设计专为您的企业而优化的身份和访问管理计划

有助于立即构建更成熟解决方案的四大关键步骤

亮点：

采用审慎的身份和访问管理方法有助于确保满足与安全、生产效率或合规相关的目标，包括短期目标以及随着组织在未来的继续演变而设定的目标。

目录

1 引言
2 超越“好坏之分”
3 成熟 IAM 计划的支柱
7 系统崩溃时
7 深思熟虑的成熟之旅
8 第 1 步：评估
9 第 2 步：设计
10 第 3 步：执行
10 第 4 步：立即采取行动

引言

在当今复杂且分散的 IT 环境中，身份和访问管理 (IAM) 计划所要实现的不仅仅是简单地管理用户身份并授予访问权限。它们是实现与每个高绩效组织相关的关键业务目标的核心。如此一来，鲜有 IT 或安全计划要求同样程度的考虑和审查。

针对业务目标和其相关独特情况而优化的成熟 IAM 计划可以减少涉及身份的数据泄露风险。它可以帮助企业提高生产效率和协作能力，进而在市场上实现真正的竞争优势。此外，它有助于确保更系统地实现和维持合规管理，同时降低审计执行业务的成本。

不过，在使用单点技术解决方案的情况下，随着时间的推移会导致 IAM 计划零散、停滞且不完整，进而导致许多组织无法实现这些目标中的一个或多个目标。如此一来，企业将会面临遭受重大损失的风险，而错过了基于敏捷、互联员工队伍的竞争优势。

在现有 IAM 计划的成熟度推进方面采用审慎的方法可以实现有助于直接提升业务绩效和安全态势的优势。这种方法能够通过自动化降低成本，通过集成技术框架提升运营效率，还可以通过适当的规划支持更成功的实施项目。

60% 的攻击是由内部人员实施的

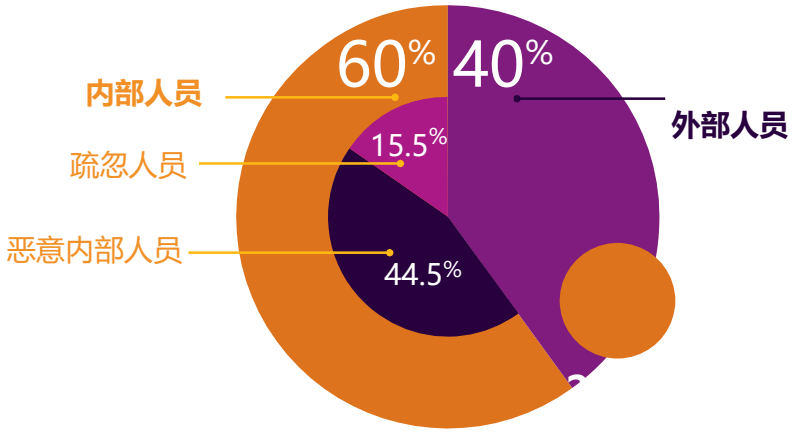

图 1: 谁是“坏家伙”？

超越“好坏之分”

如今的 IAM 解决方案需要实现的不只是“让好的进来，让坏的出去”。这是因为越来越多的安全漏洞是内部人员造成的，无论他们是恶意的还是无意的。当员工共享密码或丢失公司数据时 - 或第三方在没有足够防护措施的情况下将信息置于险地 - 即使是“好家伙”也会构成安全隐患。

IBM® X-Force® 发布的相关报告发现，在调查的攻击中，有 60% 的攻击是由于内部人员导致的。[1] 其中，有 15.5% 的攻击是由于内部人员疏忽所致。他们经常会在不知不觉中被带有恶意企图的攻击者所利用，进而成为实施极具破坏性的攻击（甚至可能是长期攻击）的关键参与者。此外，由于他们是内部人员，因此可以在不引起任何怀疑的情况下做到这一点，具体来说就是：他们会通过与公司网络连接的设备登录到社交媒体网站，或者点开由看上去合法的业务联系人发送的电子邮件附件。

然后是恶意内部人员，剩余 44.5% 的攻击是这部分人员所致，这些人员的行为从根本上说就是恶意的。令人不安的一个事实是，仅仅因为他们被视为“内部人员”，并不意味着他们就可以被信任。因此，要切记的重要一点是：情况和关系会随着时间而改变 - 并非总是会向更好的方向发展。

