IBM Security

Designing a modern IAM program for your business

IBM

Three critical steps to a successful journey

Introduction

Identity and access management (IAM) programs provide security and risk leaders thorough practices, processes and technologies to manage identities and entitlements of people, services and things. These programs also cover the relationships and trust among those people, services and things. In today's complex and distributed IT environments, modern IAM programs should do much more than simply provision user identities and grant access. IAM programs are at the core of achieving critical business objectives and relevant to every high-performing organization. As a result, few IT or security initiatives demand as much deliberation and scrutiny than IAM.

A modern IAM program moves beyond established tooling and focuses on outcomes and the elimination of technical debt or heavy customizations that hinder the organization's ability to deploy at scale. Modern IAM programs shift the focus from tactical or manual operations to more of a strategic function that's optimized to a business's objectives. In addition, the distinctive features of a modernized IAM program can help reduce the risk of data breaches involving identities and credentials. These programs can help improve productivity and collaboration, delivering a competitive advantage in the market. Finally, a modern program can help ensure that regulatory compliance management is more systematically achieved and maintained, while reducing the costs of remediating audit findings involving IAM.

Many enterprises that seek digital transformation find that IAM programs are key to this change initiative. The optimization strategies of digital transformation include modernization of workplace tools, migration to the cloud, integrating Software as a Service (SaaS) and on-premises applications, work-from-home initiatives, and expanding customer engagement channels. These imperatives can deliver recognized business value and a competitive advantage. Likewise, IAM has a significant opportunity to deliver direct business value by enabling lower-cost, risk-managed interactions with vendors, partners and customers and help enhance the overall user and customer experience.[1]

[1] Hype Cycle for Identity and Access Management Technologies, 2020, Gartner, 16 July 2020.

Three critical steps to a successful journey continued

IAM programs allow end users, stakeholders, suppliers and vendors to access resources seamlessly, rapidly and efficiently, so that the right user is granted the right access to the right protected resources under the right conditions.

82% of CEOs have a digital transformation or management initiative[2]

But many organizations fail to meet one or more of these objectives due to fragmented, stagnant and incomplete IAM programs that have been developed over time using monolithic point-technology solutions. As a result, businesses face significant risks of failure and can lose the competitive advantage of an agile and connected workforce.

Traditional IAM programs also face the following pressures:

- **More complexity**—Businesses typically add more applications, information, methods of access and user entitlements as needed.
- **More focus on the user**—Increasing expectations to protect personally identifiable information (PII) and deliver seamless user experiences.
- **More regulations**—New and evolving standards required for accessing and sharing PII and sensitive information.
- **More security tools**—On average, organizations are running 25 to 49 different security tools from up to 10 different vendors.[3]

Taking a deliberate approach to modernizing an existing IAM program can lead to benefits that directly improve business performance and security posture, such as the following results:

- Reduce costs through automation
- Deliver operational efficiency for people and systems through an integrated technology framework
- Help support more successful implementations through proper planning
- Improve risk analyses
- Lower the cost of compliance
- Enhance the customer and workforce experience

[2] 2019 Gartner CEO and Senior Business Executive Survey, Gartner, May 2019, www.gartner.com/smarterwithgartner/ceos-look-for-growth-opportunities-in-2019-ceo-survey
[3] ESG Brief: Cybersecurity Landscape: The Evolution of Enterprise-class Vendors, November 2018, research.esg-global.com/reportaction/cybersecuritylandscape/Marketing

Pitfalls of not adopting a modern IAM program

An IAM program optimized to meet the needs and unique circumstances of an organization helps enhance regulatory compliance management capabilities, grant convenient access to authorized users and protect valuable data. But without using a modern IAM program framework, a business can face the following significant hurdles:

– Added time and costs of manual IAM processes

– Poor user experiences

– Lack of skills to deploy modern solutions

– High technical debt with monolithic customizations

– Poor innovation and productivity from employees

The potential rise in costs is also a factor especially troublesome for enterprises lacking a modern IAM program. According to the 2020 Ponemon Cost of an Insider Threat report, the costliest insider threat per incident is credential theft. These incidents have increased significantly in frequency and cost. In fact, the frequency of incidents per company has tripled since 2016 from an average of 1 to 3.2, and the average cost has nearly doubled from USD $493,093 in the same period.

