及对合规性及企业监管的持续关注，控制对数据和应用程序的访问非常重要。组织必须证明它们有强大且一致的访问控制。它们还希望确保有关用户授权的决策与其业务目标和策略保持一致。IBM IAM治理提供各种资源来管理业务特定的用户访问需求，具有更强的问责性和更高的透明度，有助于更有效地治理和执行用户访问。IBM使用由策略驱动的方法来管理人员、应用程序和数据，该方法提供了有效的IAM治理所需的一致性和广度，并且有助于促进合规性。

IBM指导客户使用经过证明的、由策略驱动的方法，该方法涵盖五个阶段的身份和访问管理产品生命周期，包括:

- 定义控制
- 登记和验证用户
- 发出和管理用户权限

- 管理和执行访问控制
- 对用户的权限和活动进行监视、审计和报告。

在每个阶段中，IBM IAM治理解决方案都通过改善服务，降低成本并更好地管理风险，为客户提供创造业务价值的机会。IBM的IAM治理解决方案有助于在正确的时间为正确的人提供高效且合规的访问权限。它们通过简化用户身份验证、优化应用程序访问，以及管理用户配置和取消配置活动来做到这一点。客户可以借鉴IBM深厚的安全专业知识，创建一个端到端的IAM解决方案，支持并增强其他安全组件，提高相关领域（如合规性、使用策略和报告）的效率。通过简化用户生命周期管理，并对用户授权提供更好的可见性，IBM身份和访问管理（IBM Identity and Access Management）治理可以帮助最大限度地提高IT员工的工作效率，并降低安全性与合规性的成本和复杂性。

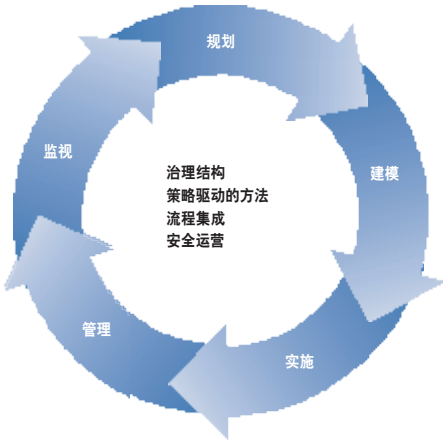

图3:一个可行的IAM治理计划需要一个多步骤的闭环流程。

探索IBM的IAM治理解决方案

由于需要证明数据访问和管理的问责性，法规遵从性促使企业采用IAM技术。IAM还可以帮助防止欺诈并提高运营效率。一致的身份和访问管理有助于保护数据完整性，并促进合规性——即使基于云的用户社区、大数据存储和增加的移动性带来了复杂性也是如此。IBM的IAM治理解决方案迅速为用户提供完成其工作所需资源的授权访问，同时保护应用程序和数据。IBM的IAM治理解决方案包括:

身份管理

身份管理是一个管理信息的流程，用于识别用户，控制用户访问，确定用户的权限和委托管理机构。涉及到最终用户时，并没有万全之策。用户生命周期在不断地变化，因为人的角色和责任经常改变。如果员工在组织内被赋予了新的职责或换岗，需要对他们的访问权限进行审查、批准和更新——可能会暂停或删除以前的访问权限。客户的访问配置文件也有可能演变。例如，拍卖现场具有超强实力的卖家，或到达指定交易额的股票投资者，就需要无缝地更新他们的个人资料和授权。

授权的速度和准确性同样重要。新员工在能够访问业务或电子邮件应用程序之前都可能会保持空闲状态。基于云计算的客户社区和用户也需要立即访问资源。

安全策略也是动态的，因此身份管理解决方案所包括的工具应该能够简化策略的创建过程，让管理员无需在生产环境中引入策略就能评估潜在策略变更的影响。合规性和监督要求能够管理身份和访问数据。预定义的报告和审计事件应帮助审计人员快速获得关于组织的安全状况以及合规性状态的准确视图。

凭借在整个IT基础架构中提供基于策略的用户和角色管理的能力，Tivoli® Identity Manager是身份和访问治理的一个关键驱动因素。Tivoli Identity Manager有助于在整个用户生命周期中自动化用户权限的创建、修改和终止过程。它提供的功能包括:用户自助管理、用户帐户的配置和取消配置，以及重新认证。其角色和策略建模特性为全面的生命周期管理提供了角色挖掘与建模、责任分离、组管理功能，以及模拟多种访问场景的能力。

访问管理

访问管理是指能够跨各个企业系统管理一套一致的访问控制策略，使其满足安全策略及法规遵从性的要求，它包括策略的管理、监视与执行。

访问管理解决方案管理已授权人员对资源的日常访问。有效的解决方案将正式的安全策略集成到访问管理工作流中，实现操作系统、网络、服务器、存储设备、数据库、桌面应用程序、在线商务系统和企业应用程序的自动化访问管理。访问管理也将用户一般针对多个资源和应用程序所使用的多个用户名和密码统一为单个安全性增强的身份验证和授权流程——通常利用单点登录(SSO)来实现。