1 IBM 网络安全情报指数（2016 年）http://www-03.ibm.com/security/data-breach/cyber-security-index.html

成熟 IAM 计划的支柱

针对组织的需求和独特情况进行了优化的 IAM 计划有助于增强合规管理功能、确保经授权用户能够方便地访问数据并保护有价值的数据。每个组织在技术成熟度方面都会有不同的要求，而且会在不同的条件下制定 IAM 计划。

不过，成功的 IAM 计划都有一个共性：它们包含身份保证、身份智能和治理功能，它们以集成的方式在整个组织的 IT 环境中保持一致。如此一来，组织能够实现适当级别的访问控制和安全性，而不会损害生产效率，也不会带给用户难以承受的登录体验。

在多边界世界中增强身份保证

许多组织仍然采用简单的密码作为身份证明。但是密码是静态的，本质上不利于确保安全。大多数用户都会选择最省力的方式，也就是使用易于记忆的密码，但这些密码却容易被窃取、破解和破坏，并导致系统暴露在欺诈性攻击风险中。一旦攻击者破译了静态密码，便可轻松地模拟原始用户并获得对多种类型的机密数据的访问权限。由于许多用户通过单点登录受益，或在许多企业系统中重复使用相同的密码，因此存储在应用之中的数据即便与最初的数据泄露事件几乎无关，也可能会受到威胁。此外，如果您觉得这一点还不够的话，还有重要的一点是：静态密码也容易受到各种网络钓鱼和木马的攻击。

若要防止欺诈性访问，用户必须能够在访问公司资源的情境中证明其身份。该情境可能包含他们正在使用的设备类型、位置或活动方式。最新的安全技术可以使用该情境来确定特定用户是否获得访问授权。

使用情境数据分析来分析风险，组织可以基于对事务和相关用户的动态评估来授予访问权限。举例来说，如果一名北美地区的工人突然在非洲使用移动设备，软件便会记录情境的异常变化，而且可能要求用户提供其他身份证明，例如一次性密码等。在某些情况下，可能会因为认为安全风险过高而拒绝用户访问某些 IT 资源。

通过要求用户进行多种形式的身份验证，组织便可确保向适当的用户授予对受保护资源的访问权限，并防止那些不应访问此类资源用户访问此类资源。除了提升访问请求的安全性之外，利用情境信息还可以让最终用户的体验更加流畅，从而提高他们的生产效率。在低风险尝试中，用户体验可以毫无摩擦。

可以通过结合采用复杂策略引擎（或理想情况下的风险引擎）与多种身份验证方法（从生物特征识别到针对移动设备进行了优化的推送通知再到硬令牌）来增强最终用户的身份保证。通过策略引擎，管理员可以为每个访问请求设置特定规则，而要实现良好的身份保证还有很长的路要走。风险引擎则更进一步 - 当用户请求访问受保护的资源时，系统会计算风险评分并确定在满足条件后是允许还是拒绝访问。

将身份智能整合到流程中

随着安全威胁变得越来越复杂，风险和合规的压力持续增长，企业也日益需要一种将风险控制融入到结构之中的新的主动身份管理方法。如今最有效的身份管理解决方案是将权利管理与特权控制和“身份情境感知”安全智能结合在一起。

与特权身份管理相集成

特权 ID 是指对企业资源（包括服务器、网络设备、数据库系统和企业资源规划应用）具有特殊或额外权限的任何帐户。当然，攻击者攻击特权 ID 的威胁会带来明显的风险。但是风险远不止于此。设有特权帐户的组织的授权用户也可能对其 IT 基础架构的安全构成威胁。与此同时，组织越来越多地将特定的管理任务委托给员工和承包商处理，这进一步增加了特权帐户相关风险。

设有特权帐户的组织的授权用户也可能对其 IT 基础架构的安全构成威胁。

正因为如此，以下各种措施才会如此重要：

- 优先考虑特权身份需求
- 识别并监控最高风险的用户
- 了解哪些用户有权访问敏感数据和系统
- 制定正常行为基准。

满足这些需求的最实用方法是使用允许 IT 人员共享特权 ID 的成熟身份管理系统。这样的系统必须包括：

- 一个凭证保险库，用于将凭证安全地存储到特权 ID
- 一种签出签入机制，允许特权用户在必要时（使用密码）签出 ID，以供独占使用且限定期限；然后在完成后签入 ID，这时密码会自动更改
- 一种集中配备和管理与各种资源相关的 ID 的方法
- 决定哪些用户有权访问哪些 ID 的角色和策略
- 用户请求访问 ID 和管理者批准请求的流程
- 集成的审核日志，此类日志向安全智能解决方案馈入信息，以记录所有签出签入活动，并显示在特定时间段内哪些用户可以访问哪些 ID。