$871K+

Average cost per incident of theft of credentials for enterprises in 2019.[4]

For organizations that want to improve the accuracy and speed of providing access to the right person at the right time under the right conditions, the need for a modern IAM program is paramount. But other compelling reasons for the implementation exist that security and IT leaders at enterprises should consider as well.

[4] Cost of Insider Threats: Global Report 2020, IBM Security, Independently conducted by Ponemon Institute, 2020, www.ibm.com/downloads/cas/LQZ4RONE

Why a modern IAM program matters

Among the incentives to transform to modern IAM is to assist future growth. By shedding a traditional IAM program, enterprise officers move beyond tooling to focus more on outcomes and the elimination of technical debt or overly customized solutions. With an Agile approach, organizations can rapidly deploy a modern IAM solution to automate workflows. The shift to more strategic use cases frees up IAM resources for other high-value projects. The result is that enterprises can prepare for microservices that deliver more value, deliver an advantage in the marketplace and make IAM smarter through the use of automation to keep up with rigorous business demands.

Another important factor to consider is a seamless end user experience, whether for your workforce or your consumers. Gartner reports that 70 percent of IAM projects fail due to the lack of user acceptance.[5] With a modern IAM program, users need to feel a sense of ownership as new solutions are deployed. That experience can encourage widespread adoption and the success of an overall IAM program initiative.

The following other benefits can occur with a cloud-based IAM program:

- Reduced infrastructure and Infrastructure as a Service (IaaS) appliance costs — No additional hardware is necessary, even for scaling.
- Less time to deploy and maintain—Software updates, patches, version upgrades and related new features are immediately available.
- Ease of management—With no hardware failures or capacity issues to address, an organization should experience a reduced need for operational oversight while still having clear visibility into usage patterns.
- Opportunity for more secure operations—The infrastructure, platform and IAM application risks are outsourced to the providers, leaving the organization to focus on securing data and access to endpoints.

While these opportunities have appeal, implementing a modern IAM program does require tradeoffs for enterprises. All parties have to prepare for performing operations differently than they had previously. A big technology change impacts user experiences and can cause adoption challenges. What businesses need to do is retain and redeploy resources to the new operating model and continue to improve the IAM program to be most effective.

[5] Predicts 2020: Identity and Access Management, 9 December 2019, www.gartner.com/document/3976106

The pillars of a modern IAM program

Businesses with the most successful IAM programs share a common factor. They employ identity assurance, identity intelligence and governance, working in an integrated fashion, consistently across an organization's IT landscape. All elements are essential to have in place for maximizing the potential that a modern IAM program can provide.

Enhancing identity assurance in a world without perimeters

Many organizations still rely on passwords as proof of identity. Passwords with eight characters using one special character and a number are still static and inherently weak. Static passwords are vulnerable to a wide variety of phishing and social engineering attacks. Because many users benefit from single sign-on (SSO) or reuse of the same password across many enterprise systems, data stored in applications far removed from the initial breach can be compromised.

To help prevent fraudulent access, users must be able to prove their identities within the context in which they're accessing corporate resources. That context could encompass the type of device they're using, their location, or their patterns of activity. The latest security technologies can use this context information to determine whether a specific user is authorized for access.

Using contextual data analytics to analyze risk, organizations can grant access based on a dynamic assessment of the transaction and the user in question. For example, if a North American worker suddenly uses a mobile device from Africa, the software notes an unusual change in context and may require the user to provide additional proof of identity, such as a one-time password. In some situations, the user may be denied access to certain IT resources because the security risk is deemed to be too high.

The pillars of a modern IAM program continued

By requiring more than one form of authentication, organizations can help ensure that the following events occur:

– The right user is granted the right access to the right protected resources.

– Those without correct authentication can't access those protected resources.

Increasing the security of an access request and multiplying its context makes the experience smoother for the end user and increases their productivity. In low-risk attempts, the user experience can be frictionless.

Enhancing end users' identity assurance can occur by combining a variety of authentication methods, from biometrics, to mobile-optimized push notification, to hard tokens, with a sophisticated policy engine, or ideally, a risk engine. A policy engine enables administrators to set specific rules for each access request and goes a long way toward achieving good identity assurance. A risk engine goes one step further. When a user requests access to a protected resource, the system calculates a risk score and determines whether access may be permitted, denied, or permitted after a condition is met.

