选择合适的身份和访问保障方案，实现业务价值

IBM

组织需要管理越来越多的用户、应用程序和访问点，同时还要努力确保遵从法规。他们需要安全的基础设施，既能解决短期需求，比如降低成本、整合合并与收购、有效管理劳动力的变更；又能满足长期需求，比如让组织可以通过新的门户和 Web 服务项目实施发展计划，以及让组织可以快速地利用新的交付平台，如云计算和面向服务的架构 (SOA)。

执行人员越来越希望看到由身份和访问保障方案所交付的业务价值，这是因为组织如何有效地解决这些挑战可对其竞争态势和盈利能力产生重大影响。他们希望实现创新，便捷地访问应用程序和系统，同时确保稳固的安全性和合规性。为了保持竞争力，他们希望通过基于角色的门户促进员工、客户或机构及合作伙伴之间的协作，并将新的服务快速导出给这些用户。

为了实现这些目标，组织必须能够：

- 在用户访问资源之前，对用户进行认证和授权。
- 解决访问控制策略，包括基于组成员关系的简单决策以及基于业务条件和数据的实时决策。
- 监控访问是否遵从使用策略并符合法规。
- 在检查到不遵从法规时，采取校正行动。
- 在组织中保护对关键数据的访问权。
- 整合由合并与收购产生的新身份。
- 确保不再需要用户权利时，及时撤销权利。
- 控制帮助台、应用程序开发安全编码和合规性报告等领域的成本，为新的计划留出预算。
- 支持对新计划的请求，比如云计算、门户和 SOA 项目。
- 提高员工、管理员和用户的生产力。

有效的身份和访问保障方案可通过受信任的合作伙伴整合完整的功能，用以管理、保障和审计用户对资源的访问。这类解决方案可帮助组织实现业务价值，并实现短期和长期目标。

这份买方指南可帮您选择合适的解决方案，成功地管理和控制组织内、跨组织以及组织间的访问，从而获得身份和访问保障。本文从 CSO、IT 操作员工、业务线管理人员和企业架构人员的角度概述了组织面临的最常见身份和访问管理挑战。随后提供了直接解决复杂性、合规性和成本等挑战所需的功能信息。这些信息可帮您评估特定供应商的服务产品是否能以最佳方式解决您已进行优先排序的挑战。

从身份和访问管理开始

在选择能交付身份和访问保障的解决方案时，应该解决以下主要类别：

1. 在整个生命周期中管理用户和用户信息

2. 确保有效地访问资源，从而使用户生产力最大化

3. 跨每个应用程序、数据源、操作系统和组织边界，一致地管理和执行访问控制策略

4. 监控和审计用户访问

5. 加速价值实现

6. 选择合适的身份和访问保障提供商

对于每个类别，您将找到以下检查清单，可用于评估供应商及其产品。

1. 在整个生命周期中管理用户和用户信息

IT 人员通常要花费过多的时间管理存在于数百个不同地点的用户权限和策略。按案例添加用户角色、身份和访问权利是一项复杂的任务，可耗费几小时到几个星期。移除这些权利要花费同等时间，还带来额外的风险：丢失应终止其访问的用户。

即使在指派最初的用户权利以后，IT 人员也必须执行持续的协调、再认证和报告，以确保门户和 Web 站点的访问点安全，且数据保持安全。每次改变工作、角色或雇用状况时，必然会对所有的现有权利进行评估，且随之改变，同时维持适当的职责分离。

集中、自动化的解决方案可以让您管理任务，以更加有效地管理和审计用户角色、身份、凭证、账户和访问权限。自动化可缓解 IT 人员的重复性任务，从而降低成本，进而帮助确保从最初的登录到最终的登出都能一致地管理安全性。

