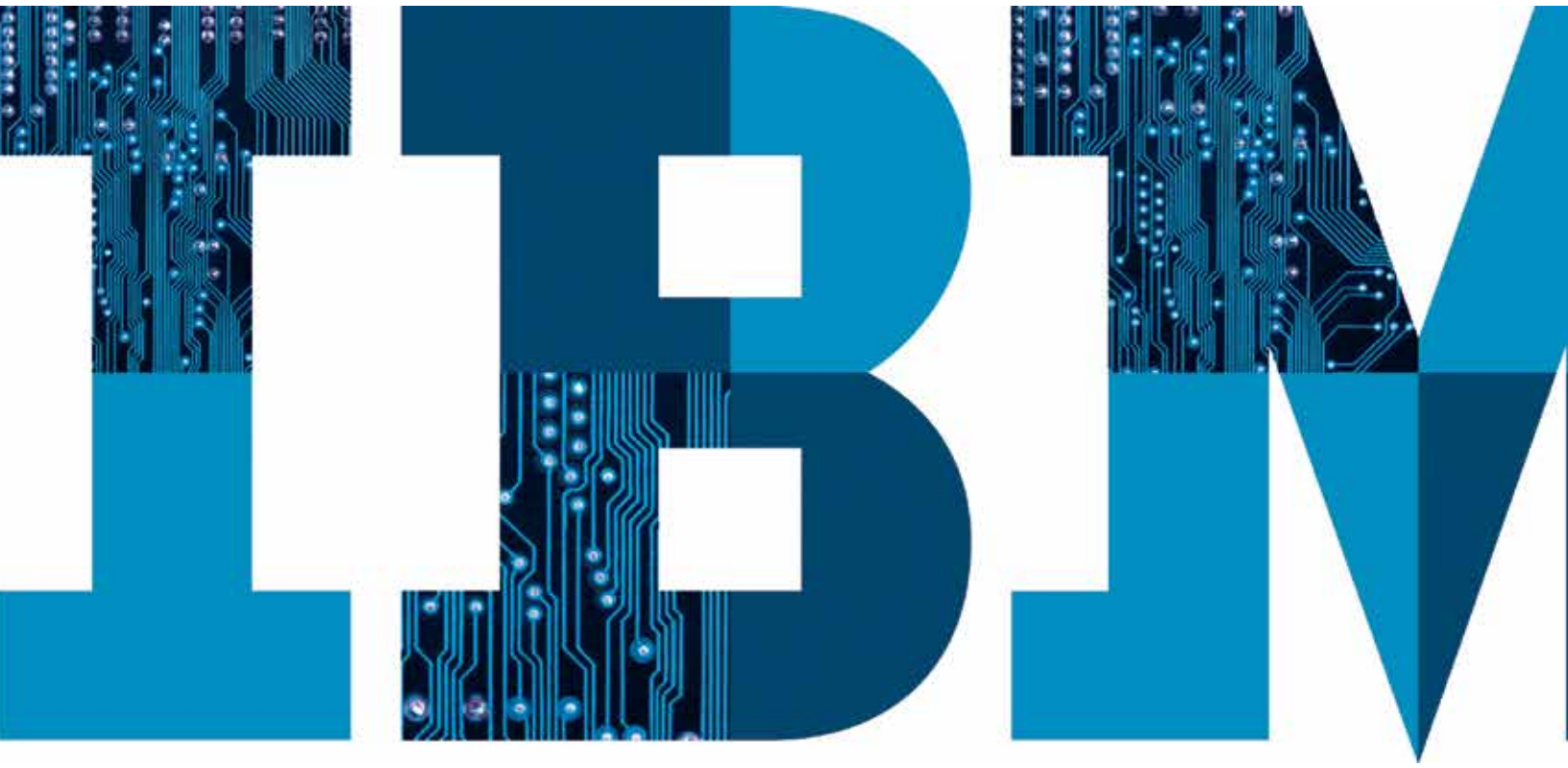
Building a next-generation identity and access management program

Four key steps that can move you toward a more mature solution now



IBM

Contents

Introduction

Identity and access management plays a key role in enterprise data defense. It's fundamental to determining who has authorized access to which resources, for what purpose and for how long. And in today's data-dependent organizations, there are few security initiatives that demand as much deliberation and scrutiny.

At its heart, identity and access management is all about providing people with secure and controllable access to online and enterprise resources, while simultaneously helping to protect those resources from unauthorized users. But the needs it addresses today have never been greater. And the challenges it involves have never been more complex.