Integrating identity intelligence into the process

As security threats become more sophisticated and the pressures of risk and compliance continue to grow, so does the demand for a more proactive approach to identity management. Today's most effective identity management solutions combine entitlement management with privilege control and "identity context aware" security intelligence.

A privileged credential refers to any account that includes administrative, special or super user permissions for enterprise resources, such as servers, network appliances, database systems and enterprise resource planning applications. The threat of attackers compromising a privileged credential poses an obvious risk to an organization's IT infrastructure, as do authorized users with privileged accounts. Organizations whose leaders delegate unaudited administrative tasks to staff and contractors introduce further risks associated with privileged accounts.

These reasons are why it's important for organizations to have the following processes in place:

– Prioritizing the need for account access applying least privilege principles

– Identifying and monitoring the highest risk users and privileged credential used

– Knowing and reassessing who has access to sensitive data and systems

– Developing baselines for normal and abnormal behavior

Integrating identity intelligence into the process continued

The most practical way to meet those requirements is with a sophisticated privileged access management system that incorporates a vault for privileged credentials. This solution allows organizations to achieve the following goals:

- Avoid the proliferation of privileged accounts linked to its resources
- Allow privileged users to access a privileged credential if, when and on the condition they need it—for only as long as they need it and for only the resources assigned
- Make privileged users accountable for the credentials that they've owned or checked out
- Collect identity attributes and use that data in conjunction with log events and network flow data rules to provide "identity context aware" security intelligence
- Record administrative sessions for review of tasks and actions should an incident occur

Security intelligence solutions, such as security information and event management (SIEM) systems, can provide usable log files and metrics that help identify anomalies, highlight risky or abnormal behaviors and assist in compliance reporting. By integrating identity and access management or privileged access management with these solutions, organizations can combine that output with log events and network flow data to develop "identity context aware" security intelligence.

With an expanded view of activities across different security domains throughout the enterprise—and by correlating identity and access management data with other important security events—security and risk leaders can address two challenges. They can more quickly uncover inappropriate or suspicious user behavior, including insider threats, and significantly decrease threat response times.

Addressing compliance mandates with identity and access governance

Countless government regulations around the world stress the importance of visibility and control for individuals' entitlements and access rights. Escalating security and privacy concerns and a focus on corporate oversight and governance have put risk management and compliance measures in the business forefront. Organizations must prove that they have strong and consistent access controls to meet their compliance requirements and those of their business partners.

It's far more likely that security breaches and compliance issues can occur when users have outdated or inappropriate levels of access, driving up the potential for insider threat or credential theft activity. Outside attackers often look for the "easy prey" that poorly controlled and managed user access programs offer. This situation means enterprises must develop and keep a modern IAM program functioning properly.

Identity and access governance provides guidelines on how user roles are defined and how entitlements are granted. Access is provisioned, managed and enforced throughout the lifecycles of users, from joining, moving through and leaving the organization. In the case of consumer identities, access is provisioned through a concept called progressive profiling, where trust rises as consumers provide more of their PII and data through identity capture.

Identity governance solutions are designed to manage user identities and entitlements with greater accountability and transparency. This process helps IAM and security leaders govern and enforce user rights more effectively and efficiently. These governance tools can help administrators ensure that user accounts and privileges are updated and appropriate to their roles. In addition, identity and access governance can help organizations implement more thorough and consistently enforced control over who can do what with specific resources.

A policy-driven approach for an identity and access governance program should include the following elements:

– Planning for an identity and access governance strategy

– Defining standards, policies, processes and controls for identity and access governance