这种解决方案能够让组织：

- 避免与其资源链接的特权 ID 扩散
- 允许特权用户在需要特权时访问特权 ID（仅在需要的时长内）
- 让特权用户对他们所拥有或签出的 ID 负责
- 将 ID 和访问策略的管理任务委派给各个资源所有者
- 收集身份属性，并将此类数据结合日志事件和网络流数据规则一起使用，以提供“身份情境感知”安全信息。

与身份智能相集成

有多种安全智能解决方案（包括安全信息和事件管理系统）可以提供可用的日志文件和度量标准，用以识别异常、突出有风险的行为或不当行为，并协助进行合规报告。通过将身份和访问管理功能与这些解决方案相集成，组织可以将输出与日志事件和网络流数据相结合，以开发“身份情境感知”安全智能。借助针对整个企业范围内不同安全领域的活动的扩展视图，同时通过将身份和访问管理数据与其他重要安全事件相关联，组织可以更快地发现不当或可疑用户行为（包括内部威胁），并显著缩短威胁响应时间。

通过身份和访问治理来解决合规需求

几乎每个行业都面临着某种程度上的合规需求。全球的许多政府法规都强调了可视性和可控性对于个人用户的权利和访问特权而言的重要性。

随着对安全和隐私问题的关注日益加深，加上公司监督和治理再次得到关注，风险管理和合规措施正在被推向业务前沿。因此，组织必须证明他们具有强大而一致的访问控制，以满足其自身和业务合作伙伴的合规需求。

当用户的访问级别过时或不适当时，很可能会发生安全泄露事件和合规问题，进而增加了出现内部人员威胁活动的可能性。外部攻击者经常会寻找那些控制和管理不善的用户访问计划所提供的“易得手猎物”。因此，仅仅制定一个可靠的身份和访问管理计划是远远不够的。您还需要保持它能够正常发挥作用。

案例研究：客户管理领域的一家全球领先企业简化并改进了其身份和访问管理计划

最近的合并和收购活动，加上组织变更所造成的中断，突显了该公司对更健全、敏捷且一致实施的身份和访问管理解决方案的需求。

IBM 评估了该公司的业务优先事项，确定了与身份和访问管理相关的优缺点，并根据行业标准和最佳实践对其进行了评估，进而制定了明确的业务驱动战略路线图，以期改善该公司的身份和访问管理能力。

借助 IBM 的身份与访问管理服务，该组织将其管理身份和访问管理筒仓整合到单个通用框架中，该框架旨在通过基于标准的通用、可复用的组件、技术和服务来降低成本和复杂性。最终，该公司能够更好地避免和减轻合规风险。

通过治理降低风险

身份和访问治理能够指导企业如何定义用户角色、如何在用户的整个生命周期中配置、管理和实施访问。

专为管理用户访问需求而设计的解决方案，具有更好的问责机制和透明度，可帮助您更有效地管理和实施用户访问。这些工具可以帮助管理员确保用户帐户和特权得到更新并适合其角色。此外，身份和访问治理可以帮助组织更全面、统一地控制谁可以使用哪些资源。

身份和访问治理计划的策略驱动型方法应包括：

- 规划身份和访问治理战略
- 定义身份和访问治理的标准、流程和控制
- 实施身份和访问治理
- 监控、衡量和报告身份和访问治理计划的有效性。

系统崩溃时

大多数企业之前早就开始在 IAM 上进行投资，其后又进行了一系列投入，以期实现不同程度的现代化。尽管这些实质性的实施奠定了一个很好的基础，而且通常具有前文所述的支柱元素，但随着时间的流逝，它们往往无法跟上组织不断发展的 IT 格局的步伐。结果，它们再也无法抵御内部威胁或身份欺诈，无法为业务线提供支持，也难以实现合规性。

这种现象是由几种因素所致。各种业务职能部门在云应用采用方面通常以筒仓的方式进行，同时采用并行的方式来管理访问（有时甚至是在 IT 人员不了解的情况下完成的）。如此一来，这些措施不会自动包含在中央策略管理系统中。随着组织由于并购 (M&A) 或重组，或者仅仅是因为有机增长而变得愈发复杂，这些问题会迅速加剧。此外，用户的访问需求变得越来越不同，导致这些问题更加复杂。由 IAM 计划管理的最终用户组可以包括员工、合作伙伴、承包商甚至是客户，这些用户有时会自带设备甚至是通过社交媒体帐户自带身份。