访问管理产品在整个用户生命周期中执行访问政策——跨多种环境和安全域进行身份验证，并向授权用户提供访问权限，同时执行安全策略，并防止内部和外部的威胁。IBM的访问管理产品有助于支持跨多个应用程序和用户一致地执行安全策略。它们支持SSO，可改善用户体验并减少帮助台成本。

它们也可以利用授权管理提供细粒度的访问执行。IBM Access Management产品包括:

- IBM Tivoli Access Manager for e-business—作为Web和其他应用程序的身份验证和授权中心，集中实现访问管理，使安全应用程序的部署更容易，并且更为经济高效。
- IBM Security Access Manager for Enterprise Single Sign On—通过集成企业单点登录和强身份认证、访问工作流自动化、快速用户切换和审计报告，简化、加强并跟踪访问。
- IBM Tivoli Federated Identity Manager—使用面向SOA和Web服务部署的开放标准，跨分布式门户和大型主机环境提供以用户为中心的联合单点登录，从而在可信的合作伙伴之间安全地共享信息，并简化应用程序集成工作。
- Tivoli Security Policy Manager—为应用程序、数据库、门户和服务实现集中的安全策略管理和细粒度的数据访问控制。
- QRadar Security Intelligence Platform—提供一个统一架构，用于收集、存储、分析和查询与日志、威胁、漏洞和风险相关的数据，帮助防止内部威胁，并控制合规性证明的成本。
- IBM Security zSecure suite—提高了企业实施安全遵从性、监视和审计事件，以及自动化大型机日常管理任务的能力。

IBM Security Identity and Access Assurance

IBM提供一个捆绑的软件解决方案，在整个用户生命周期中帮助简化身份管理，并执行访问策略。该解决方案还包括日志管理和特权用户监视，以加强内部威胁检测，提高审计能力，并促进执行各种合规性措施。

IBM Identity and Access Management Services是一个全面的功能组合，几乎涵盖了身份管理的每个环节——从身份证明到用户配置，再到访问控制。

IBM的IAM治理产品构成了一个全面的方法，可帮助您满足关键的业务和安全需求，包括:

- 发现、记录和分析用户访问
- 建立一个用户访问治理流程
- 确保各种约束有助于管理业务冲突
- 以可控的集中化方式执行策略
- 促进工作流、任务和流程的自动化
- 监视、报告和审计，有助于确保正确的访问，并实现合规性

利用IBM的IAM治理解决方案实现切实收益

使用正确的IAM治理解决方案的一个由策略驱动的方法，提供管理业务特定的用户访问要求所需的可见性、控制力和自动化，并提供更强的问责性。下面的IBM客户在简化IT效率、加强安全性、降低风险和实现合规性等方面都受益于这种方法。

拉丁美洲银行

某巴西银行从多个办事处和超过1000个销售点为超过10万名客户提供工资贷款和信用解决方案。由于在几十个应用程序上的多种安全标准和登录过程，工作人员需要尽力确保向其雇员提供了适当和快速的访问，并证明符合巴西的监管标准要求。

该客户部署了IBM一个集成的身份管理和单点登录解决方案，以加强安全性，同时简化信息的访问。

该解决方案确保用户可以访问合适的应用程序，并提供简化的IT资源访问。现在，工作人员和代理人只需登录银行网络一次，并且能够即时访问他们有权使用的所有应用程序。在此之前，用户必须分别登录15~30个不同的应用程序，才可以为客户建立一个贷款方案。如果员工离开公司，或者代理人的角色发生了变化，安全团队只需敲几下键盘就可立即在所有系统上取消其配置，保持银行的数据安全。

因此，银行的帮助台成本每年降低了大约R$32,000(US$20,000)。它也将配置新用户的时间从长达5天缩短为仅仅两小时，并且将重置密码的时间从四小时缩短为数秒。通过在有需要的时候快速取消用户的配置，系统的安全性得到了提高，这也让安全团队在没有增加员工的情况下可以支持新的项目。

欧洲城市

捷克的一座城市有着悠久的历史，并且已逐渐成为商业和旅游中心。要为一座成长中的城市确保实现全面的IT安全性，需要许多流程的集中化和智能自动化，包括监视和防止对该城市IT系统进行未经授权的访问。

该城市已实施了基于规则的身份管理系统，根据员工职位、角色和部门来自动化员工帐户的访问。该系统将使用自动帐户调节流程，检测和纠正（或删除）不符合预定义规则任何帐户。闭环调节流程可识别“孤儿”或过期的帐户，并在雇员离职时自动删除帐户访问权限。这个城市现在充满信心，需要访问帐户的员工可以快速高效地获得访问权，同时其IT系统的安全性仍然得到了保证。