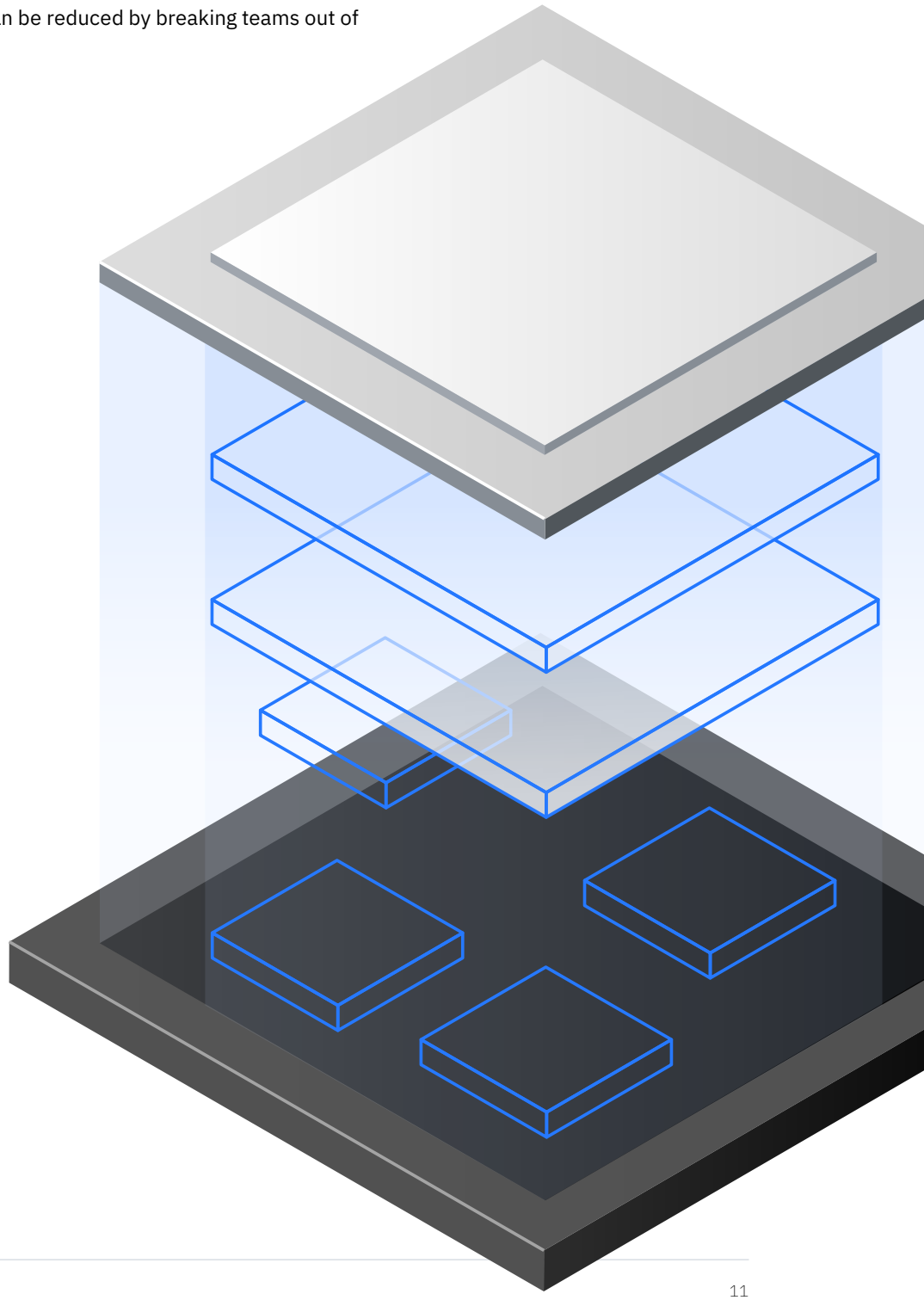
– Enabling the implementation of identity and access governance

– Monitoring, measuring and reporting on the effectiveness of the identity and access governance program

A deliberate journey to maturity and modernization

Taking a deliberate approach to identity and access management helps ensure that business objectives related to security, productivity, or compliance can be met in the short and long term. Organizations can watch their IAM investments grow from providing the bare minimum function to creating long-term value for their users and their bottom line.

A deliberate approach to IAM also allows business leaders to prioritize their digital transformation and security roadmaps to address their most pressing issues. In the long term, costs can be reduced by breaking teams out of reactive spending cycles.



Total economic impact of modern IAM

To examine the potential return on investment (ROI) enterprises may realize from implementing a modern IAM program, IBM® commissioned Forrester Consulting to conduct a Total Economic Impact™ study. The purpose of the study was to evaluate the potential financial impact on organizations using a modern IAM program from IBM Security™ Identity and Access Management Services. The quantified benefits included the following results:

86% Lowered costs to onboard an IAM application onto the public cloud

$1.9M Three-year present value of resulting labor cost savings

96% Reduced maintenance hours to support IAM software and hardware

$323K

Three-year value of time savings; IBM Security Identity and Access Management Services, coupled with reduced hardware needed for cloud solutions, meant that the organization only needed a single employee to spend 20% of their time providing basic software upkeep.[6]

The following case studies also show how modern IAM programs from IBM Security Identity and Access Management Services have benefited enterprises in the areas of access, governance and privileged management.