用户生命周期管理

寻找具有以下功能的解决方案：	IBM	其他供应商
提供单个安全的可审计的身份库。	✓	
提供整合的基于 Web 的界面，包括简单的向导和丰富的配置编辑器，让您可以轻松地创建、修改和查看配置对象及其关系。	✓	
交付有效安全地将账户映射给其用户所需的灵活的账户采用方法。	✓	
提供整合的基于角色的访问控制 (RBAC)、基于规则/属性的访问控制 (ABAC) 以及基于请求的配置选项。	✓	
提供操作角色管理，作为用户配置平台内部的嵌入式功能。	✓	
利用角色管理、职责分离和再认证，将用户配置与开放接口密切集成，从而与持续的业务控制系统集成。	✓	
提供角色层次，简化用户与角色和权限的映射。	✓	
实现预防性和检测性的职责分离，缓解由用户访问权利冲突所产生的风险。	✓	
独立、简单地实现用户角色、账户和组成员关系的再认证。	✓	
支持按组进行身份管理，简化用户管理，并降低管理成本。	✓	
支持工具，使用简单的基于向导的导航和拖放 GUI 构建用户配置工作流，从而通过普通的 Web 界面实现更加高级的业务流程。	✓	

用户生命周期管理

寻找具有以下功能的解决方案：	IBM	其他供应商
管理分布式用户集,包括将这些用户指派给单个多个角色的能力。	✓	
支持自动且按需协调账户,快速可靠地发现不合法的"孤立”账户和不必要的授权,并启动自动或手动修复过程。	✓	
从登录到登出,自动化用户生命周期管理。	✓	
充分利用身份集成功能建立规则,识别哪些组和个人具有更改哪些数据领域的权威。	✓	
为便于审计，维持精确地配置记录和用户访问权利的变更记录。	✓	
提供对审批和操作工作流的访问权，以实现自定义配置活动。	✓	
支持同等地配置内网和外网的配置文件。	✓	
支持开箱即用的手动服务，这样个别人员就可快速、轻松地使与电话订单或其他手动管理项目相关的业务流程自动化，从而获得对目标的管理，同时还手动执行配置任务。	✓	
提供自定义的基于角色的用户 GUI，拥有 Manager、End User、Auditor 和开箱即用的 Help Desk 等视图。	✓	
支持提供特权和共享身份的生命周期管理，确保个人责任制。	✓	

2. 确保有效地访问资源，使用户生产力最大化

让员工及时、方便地访问应用程序和服务，这样就可以提高他们的生产力，而根据需要保护对业务敏感数据的访问则有助于保护组织免受不断增长的威胁和漏洞。 为客户、机构和合作伙伴开放访问权，也可带来新的价值和增长机遇。但是增加合法用户的数量，也可使环境变得复杂，带来巨大的安全挑战。如果安全控制阻止对所需资源的访问或者访问因需要多次登录和身份验证而变得异常麻烦，用户都不会感到满意，生产力也不会高。

键入、更改以及重置密码都会明显占用员工和 IT 人员的时间，导致运营成本增加。跨企业的单点登录 (SSO) 功能、基于 Web 的联邦系统可减少大量与密码相关的问题，并提高员工生产力。

联邦 SSO 功能让用户可以跨域边界在多个 Web 站点之间无缝地导航。 联邦 SSO 功能可减少挫折，降低用户管理成本，可促成与合作伙伴组织的无缝协作环境。

自助功能让用户可以管理其自身的账户并重置密码，从而进一步提升用户体验。有了这些功能，用户就可以快速备份和运行，而不会增加调用 IT 帮助台所需的时间和成本。

用户访问管理的核心功能

寻找具有以下功能的解决方案：	IBM	其他供应商
提供直观、自定义的管理 GUI，具有点击功能，让您可以轻松创建新的 GUI 视图。	✓	
包括管理 GUI 内的多任务功能，让您可以开始任务，打开第二个任务，然后切回到原始任务，并完成该项任务。	✓	
让您可以提交和追踪状态请求，并监控单个 GUI 中的工作流任务。	✓	
交付向导和模板，以快速、轻松地配置，并通过 GUI 轻松访问为粒度化的自定义而产生的脚本。	✓	
利用所记录的与开放 API 的集成路径，提供开箱即用的身份验证集成功能，以实现各种身份验证方案。	✓	
提供完整且全面的联邦与信任管理方案，包括一般目的的安全标记服务，适用于 Web 服务/SOA 环境内常见的基于标准的身份传播。	✓	
提供基于标准的开发过程，用于通过基于 Eclipse 的插件扩展安全标记服务。	✓	
提供与企业服务总线 (ESB) （包括 IBM WebSphere® Enterprise Service Bus） 的强大集成功能，促进对 ESB 安全的联邦访问。	✓	