解决方案的收益包括:

- 新员工的激活速度提高100%——新员工在几个小时而不是几天内就可以访问所有系统，从而变得更高效。
- 提高管理效率并降低成本；一位全职雇员现在可以管理
- 所有用户帐户，而其余的IT人员可开发和增强组织的IT环境。
- 在雇佣合约终止后的几小时内删除孤儿帐户并停用雇员帐户，从而提高系统的安全性。

南美社会服务机构

在乌拉圭，一个令人兴奋的试点项目正在进行中，当一个孩子出生时，医院可以在线通知政府社会保障和社会服务机构。这是该国正在开展的一系列电子政府计划中的一个，目的是取代基于纸张的流程，并提供更高的效率和透明度。最终将有约50,000名政府雇员和200万市民使用这些在线服务。

与IBM及一家IBM业务合作伙伴携手，该组织实施了一个多层次架构，为其电子政府服务提供全面的安全解决方案，并解决传输安全性、访问控制和身份管理问题。为了保持Web服务的机密性和完整性，IBM WebSphere® DataPower® Integration Appliance作为策略执行点，从IBM Tivoli Security Policy Manager接收策略。安全令牌由Tivoli Federated Identity Manager发出，以确认声称要发送消息的个人正是他自己所报称的身份。IBM Tivoli Access Manager for e-business提供了集中的身份验证、政策管理和访问控制服务，为市民和政府工作人员提供快速、安全的在线服务访问。IBM Tivoli Directory Server和IBM Tivoli Identity Manager提供可信的身份数据，跨所有Web服务支持身份验证流程。

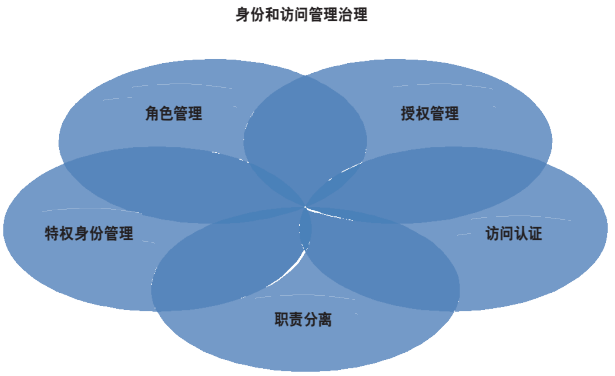

图4:根据业务优先级，组织应从身份管理的分类开始，如本图所示，然后制定一个完整的IAM治理计划。

入门——利用IAM治理提高安全性和业务效率

由于监管方面的障碍在成倍增长，数据量也在不断扩张，并且社交商务在继续转变人们的访问需求，IAM治理解决方案对于组织的日常安全性和业务运营，以及持续的合规性工作正变得越来越重要。利用由策略驱动的战略性方法，身份和访问管理可以帮助您应对各种变化，降低管理成本，并保护您最有价值的信息资产。

考虑到这些因素，就不会对IAM从外围移到IT优先级的最前沿感到奇怪了。IBM的IAM治理解决方案帮助客户实现多种安全性和面向业务的收益，包括:

- 利用集中的视图提高合规性状态的显示，以及验证身份和授予访问权限的业务流程

- 通过独立的自定义身份管理解决方案子集降低成本
- 通过减少员工登录的次数和凭据，提高安全性，降低成本
- 通过单点登录(SSO)体验和按需访问配置，提高生产效率，降低帮助台成本，提高员工和/或客户满意度
- 通过更快的产品上市时间，以及集中化、标准化的安全基础架构，提高业务的灵活性
- 运行时授权事件的集中化审计视图，能够更容易地检测恶意行为

为什么选择IBM?

一致的身份和访问管理治理可保护数据的完整性，并促进实现合规性。IBM是全球IAM市场中公认的领导者，具有国际视野，并了解各行业不断发展的区域性需求。此外，IBM凭借其卓越的解决方案得到了分析师和安全社区的一致认可，在几个不同的报告中均被分析师列为“领导者”，并被SC Computing杂志评选为2011年度最佳身份管理解决方案。许多IAM厂商只提供全面IAM治理解决方案的某些部分，需要客户部署并管理来自若干个厂商的不同产品。但IBM提供一个身份和访问管理软件以及服务的广泛集成套件，可以支持第三方环境，如Oracle、Microsoft和SAP。

更多信息

如需进一步了解IBM Security Systems，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

此外，IBM Global Financing的财务解决方案可以支持有效的现金管理，保护技术不会过时，改善总体拥有成本和投资回报。此外，我们的Global Asset Recovery可以利用更高效节能的新解决方案帮助您解决环保问题。有关IBM Global Financing的更多信息，请访问:**ibm.com**/financing

IBM Corporation Software Group Route 100
Somers, NY 10589
U.S.A.
在中国印制
2012年7月

WGB03002-CNZH-00