[6] The Total Economic Impact™ Of IBM Identity And Access Management Services, A Forrester Total Economic Impact Study Commissioned By IBM, June 2019, ibm.com/downloads/cas/LWDNAK97

Access case study: An enterprise undergoes modern IAM transformation for better authentication

An organization faced high maintenance, support and operating costs with an existing dedicated hosted solution. Adding new features and capabilities was time-consuming and expensive. The enterprise had no automated monitoring of vulnerabilities within the established architecture, which led to expensive annual manual security assessments.

IBM Security Identity and Access Management Services helped the business's leader with designing and securing access for 220,000 internal and external users and setting up 40 new workflows to streamline core IAM processes.

These changes gave the enterprise a clear roadmap for migrating essential IAM functions to a cost-effective IAM solution in the cloud. Leaders had an end-to-end secured SSO for all IAM services and components. Additionally, users quickly and efficiently deployed SSO and authentication from the cloud with application programming interface (API) specifications that comply with new regulations.

Governance case study: A manufacturer implements identity governance to decrease administrative efforts and increase user productivity

A company with manufacturing plants and offices in various locations worldwide wanted to integrate an identity governance-based solution with its broader IAM infrastructure. The client's existing identity governance and administration (IGA) systems were heterogeneous, complex, difficult to maintain and costly to operate, as the systems required extensive manual intervention. Among many challenges faced was a wait time of up to 30 days for user provisioning to complete with all access.

IBM Security Identity and Access Management Services assisted with establishing a governance program and deployment of a chosen IGA solution to enable identity management of users. By implementing a governance framework, IBM provided additional functionalities including onboarding applications, user review and role-based access.

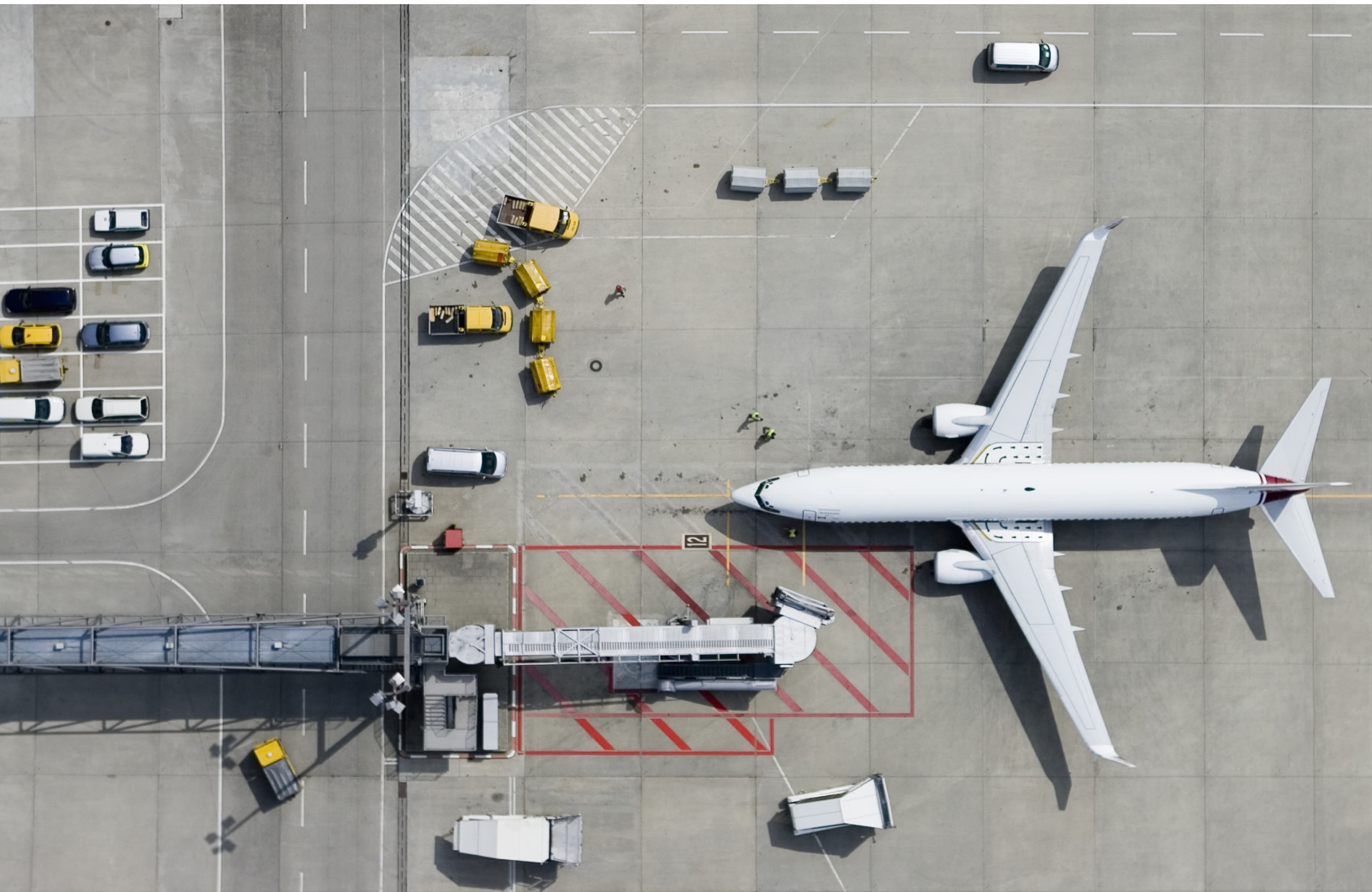
The benefits of the solution included allowing a unified user onboarding experience, which enables automated User Life Cycle Management. The manufacturer's security and IAM leaders received a centralized tool to manage users' identities and access across applications. The solution reduced the time frame for user provisioning and user access request as well.