用户访问管理的核心功能

寻找具有以下功能的解决方案：	IBM	其他供应商
包括强大的目录和目录集成及同步化产品，而无需额外费用。	✓	
支持指派访问受保护的资源所需的授权级别，且在用户必须提供下一验证级别时，执行递升策略。	✓	
提供基于标准的 (XACML) 赋权管理（角色、规则、属性），以实现数据安全性和精细粒度的访问控制。	✓	
提供 SOA 安全策略管理（消息保护策略支持）。	✓	
提供完全可配置的身份验证机制以及外部验证接口，以任何语言来适应 Web 应用程序。	✓	
解决 Linux® 和 UNIX® 环境（包括虚拟化化境，IBM AIX® LPARs/WPARs、Solaris Zones、VMware）的密码策略、登录策略、文件访问控制、TCP 端口访问控制、应用程序保护和责任制。	✓	
广泛地集成身份服务器、应用程序、中间件、操作系统和平台。	✓	
提供闭合回路的访问和审计管理支持，包括与现有安全信息和事件管理工具的集成。	✓	

Web 和联邦单点登录（SSO）

寻找具有以下功能的解决方案：	IBM	其他供应商
为所有桌面应用、Web 应用等（包括 IBM WebSphere、Microsoft®、Oracle 和许多其他的门户和应用环境）的用户交付统一的 SSO。	✓	
为 Microsoft NET 环境应用程序（比如 Microsoft SharePoint 和 Exchange server）提供直接的 SSO 支持。	✓	
尊重 Active Directory (AD) 的密码变更，支持使用 AD 替代 userPrincipalName (UPN) 电子邮件地址进行身份验证，以及使用 Active Directory Application Mode (ADAM) 进行用户注册，从而简化 Microsoft 用户的登录。	✓	
支持多个标准，进行跨站点验证，包括安全保障标记语言 (SAML)、自由联盟和 Web 服务联盟语言 (WS-Federation) 的标记通行协议。	✓	
支持 SAML 2.0 属性查询和身份验证授权，从而与业务合作伙伴安全地协作。	✓	
支持 OpenID 属性服务，.从而与客户安全地协作。	✓	
支持简单且受保护的 GSS- API 协商机制 (SPNEGO) 协议，用户可以只登录一次，就能多次访问 Web 资源。	✓	
支持 WS 安全策略，进行 Web 服务身份验证；且支持 WS 元数据交换和 WS 通知，进行安全的 IT 集成。	✓	
使用现有的应用程序身份（例如，LTPA、Kerberos 和 SAML）协议，支持 Java™ EE 和 .NET 应用程序及 Web 服务集成。	✓	

Web 和联邦单点登录（SSO）

寻找具有以下功能的解决方案：	IBM	其他供应商
支持大型机应用和 Web 服务集成，包括使用 RACF PassTicket 协议。	✓	
使解决方案具有容错能力，而不必依靠第三方操作工具。	✓	
集中控制对内部和外部应用的访问，包括 SaaS 以及基于云的服务。	✓	
提供 Java 管理 API，用以管理大规模用户和组。	✓	
支持 HTTP 1.1，持续连接应用程序。	✓	
支持 TCP 和 SSL 结合，保护 Web。	✓	
与 WebSphere DataPower® 集成，支持控制区的 Web 服务。	✓	
提供业务到客户 (B2C) 的自助界面，供用户登记、验证、更新账户、重置密码和同步化。	✓	
通过复制策略（相对于只是缓存），提供高可用性，使得即使在无法链接到服务器时，也可执行策略。	✓	
利用 Web 授权方法，提供高性能，并扩展给数千万用户实施方案和数百个应用程序。	✓	
提供灵活的 Java 基于 Web 的架构，可利用强化的反向代理或现有 Web 服务器的插件模块来保护资源。（在某些情况下，专用代理可提供较高的安全等级。）	✓	