Over the past 10 years we've seen enormous growth and change in the population of internal and external users. Employees, customers and business partners need greater access than ever before to more technology resources. They're using a new range of devices to access data and applications, which allows them to choose where and how to access those resources. Web-based collaboration with business partners, the need to grant access to third-party suppliers and online consumers, and the growing use of cloud-based services all continue to blur the organization's borders and expose it to both external threats and those arising from careless employees and nefarious insiders.

Going beyond good guys versus bad guys

Today's identity and access management solutions need to do more than just "let the good guys in and keep the bad guys out." That's because an increasing number of security breaches are the result of actions by insiders—most of whom are "good guys" inadvertently acting badly. When employees share passwords or lose corporate data—or third parties put information at risk with inadequate safeguards—even the "good guys" pose a security risk. A study of C-level executives conducted by Ponemon Institute study and sponsored by IBM, identified negligent insiders as the single greatest risk to sensitive data (see Figure 1).[1] Consider the various user groups that constitute the "good guys" in a given enterprise—including employees, contractors, suppliers, cloud and software as a service (SaaS) providers, and even customers—and it's easy to see why monitoring and managing user access is so critical to overall security.

An IBM X-Force® report found that negligent insiders comprise only five percent of the attacker population.[2] But those inadvertent accomplices, often unwittingly "recruited" to aid the cause of others with malicious intent, are becoming key players in carrying out highly damaging—and potentially prolonged—attacks. And because they're insiders, they manage to do so without arousing any suspicion, by logging onto a social media site from a corporate network-attached device or opening an email attachment sent by a legitimate-looking business contact.

Then there are the malicious insiders, whose actions are not at all innocent. They've recently been cited as the instigators behind 20 percent of sophisticated attacks.[3] The unsettling truth is that just because they're considered to be "insiders," it doesn't mean they can be trusted. So it's important to remember that situations and relationships can change over time—and not always for the better.

If you find all this surprising, it may be time to recognize that these kinds of problems don't just affect "other" organizations. And you might want to start asking some serious questions about whether your company's approach to identity and access management needs more attention.

The growing importance of the individual

Today's organizations are made up of individuals who are more likely than ever to have vast networks of online relationships—each of which involves huge amounts of personal data. But how can that personal data pose a threat to your company?

Rather than seeing a particular enterprise as only an individual entity, attackers now also look at an enterprise as collections of personalities. That means they decide to target specific people instead of enterprise infrastructures or applications. In other words, the personal lives and activities of employees can be leveraged to target an enterprise.

While that's a risk familiar to an organization's highest-level employees and spokespeople, who often have public-facing roles, it's a limited problem that's rarely been viewed as a major security issue. Now, however, that same risk extends to every individual who participates in social media activities.