Privileged case study: Airline uses privileged access management to get easier authentication process for audits and detection of suspicious activities

A large airline encountered problems with Payment Card Industry Data Security Standard (PCI-DSS) certification requirements to ensure secure storage and processing of payment card data. Its payment card data had inadequate privileged access protection, which prevented the company from being in scope for the certification. Additionally, poor visibility of privileged account activity made audits and the detection of suspicious activities difficult.

IBM Security Identity and Access Management Services provided Privileged Access Management (PAM) Services to help secure access for 1,000 privileged identities and 10,000 devices, and completed 15 target integrations for web- and client-based applications.

The changeover allowed the airline to meet the requirements of the certification audit by using two-factor authentication to access PCI. Users could access day-to-day applications without seeing the privileged account password. The IBM team also offered Managed PAM Services to monitor and manage all privileged identities in a password vault.



How IBM helps enterprises overcome three challenges

For most enterprises, three challenges can prevent a successful transition to a modern IAM program. Organizations need to address each challenge to implement an IAM program successfully.

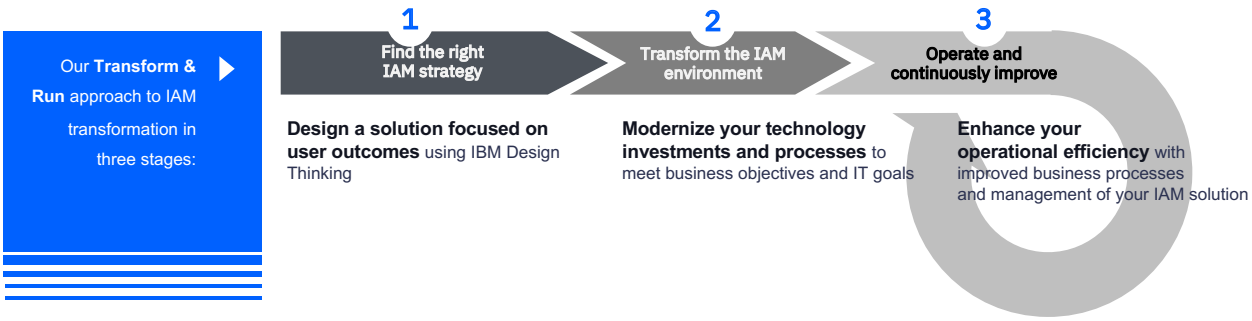
The first challenge is the planning stage. Business, security and risk leaders have to balance finding the right modern IAM strategy for their goals and user needs, while working within the realities of existing technology infrastructure and processes. High technical debt often requires a programmatic strategy to move from existing IAM infrastructure to modern cloud-based IAM infrastructure and processes.