Web 和联邦单点登录（SSO）

寻找具有以下功能的解决方案：	IBM	其他供应商
提供可靠的反向代理技术（超过 1,000 位客户安装为证），从变更和配置管理角度而言，这是一种高级方法。	✓	
包括会话管理服务，可以限制在每个领域创建的会话数量，让服务器不必重启，并实现多个服务器案例用以分享用户会话，从而提高性能。	✓	
提供会话管理服务，可立即终止恶意用户的所有主动会话。	✓	
提供后期办公室（防垃圾邮件）功能，聚集类似于电子邮件和用户工作的条目。	✓	
支持较轻程度的联邦方案，让小组织可以快速与大组织建立联盟。	✓	
使用 Microsoft CardSpace 或 Higgins 身份框架等身份选择程序，支持具有新兴的用户中心身份的 B2C 联盟，包括 OpenID 和信息卡配置文件。	✓	
支持跨 Web 2.0 和 Web 服务的用户访问，包括与现有 XML（例如，WebSphere DataPower）网关开箱即用的集成。	✓	
支持与第三方验证方案进行广泛且灵活的集成。	✓	

自动化地访问企业应用程序

寻找具有以下功能的解决方案：	IBM	其他供应商
包括企业单点登录 (ESSO) 方案，因其先进的功能而在市场中脱颖而出，可与许多不同种类的应用程序合作，与强大的身份验证功能集成，灵活地管理会话，且能够记录和审计终端用户的活动。	✓	
包括领先的 ESSO 方案，可由同一供应商进行完整的集成、开发和支持，从而提供全面的身份和访问保障。	✓	
提供以 Java EE 架构为基础的 ESSO 方案。	✓	
提供 ESSO 方案，可与 Web、桌面、电传打字机、大型机应用进行集成，也可与许多客户端设备平台进行集成（比如 Microsoft Windows® CE 和 Windows XPe），容纳尽可能多的应用程序。	✓	
能够通过扩展工作流自动化登录、更改密码和登出，因此除了简单的 SSO，还能实现自动化。	✓	
提供 ESSO 方案，包括众多会议管理功能，支持个人桌面、共享桌面 (kiosk)、私人桌面（具有多次会话的 kiosk）、终端客户、拨号会议、普适设备和漫游桌面。	✓	
利用同一共享工作站上用户之间的真实私人桌面，快速切换用户和执行完整的 AD 策略，使得一人登出时另一人可登录，缩短宕机时间。	✓	

自动化对企业应用程序的访问

寻找具有以下功能的解决方案：	IBM	其他供应商
提供多个可选择的身份验证因素，包括用户 ID 和密码、USB 智慧标记、构建访问徽章、主动 RFID、生物指标、以及开放的身份验证设备接口，用于轻松地集成第三方设备。	✓	
提供能支持桌面密码重置功能的 ESSO 方案。	✓	
支持 ESSO，而不会对目录基础设施造成额外负担，也不会修改目录模式。	✓	
提供向导，自动产生 SSO 配置文件，并提供可视化配置，使高级用户可以自动实现复杂的应用程序。	✓	
超越 SSO，无需改变应用程序就可控制应用程序的用户界面。	✓	
针对所有的会话管理模式，确保安全完全执行 AD GPO 设置。	✓	
追踪应用程序登录/登出，审计账户使用情况。	✓	
能够自定义地追踪应用程序。	✓	
集成有配置功能，为特权身份管理提供共享和特权身份的自动化的登录/登出。	✓	
与其他身份和访问管理组件（比如配置、合规追踪和报告、Web SSO 和联邦 SSO）完全整合，提供端到端的身份和访问保障框架，且可根据您的需求而增长。	✓	

3. 跨每个应用程序、数据源、操作系统和组织边界，一致地管理和执行访问控制策略

随着用户数量呈指数型增长，组织需要有效方案以管理和执行访问控制策略。这些策略需要与核心业务系统集成，并使身份信息在多个来源中保持同步。但是有一点很重要，这些策略需要使业务规则与业务控制决策保持一致，并能够在实施策略之前模拟策略的变更。组织必须能够实现访问控制策略，帮助确保遵从法规，同时经济高效。