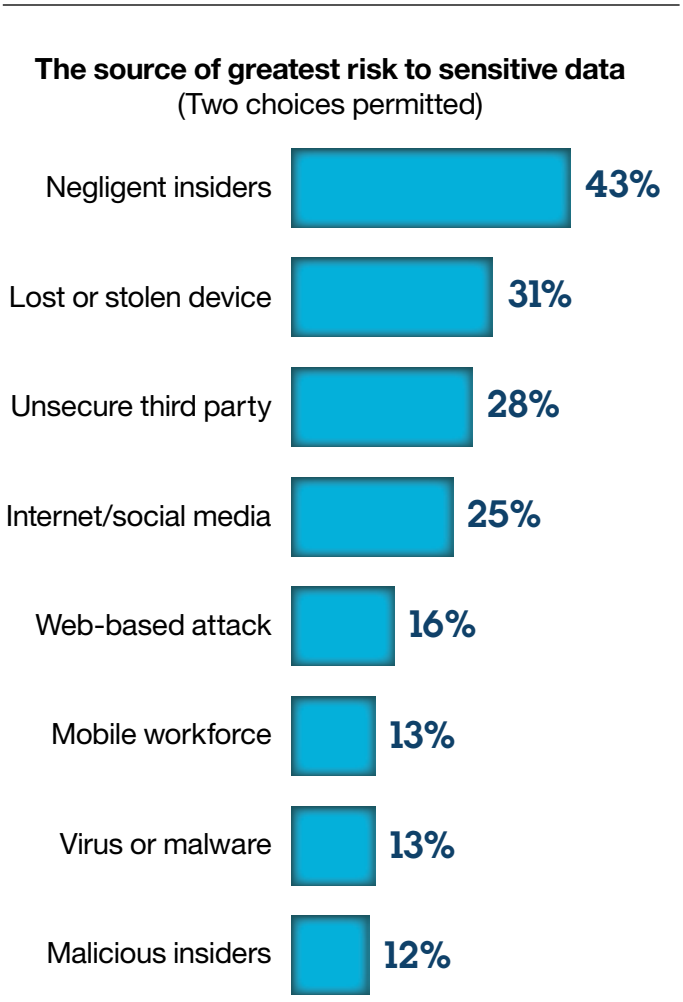


Figure 1. IBM and the Ponemon Institute surveyed more than 265 C-level executives to determine what organizations believe are the most important factors when considering sensitive data and complying with strict security regulations.

Social networks intentionally make it easy for users to contact one another. It's a great way to wish a faraway friend a happy birthday. But it's also an easy way for an attacker to send a user to a malicious website or to send malware directly to that user—all of which renders enterprise email security countermeasures completely useless. For example, a user can access social media using a corporate network-attached device and thus open up a pathway for the malware. Or an attacker can take advantage of personal information available online to learn enough about the individual to execute a targeted phishing campaign via the corporate email account. In this scenario the bad guy sends what appears to be legitimate business correspondence and dupes the employee into opening an infected email attachment.

Either way, the command and control malware gets into the enterprise systems. In addition, employees accessing work email outside the office—via mobile device or a home network—may inadvertently allow an attacker to bypass perimeter security completely.

The entire risk landscape, including identity and access management, has clearly become considerably more complicated over the past 10 years. And it points to four key steps that organizations must take if they're going to have a successful identity and access management program.

Step 1: Safeguard mobile, cloud and social interactions

Many organizations around the world are undergoing business and technological transformation, exploiting new technologies to increase efficiency, improve customer relationships and expand business growth. Thanks to the increasing popularity of BYOD (bring-your-own-device) programs, growing numbers of users are connecting their personal mobile devices to corporate networks after hours and off site, allowing them the flexibility to work anytime and anywhere—and simultaneously boost productivity.

They're also using cloud-based applications and services—such as SaaS tools for customer relationship management, office productivity and the like—to handle day-to-day tasks. With its cost-effective "pay as you go" model, elastic capabilities and self-service features, cloud computing continues to offer significant benefits to organizations of all sizes, across virtually every industry. As more and more businesses continue to take advantage of public cloud solutions, there's a fast-growing employee base that needs easy and secure access to these externally based services.

To attract and retain new customers, many businesses are also leveraging social media sites for user registration, providing a simplified and integrated customer social identity experience for authentication, registration, and ongoing online interaction.

That means those organizations' information and data are now being distributed beyond their traditional network perimeters. Not surprisingly, the need for security has emerged as the most important element in this transformation, rendering most traditional access and authentication controls woefully inadequate.

Redefining the security perimeter

Until recently, identity and access management typically focused on securing people and infrastructure to a traditional IT network perimeter. People were identified by user IDs

and password and infrastructure devices by an IP address. But thanks to the introduction of newer technologies, including cloud, mobile and social, all that is changing. (See Figure 2.) Organizations now need to look at how they're accessing and using technology in light of the interactions among people, data, applications and infrastructure that need to be secured. Today's sophisticated attackers don't think about going after specific security domains or silos. And it's why you shouldn't limit your thinking along those lines either.

Enhancing identity assurance in a multi-perimeter world

Many organizations still rely on simple passwords as proof of identity. But passwords are static and inherently weak. Most users take the path of least resistance, using easy-to-remember, weak passwords that can easily be stolen, cracked and compromised, exposing a system to fraudulent attacks. Once an attacker deciphers a static password, it becomes easy to impersonate the original user and gain access to all sorts of confidential data. And if that's not concerning enough, it's important to note that static passwords are also vulnerable to a wide variety of phishing and Trojan attacks.

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 calculate risk, organizations can grant access based on a dynamic risk assessment of both the transaction and the user in question. 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. For example, if a North American worker suddenly uses her 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, depending on the risk score, the user may be denied access to certain IT resources because the security risk is deemed to be too high.

By requiring more than one form of authentication, organizations can help ensure that both the right user is granted access to protected resources, and that those resources are in fact protected from those who shouldn't be able to access them. With multi-factor authentication, the user provides two or more of the following three means of identification (factors) for authentication:

- A knowledge factor—something the user knows; for example, a static password or PIN
- A possession factor—generated by something that the user has; for example, a mobile device, or a hardware or software token
- An inherence factor—something the user is; for example, a biometric finger print or facial recognition.