In the second challenge—the transformation stage—IT leaders face pressure to lower infrastructure costs quickly. These demands can include the ongoing maintenance and licensing costs of on-premises solutions and the need to demonstrate success in changing IAM programs across various user types and populations. Additionally, leaders may find that customizations of on-premises implementations are often complex and difficult to discontinue.

The final challenge is the new operations stage. Business stakeholders have to continuously drive improvements in their businesses while retaining and redeploying valuable IAM talent to a new environment. Executives have to understand a phased migration of processes and technology is essential to have a thriving, ongoing modern IAM program.

To address each of these challenges, IBM Security Identity and Access Management Services suggests enterprises follow this transformational approach:

- Plan the right modern IAM platform, strategy and operational model for an organization.
- Design a journey to modern IAM and minimize user disruption while meeting business objectives and IT goals.
- Manage the change to enhance operational efficiency with IAM team members.



Here's a more in-depth exploration of how IBM Security consultants and specialists assist enterprises in overcoming these areas.

Planning

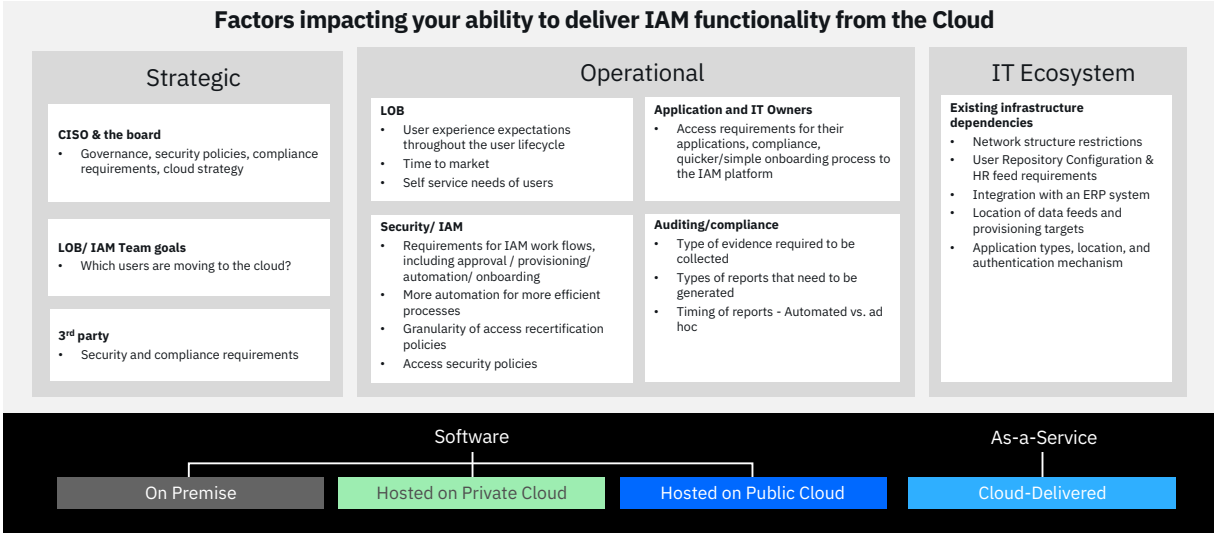
The planning phase starts with project planning and requirements gathering to determine the right approach in IAM functionality for an enterprise. Security and risk leaders need to determine what elements of their modern IAM program can stay on premises and what should go to the cloud.

This effort of modernizing IAM with a hybrid cloud architecture can be tricky to determine. On premises offers more possibilities for customizations, including greater flexibility, in-house control and full business workflow capabilities. However, a cloud-based IAM solution can provide more cost savings with higher agility, faster deployment and simplified operations.

To help leaders determine the best answer for their business, IBM Security recommends conducting a facilitated, specialized workshop using a framework called Enterprise Design Thinking. This workshop helps the organizational leaders identify and empathize with the needs of their end users and key organizational stakeholders. Using the findings from this workshop, the team members can then design a roadmap and target physical and functional architectures using industry best practices. When that solution is ready to be built, a team of identity specialists use an Agile approach to accelerate the test and deployment phases. The goal of this entire process is to align the business around which IAM challenges are the right ones to solve.