大多数公司试图使用单点解决方案来跟上这些变化的步伐，以应对每一个不断增长的需求和挑战。但是随着时间的流逝，最终的结果是一个不再符合目标的零散 IAM 系统。相比之下，投入时间去专门设计一个针对特定目标而优化的 IAM 计划会带来诸多优势。

审慎的成熟度之旅

采用审慎的身份和访问管理方法有助于确保满足与安全、生产效率或合规相关的目标，包括短期目标以及随着组织在未来的继续演变而设定的目标。如此一来，组织会发现他们在 IAM 方面的投资会从仅提供最低限度的功能演变到能够为用户创造真正的价值并实现利润。

审慎的方法还使组织能够对其路线图进行优先排序，以解决最紧迫的问题。从长远来看，可以让团队从被动支出怪圈中跳脱出来，进而降低成本。

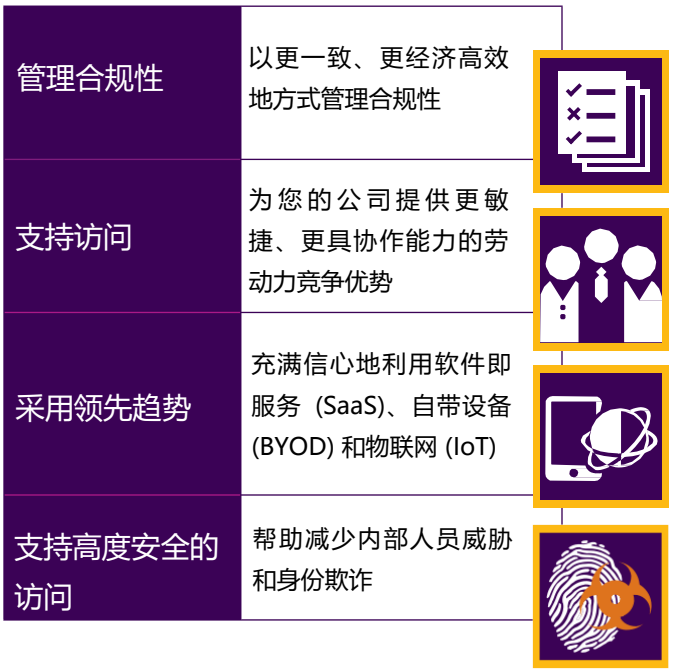

图 2: 针对您的组织量身定制的 IAM 计划有助于实现您的业务目标

对您的 IAM 计划进行未来验证

优化路线图

充分利用预算

图 3：采用审慎的身份和访问管理方法所能实现的优势

此外，该方法可以帮助组织避免过早跳到技术供应商选择怪圈这一高代价错误。IAM 项目涉及大量的业务重构。过早地专注于技术选择会导致企业无法专注于有助于确保 IAM 解决方案与业务目标紧密相关的核心活动。

审慎的身份和访问管理方法涵盖三个步骤。首先是***评估***当前计划的运行状况，以评估关键的 IAM 差距及其对组织的影响，以及 IAM 计划实现业务目标和 IT 目标的能力。第二步是***设计***可执行的 IAM 战略，以支持长期业务需求，并确定经优先排序的 IAM 路线图、时间表和预算需求，确保此类战略能够在业务情境中得到执行。一旦完成了这一步的战略性工作，便可为第三步打下坚实基础：***执行*** IAM 计划，将实现此类战略所需的产品、流程和人员汇聚到一起。

第 1 步：评估

从评估当前的 IAM 计划开始着手会带来许多优势。首先，组织可以执行运行状况检查，真正地识别出最紧迫的漏洞和痛点，而不仅仅是找出最受关注的问题。尽管大多数组织都止步于此，但这种方法意味着企业需要更进一步：不能单单从这些漏洞本身进行考虑，而是要放到更大的业务目标情境之中 - 通常是要在安全、合规和生产效率需求之间取得一定的平衡。这意味着不仅要重点关注最关键的痛点，还要帮助他们确定解决方案，以解决当前迫在眉睫的挑战，进而确保部署可实现业务目标的解决方案。

此外，投入时间敲定未来愿景，可以让组织从被动转变到更具战略意义的地位，进而确保系统不仅仅只是避免问题。不必在某个痛点无法避免时匆匆上马 IAM 计划然后再在后续修补，可行的做法是更好地预测未来的挑战并维持可控性。

通常，这种演练的附带好处是能够清楚地阐明分配给 IAM 计划的预算与以待实现的业务目标形式获得的明确投资回报之间的关联。提高最终用户的生产效率能够降低成本并增加收入，而且数据泄露风险的降低情况与合规投入均可量化。