需要横跨多个对话追踪用户，同时确保执行访问策略，比如静止超时。 需要在应用程序代码以外维护和管理访问控制业务规则，以提高灵活性。资源也需要具有有意义的说明，从而更容易管理。

随着更多的用户依赖这些应用程序，安全方案的可延伸性和可用性变得极为重要。组织需要一种解决方案，既可以扩展给极大数量的应用程序，又可提供合适技术支持水平及故障恢复功能，从而维护业务关键应用程序的可用性。

数据和应用程序赋权及访问控制策略

寻找具有以下功能的解决方案：	IBM	其他供应商
提供灵活和配置快速且可扩展的身份馈送法，可从单个授权来源推动身份数据，或者从多个来源拉动和聚集数据。	✓	
从业务友好的角度为业务管理员和审核员描述用户可以如何处理访问权利，从而在新的访问审批请求、再认证和审计访问中更好地作出决策。	✓	
管理员可以对细粒度资源应用有意义的说明，将其分类以做快速参考和搜索，为其指派所有者，定义独特的审批和再认证工作流，并提供这些资源的详细报告。	✓	
企业架构师可以对安全策略进行建模，并创建安全策略模板，在组织内部一致地使用。	✓	
应用程序所有者可以使用应用程序角色和属性创建数据授权，而无需 IT 操作环境方面的知识。	✓	
拥有的工作流可利用灵活的异常情况处理方法，与 SAP 及 Oracle ERP，以及细粒度职责分离检查无缝地集成。	✓	
提供集中管理的 GUI，用于控制和修改，且无需手动更新每个适配器，就能反映验证和授权方法的变更。	✓	

数据和应用程序权限及访问控制策略

寻找具有以下功能的解决方案：	IBM	其他供应商
包括“情景假设”策略的变更模拟分析，在变更之前识别会对哪些人员和内容的权利造成影响。深入地分析和实现查看策略变更	✓	
将业务价值并入访问控制决策中，并在运行时动态评估这些规则。	✓	
在应用程序代码之外管理访问控制业务规则，让您可以改变影响访问的策略参数，而无需重新编写和汇编应用程序。	✓	
一致追踪用户在多个并发会话中的所做内容，这样一旦有用户登出，方案就可让用户在任何地方登出，避免并发的登录。	✓	
在静止超时期间执行访问策略，在多个实施点实行三振出局的规则及其他规则。	✓	
提供统一的策略，从操作系统资源到基于 Web 的应用 SSO，管理集中管理和控制访问。	✓	
定义基于策略的规则，您就可以轻松设定安全策略，并将策略应用于不用的系统、用户、存储或信息。	✓	
设定访问策略，自动实时地检测和修复不符合法规的有意和无意的事件。	✓	

数据和应用程序权限及访问控制策略

寻找具有以下功能的解决方案：	IBM	其他供应商
在未采取及时行动时，自动提升并重新引导工作流程至替代方案。	✓	
扩展到数千万用户以作身份验证和授权；同时也扩展为满足内网、外网和互联网用户的需求。	✓	
支持非标准、安全 IP 负载平衡器、经由复制服务器实现智能的负载平衡且包括聚集支持，从而提供可伸缩性和可用性。	✓	
在决策组件可进行本地访问的地方，复制所有的策略规则，从而确保可用性。	✓	
在 Web 服务基础设施中为 DataPower®、WebSphere 和其他 Web 服务资源实现多个策略实施点。	✓	
为应用程序和数据源（比如 SharePoint、WebSphere Portal、WebSphere Application Server、IBM FileNet®、IBM DB2® 和其他应用程序及数据资源）实现多个策略实施点。	✓	
确保硬件关键存储的安全，并提供故障恢复功能，支持自动切换到备份的 Web 服务器，从而充分利用 SSL 加速卡技术。	✓	

4. 监控和审计用户访问

组织不仅要能够控制对数据和应用程序的访问，同时还必须能够证明其访问控制的强度和一致性，从而关闭身份和访问生命周期，并提供可审计的合规证据。在如今复杂的计算环境下，组织需要封闭环的视图，查看谁可访问何种内容，为何拥有访问权限，以及他们如何处理这类访问权限。必须将这种可见性扩展到特权用户和受信任的用户，因为他们的账号尤其容易被滥用。