The combination of context-based access control and multi-factor authentication ensures that access to corporate resources is granted only when a known and recognized device (the second factor) is being used in an acceptable, known context, such as during a specific time of day and from a specific location.

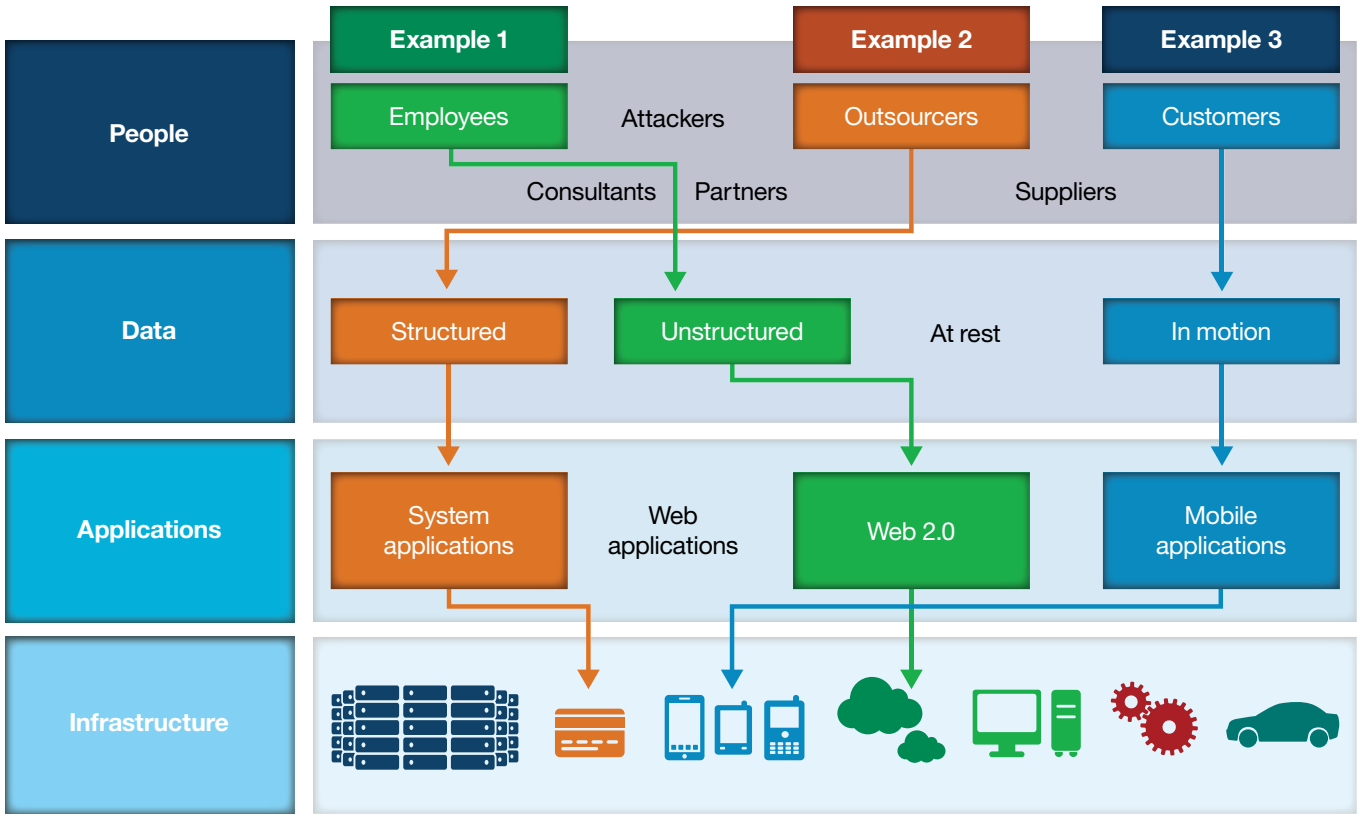


Figure 2. Today's security perimeter has come to resemble a four-dimensional puzzle of complex requirements spread across multiple security domains—including people, data, applications and infrastructure.

Step 2: Integrate identity intelligence into the process

Identity management helps organizations reduce the complexity, cost and risks associated with controlling and managing user access to sensitive applications and data. It eliminates most of the manual, labor-intensive processes often employed to provision users and helps ensure that user lifecycle management is governed according to security policy.