在制定这一未来愿景时，重要的是要考虑组织所处环境的特定情况。需求会根据需要访问的用户类型、访问需求的可变性、用户所处位置及用户身份信息的存储位置而有所不同。合规压力也会因行业和运营所在国家/地区的不同而有巨大差异。数据泄露的风险因素还取决于受保护的信息，这会对安全义务造成影响。

对于每个组织来说，关于是否顺应新趋势、以什么速度来顺应的决策也具有唯一性。软件即服务 (SaaS) 应用、物联网 (IoT)、自带设备 (BYOD) 和自带身份 (BYOI) 等计划，提供了几乎无限的自定义选项集，组织可以根据自己的业务需求和情况优化选择。

第 2 步：设计

一旦对 IAM 计划的当前状态有了清晰的了解，并对未来状态目标有了明确的构想，便可以根据合理的时间表和预算设计一个路线图，以从一种状态转变到另一种状态。

在该框架内，可以对现有资产进行评估，优化其价值、减少低效环节并提高成本效益。可以在考虑集成的情况下制定新解决方案的推出计划，以便始终如一地执行控制措施并消除 IAM 筒仓。可以确定关键标准，以便在将来的购买时选择供应商和技术。

最终结果是明确了经过优先排序的路线图和清晰的时序计划，这些有助于充分利用现有技术并以适当的顺序实施新技术。如此一来便可达到更高的项目实施成功率和正的投资回报率。

第 3 步：执行

在该阶段，投入更多的时间和精力来评估当前的 IAM 计划，并设计适合业务需求的未来状态，便可显示其价值。项目和支出建议书可以更快、更轻松地获得批准，因为请求具有结构和目的，会将它们与总体业务需求联系在一起。这也有助于为每次部署和实施提供清晰、可量化的成功度量标准。最后，由于可以提前充分了解并简化需求和业务流程，因此可以大大降低 IAM 产品的部署成本。

有了适当的支持、期望和准备，就可以有条不紊、成功地将必要的人员、流程和技术结合在一起，确保战略得到执行。

第 4 步：立即采取行动

尽管如今有许多组织采用了旨在保护其系统、应用和数据免遭未经授权访问的长期战略，但对于真正全面的身份和访问管理战略的需求却往往未得到满足。不过如今，身份显然已经成为一种新的安全边界，需要通过控制措施来管理、实施和监控用户权利及访问活动，因此正是需要采取行动的时候。

IBM 的身份和访问管理服务可以通过一种整体方法为您提供帮助，而 IBM 因为这种方法所提供的服务和技术被认可为安全解决方案开发和交付方面的领导者。我们的身份和访问管理服务专注于当今企业 IT 和业务线经理面临的关键安全挑战，可帮助他们：

- 保障移动、云和社交互动
- 防范内部人员威胁和身份欺诈
- 简化身份筒仓和云集成
- 提供智能身份和访问保证

我们可提供各种专业和托管的服务，包括：

- ***身份和访问战略与评估服务*** - 业务和技术咨询，可帮助客户设计适合其业务需求的 IAM 计划。该产品旨在提供可行计划，以增强合规管理功能、确保经授权用户能够方便地访问数据并保护有价值的数据。

  这种方法使用系统且强大的成熟度模型，可以帮助客户优化 IAM 计划，并在其预算要求内、按照经过优先排序的项目列表在合理的时间内执行计划。

- ***身份和访问管理设计与实施服务*** - 久经时间考验的最佳实践框架和方法，用于设计和实施解决方案，帮助企业维持对移动设备的安全控制，减轻内部和外部威胁，降低云环境中的安全风险并自动执行合规管理。

- ***身份和访问管理托管服务*** - 内部、托管或基于云的交付模型，提供了一系列功能，包括用户配置、生命周期管理、单点登录、企业用户注册表服务、联合身份验证和多重身份验证等。

图 4: IBM 可以提供端到端解决方案，支持您从 IAM 战略评估和设计到执行的所有 IAM 相关需求。

长期以来，IBM 一直是安全解决方案领域的公认思想领袖，而且是能够提供从战略开发到设计、构建和管理的端到端身份和访问管理解决方案的少数服务提供商之一。我们的安全专家会与您紧密协作，解决您的独特需求，并提供最适合您业务目标的解决方案。

有关更多信息

如欲了解 IBM Security Services 如何帮助您降低成本、提升高级威胁防范能力的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：
ibm.com/services/security

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

美国印刷
2016 年 7 月