可使用监控报告来理解用户活动是否符合组织的权利和策略。应突出任何异常或不符合策略的活动，从而解决并校正这类活动。 将监控作为整个合规流程的一部分，这么做可以关闭回路，有助于确保具有合适的安全级别。[1]

无论用户是通过门户、Web 站点还是企业网络获得访问权，以正确的解决方法为基础的集中、策略驱动办法都可以提供可见性，追踪访问系统的每一个人，使授予的访问等级符合组织优先权和需求，以更强的责任制来管理访问，并确保实施访问策略。

为了帮助治理 SOA 环境，企业架构也应该能够在整个 SOA 中有效且高效地管理和配置用户身份，从而扩展企业服务总线 (EAB) 的功能。

这种方法可创建“了解身份”的 ESB，让组织可以确保用户根据他们的安全凭证和访问级别来访问应用程序、数据和信息，而不管他们是访问哪个应用程序。

监控和审计用户访问

寻找具有以下功能的解决方案：	IBM	其他供应商
提供自动化日志管理，有效收集、存储、调查和检索日志。	✓	
包括可扩展的日志收集程序，确保从几乎任何平台可靠且可验证地收集本机日志，包括系统日志、简单网络管理协议 (SNMP) 等安全日志类型（包括操作系统、数据库和安全设备）。	✓	
利用单个安全的身份库，实际上可从这些身份库追踪并审计所有的身份事件。	✓	
跨各种周界的安全设备集中收集、简化并关联与安全性相关的事件和警报。	✓	
自动且开箱即用地提供所有活动的审计记录，包括策略修改等管理活动。	✓	
提供真正闭合的策略合规，可检测和修复在配置流程以外授予的访问权限，用以替代复杂的可能具有多个故障点的多步骤系列流程。	✓	

监控和审计用户访问

寻找具有以下功能的解决方案：	IBM	其他供应商
包括开箱即用的自动化、可配置且先进的鉴证/再认证处理，帮助满足需求，比如访问需求的 Sarbanes-Oxley (SOX) 404 再认证。	✓	
提供单个身份 GUI，通过该 GUI 执行所有的管理功能，并追踪和审计身份事件。	✓	
将工作流作为解决方案必不可少的一部分，这样解决方案就可管理和监控所有的生命周期和配置事件，然后就可记录所有交易数据，以供法院审计和报告。	✓	
建立集中框架，管理和保护您的 SOA 环境。	✓	
为每个服务应用程序执行和管理合适的访问控制。	✓	
跨不同服务转换和映射不同的用户身份集。	✓	
跨组织筒仓和防火墙管理针对应用程序的身份。	✓	
建立身份信任管理框架，确保安全地进行交易。	✓	
端到端地传播所需的凭证，从接触点（比如 XML 网关）通过 ESB 到后端（比如 ERP 或大型机应用程序）。	✓	

Monitor and audit user access

寻找具有以下功能的解决方案：	IBM	其他供应商
追踪和收集所有日志事件，让您可以审计应用程序访问。	✓	
提供扩展的审计和详细的报告，您可以将报告提供给调解员、外审员和内审员。	✓	
提供审计轨迹，了解谁访问了什么内容，以及谁批准了这些访问权利。	✓	
与配置文件集成，为特权身份管理提供共享和特权的身份的自动化登录/登出。	✓	
提供对数据库、应用程序、服务器和大型机的特权用户监控、报告和审计。	✓	
支持开箱即用的主要法规和最佳实践，包括 ISO 27001、SOX、GLBA、FISMA、PCI-DSS、Basel II、HIPAA、NERC 和 COBIT。	✓	
在整个组织监控分布式和大型机环境，检测不符合法规的策略异常情况。	✓	
将所捕获的本地日志数据转化为易于理解的报告，调解人员及外审员和企业审核员无需任何平台知识就可加以使用。	✓	
提供易于使用的界面用于创建自定义报告，包括概况和详情、Top-N 及阈值报告。	✓	
提供常见的报告系统，用于跨所有方案组件安排、分配、查看和自定义报告。	✓	