Factors to discuss in determining how to deliver IAM functionality to an organization from the cloud are focused around three categories: strategic, operational and the IT ecosystem. Strategic considerations include business objectives, desired outcomes and compliance requirements. Operational concerns encompass application requirements for access, granularity of access recertification policies and the types of evidence and reports needed for compliance and audits. The IT ecosystem focuses on existing infrastructure dependencies, such as network restrictions and application types, location and authentication mechanism.

Planning continued



Getting answers on these categories from the Enterprise Design Thinking workshop allows users to consider the extent and complexity of the IAM functionality for an organization. The target architecture customized for a business can include access governance, privileged access management, application onboarding, security integration and identity and access analytics.

The stakeholder alignment and buy-in of the end users helps with overall adoption to create a successful, long-term IAM solution for the organization. For example, employees can access their applications quickly because hiring managers can automatically approve access based on roles and policies already predefined. Or, the organization has successfully implemented SSO and multifactor authentication (MFA) for all IAM services and components, allowing seamless and productive work experiences. This strategic planning approach creates a more streamlined onboarding process than with traditional or more manual-based programs.

Transformation

Many security and risk leaders discover that various stakeholders and end users have different requirements in fast-paced business environments. Organizations may have delayed needed improvements for their IAM systems for so long that they're unable to keep up with business demands. That pressure can negatively impact the implementation of a modern IAM program during the transformation period.

With that consideration, organizations need to manage the changes in their work culture by building the right processes that workers can understand. Leaders need to emphasize protecting existing users and processes while deploying modern IAM solutions. The effort becomes a balance to ensure consistent delivery of the right access and governance processes. The transformation focuses on the best ways to deliver a cloud-based IAM solution that can benefit the organization without disrupting operations. By addressing this challenge, enterprises can get more agility and cost efficiency while freeing up technical debt previously generated by traditional IAM programs.

New operations

A final step organizations need to take when implementing a modern IAM solution is determining what ongoing management approach to use with new applications, cloud environments and connected devices. The following three levels of ownership to manage and optimize a modern IAM program should be considered while using the latest technology:

– Self-managed identity solution—The enterprise assumes ownership of the IAM infrastructure, including the costs of maintenance, support and licensing.

– SaaS platform deployment—The enterprise still manages a modern solution while consuming IAM from the platform.

– Managed identity handled by IBM Security Identity and Access Management Services—IAM is fully delivered and managed from the cloud or on premises and tailored to the enterprise's needs.

These different ways to manage a unified IAM experience all use functional management and landscape coordination provided by IBM Security. A managed identity solution can provide organizations with oversight on all modern IAM processes. Many enterprises find that scaling and adapting to their IAM scope can be most convenient and affordable using managed identity.

Take action now

IBM Security Identity and Access Management Services provides a holistic suite of services designed to address a multitude of identity use cases, including the following:

- Developing a strategy to optimize the performance and cost of workforce and consumer IAM applications
- Planning, maintaining, managing and optimizing a diverse IAM technology stack
- Deploying IAM applications to the cloud under an Identity as a Service (IDaaS) or PAM as a Service model
- Refactoring, rearchitecting, and developing new solutions to deliver business outcomes

With IBM Security Identity and Access Management Services, enterprise leaders benefit from a modern IAM solution that can help reduce complexity and accelerate time-to-value. Experienced IAM consultants and specialists can help organizations build the right strategy and operational model that combines people, process, technology and culture.

For participating enterprises, IBM Identity and Access Management Services can help partner and deliver the following benefits:

- Strategic advisors to your business
- Deep IAM subject matter expertise
- Worldwide presence and localized delivery
- Industry recognized security software and systems
- Leading security innovation and AI solutions
- Enterprise Design Thinking practices and principles
- Broader security technology ecosystem capabilities

For more information

To learn more about how IBM Security Identity and Access Management Services can help you plan, deploy and optimize a superior consumer or workforce identity solution, please contact your IBM representative or IBM Business Partner, and visit the following website: ibm.com/security/services/identity-access-management

IBM Security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
September 2020

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

9YBEK41O

IBM