5. 加速价值实现

在您评估不同的身份和访问保障方案时，选择可快速实现价值的方案很重要。

经济高效的解决方案包括多项关键功能，这些功能旨在复杂的企业环境中轻松实现配置、集成和维护。

时间价值

寻找具有以下功能的解决方案：	IBM	其他供应商
提供所有必须的基础设施适配器、中间件和软件组件（包括所有必须的数据库）的先进商业版本、轻量目录访问协议 (LDAP) 服务器以及 Web 和应用程序服务器。	✓	
提供全面、开箱即用的功能，而对组件版本没有限制，比如必须升级才能获得所需丰富功能的工作流。	✓	
将最佳目录和数据集成及同步化工具与解决方案绑定，体面地解决集成挑战。	✓	
经全球数百位客户安装测试，证明有成熟可靠的功能。	✓	
拥有经验丰富的服务团队，确保在实施期间，生产力依然很高。	✓	

时间价值

寻找具有以下功能的解决方案：	IBM	其他供应商
能够满足您的异构目标需求。	✓	
可以与业内领先的 IBM WebSphereApplication Server 嵌入式集成。	✓	
实现自定义的身份验证，因此现有的基于 Web 的身份验证应用程序可快速集成到所有用户的验证流程中，而无需使用第三方部署工具。	✓	
包括大量功能，可与应用程序（包括 SAP、PeopleSoft 及 Siebel）集成，且支持多个目录/用户库和异构中间件（包括 Oracle WebLogic Server 和 Microsoft SharePoint）。	✓	
支持本地语言，且合并动态语言支持，以每个用户喜好的语言显示针对部署的内容，比如密码挑战/回应问题或电子邮件通知。	✓	

时间价值

寻找具有以下功能的解决方案：	IBM	其他供应商
提供广泛的平台支持，包括Windows、UNIX、Linux on distributed、Linux on IBM System z® 和 IBM z/OS®。	✓	
实现品牌自定义（视觉和感觉）及自助用户界面的布局，同时在 fixpack 应用或其他升级期间保留任何现有的自定义，从而保护您的投资。	✓	
提供三级或更高级评估保障的常见标准认证，以实现 Web 访问控制、用户配置和 LDAP Directory 的关键功能。	✓	
支持标准配置和编程语言，而不是需要专门的脚本编写或工作流定义语言。	✓	
包括用以监控身份和访问保障方案的状况和可用性的工具。	✓	
将自助密码重置功能集成到服务台（帮助台）系统中，包括产生和关闭事件（故障单）。	✓	

6. 选择合适的身份和访问保障提供商

您所选择的提供商应该是受信任的合作伙伴，可支持您所有的身份和访问保障方案，帮您解决复杂性、合规性和成本问题。理想情况下，您也希望提供商在整个实施过程中都能给您支持。因此在选择提供商之前，一定要清楚以下三个问题：

您的供应商是否利用他们的技术支持您的组织目标？

寻找解决方案符合您的组织目标的供应商。他们的解决方案是否能够提高效率、缩短业务服务部署时间、降低成本、提高合规性并加快进入市场？

您的供应商是提供总体解决方案的一部分还是整个解决方案？

如果供应商只是狭隘地关注只能应对特定环境的解决方案，那么您可能会遭遇“安全岛”问题。在涉及多个供应商时，解决方案成本以及管理多个供应商所花费的时间都会急剧增长。寻找具有完整的身份和访问保障产品组合的供应商，包括 UNIX 和主机访问控制、Web 服务安全和联邦。

您的供应商的产品是否密切集成，以实现无缝的功能？

解决方案集成得越好，您在手动集成技术时所需的工作就越少。

您的供应商拥有怎样的全球团队？

如果您的组织具有国际办事处，您应该寻找拥有全球团队且具有可靠国际经验的供应商。确保供应商可利用他们自身的本地资源支持您的海外办公室。

在您需要时，是否可依靠成熟的支持组织利用其专业特长和涉及面来支持解决方案？

您的供应商应该提供具有高度反应能力和高效的客户支持。 找到一家拥有可靠支持组织的供应商，
以帮助您提高软件投资价值。

分析师们对供应商的解决方案是否一直高度评价？

寻找顶尖分析师通过多方面的独立分析和审查后认可的解决方案。

您如何确保供应商的稳定性，如何在当今严峻的经济条件下保持动力？

如今一个重大的经济问题在于供应商的稳定性和可行性。您应考虑从业时间长，具有稳固、前瞻性的战略，且具有能克服不利经济状况的资源的供应商。

您的供应商是否能够交付设计战略化、技术领先的产品？

在比较多种安全解决方案时，寻找良好设计的功能这一技术优势，这是智能化架构设计和对行业标准的广泛支持。

利用 IBM 满足您的身份和访问保障需求

当您开始评估身份和访问保障供应商时，您会发现 IBM 不仅提供最佳的解决方案，还提供跨安全产品组合的卓越广度和集成。只有IBM 能使您集中精力，在整个 IT 安全风险领域内，通过灵活且适应性强的方法，降低保证组织安全的复杂性，从而驱动业务创新。当您准备扩展到其他安全管理领域时，IBM 是您在支持长期安全目标时所需的受信任的合作伙伴。

IBM Tivoli® Identity and Access Assurance 可提供有效、安全和合规的访问，帮助组织确保合适的用户可及时访问合适的信息。 这种解决方案可提供全面的身份管理、访问管理和用户合规审计功能。它集中且自动化用户管理，然后关闭身份和访问循环，提供业内领先的功能，不仅可以指派和执行用户访问权利，还可以监控用户行动并检测和校正不遵守安全策略的情形。组织可以选择实施 Tivoli Identity and Access Assurance 解决方案，或者从这些功能的子集开始，解决具体即时的需求，然后扩展解决方案，随着需求增长提供其他功能。

IBM Tivoli Identity and Access Assurance 与一套广泛的身份库交互操作，轻松地处理大量用户，实现流程工作流的自动化，从而提高管理效率，并最大程度地减少代价高昂的错误。.为了支持合规，自动捕捉并集中核对用户访问活动，并总结安全遵从仪表板的信息。 监控报告让您了解用户活动是否符合组织的权利和策略。仪表板和报告也会突出异常或不符合策略的活动，从而加以解决和校正。

IBM Tivoli Identity and Access Assurance 让组织可以通过基于角色的门户实现协作，促进新服务的快速导出，并实现单点登录，从而改善服务。

Tivoli Identity and Access Assurance 可提供单个供应商的解决方案，降低复杂性和总体拥有成本 (TCO)，从而帮助组织减少在整个用户生命周期中用以管理账户、组、策略、凭证和访问权利的费用，同时让用户可以快速访问所需资源。最后，依靠该解决方案对合规工作提供的整合支持，包括集中且自动化的合规报告、健壮的用户活动监控以及强大的密码策略执行功能，组织可以更好地管理风险。

IBM 可帮助提供支持如今的安全需求所需的基础设施，其对象可以是通过云计算、SOA、门户、Web 站点提供的访问，也可以是企业网络提供的访问。

除了管理用户身份和资源访问，为身份和访问保障建立集中且自动化的基础设施还可最终促成一项业务，帮助您：

- 尽量减少提供安全环境保护您的数据的复杂性。
- 遵从内部和外部需求，以安全地访问资产和信息。
- 自动化地实现可重复任务的最佳实践，从而优化生产力和成本。
- 解放 IT 员工，使他们关注较高价值的活动。
- 通过移除创新障碍，获得利用新的商机所需的敏捷性。

更多信息

要了解更多关于 IBM 身份和访问保障方案的信息，请联系您的 IBM 销售代表或 IBM 业务合作伙伴，或访问：ibm.com/tivoli/security。

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

在美国印刷
2010 年 6 月

更多关于选择合适的安全信息和事件管理方案的信息，请查看 **ibm.com**/common/ssi/fcgi-bin/ssialias?infotype=PM&subtype=RG&appname=SWGE_TI_SE_USEN&htmlfid=TIO14001USEN&attachment=TIO14001USEN.PDF 的 IBM 安全信息和事件管理方案买方指南。

请回收利用