But despite existing investments in identity management tools and techniques, many companies are now finding themselves inadequately protected. Advances in computing—including the explosive growth of structured and unstructured data, ubiquitous information access and the growth of Internet-based collaboration and cloud computing—are seriously hampering both visibility into and control of individuals' entitlements and access privileges. The problem extends even to those organizations with a specific focus on cyber security, including financial institutions and government agencies.

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

Integration with privileged identity management

A privileged ID refers to any account that includes special or extra permissions for enterprise resources, such as servers, network appliances, database systems and enterprise resource planning applications. Of course the threat of attackers compromising a privileged ID poses an obvious risk. But the risks don't end there. An organization's authorized users with privileged accounts can also represent danger to the security of its IT infrastructure. At the same time, organizations are increasingly delegating specific administrative tasks to staff and contractors, opening the door to further risks associated with privileged accounts.

An organization's authorized users with privileged accounts can also represent danger to the security of its IT infrastructure.

Studies of security breaches by various authorities consistently reveal that insider threats are an equal or even greater issue than external attackers. Insider negligence, rather than malicious behavior, is often the cause. That includes such careless actions as sharing passwords, using weak passwords or even writing passwords on Post-it notes. Then there are situations where malicious intent clearly is involved. Social engineers, disgruntled employees, suppliers, and competitors can be adept at maneuvering around strong controls to exploit points of weakness. That's why it's so important for organizations to:

- Prioritize the need for privileged identities
- Identify and monitor their highest risk users
- Know who has access to sensitive data and systems
- Develop baselines for normal behavior.

The most practical way to meet those requirements is with a sophisticated identity management system for allowing IT staff to share privileged IDs. It's critical that such a system includes the following:

- A credential vault to securely store the credentials to privileged IDs
- A check-out check-in mechanism that lets a privileged user check out an ID (with a password) for exclusive use and a limited time period, whenever necessary; and then check in the ID when finished, at which point the password changes automatically
- A means for centrally provisioning and managing IDs on various resources
- Roles and policies for dictating which users have access to which IDs
- A process for users to request access to IDs and for managers to approve the requests
- Integrated audit logs that feed into a security intelligence solution to record all check-out check-in activities and show which users had access to which IDs over a specific time period.

It's a solution that allows organizations to:

- Avoid the proliferation of privileged IDs linked to its resources
- Allow privileged users to access a privileged ID if, when and on the condition they need it—for only as long as they need it
- Make privileged users accountable for the IDs that they've owned or checked out
- Delegate management of IDs and access policies to the respective resource owners
- Collect identity attributes and use that data in conjunction with log events and network flow data rules to provide "identity context aware' security intelligence.

Integration with identity intelligence

Several security intelligence solutions—including security information and event management systems—can provide usable log files and metrics that help identify anomalies, highlight risky or inappropriate behavior and assist in compliance reporting. By integrating identity and 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—organizations can quickly uncover inappropriate or suspicious user behavior (including insider threats) and significantly decrease threat response times.

Step 3: Address compliance mandates with identity and access governance

Virtually every industry faces compliance mandates at some level. Countless government regulations around the world stress the importance of visibility and control for individuals' entitlements and access privileges.

Thanks to escalating security and privacy concerns—along with a renewed focus on corporate oversight and governance—risk management and compliance measures are now being driven to the business forefront. As a result, organizations must prove that they have strong and consistent access controls to meet both their own compliance requirements and those of their business partners.

It's far more likely that security breaches and compliance issues will occur when users have outdated or inappropriate levels of access, driving up the potential for insider threat activity. And outside attackers often look for the "easy prey" that poorly controlled and managed user access programs offer. It's simply not enough to develop a solid identity and access management program. You also need to keep it functioning properly.

Reducing risks through governance

Identity and access governance provides guidelines on how user roles are defined and access is provisioned, managed and enforced throughout the lifecycles of users (see Figure 3). Solutions designed for managing user access requirements with greater accountability and transparency can help you govern and enforce user access more effectively. These 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 which resources.

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

- Planning for an identity and access governance strategy
- Defining standards, 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.

Case study: A global leader in customer management streamlines and improves its identity and access management program

Recent merger and acquisition activity—compounded by disruptions from organizational changes—highlighted this company's need for a more robust, agile and consistently implemented identity and access management solution.

IBM assessed their business priorities, identified their identity and access management-related strengths and weaknesses and evaluated them against industry standards and best practices to develop a clear business-driven strategic roadmap for improving the company's identity and access management capabilities.

With the help of IBM Identity and Access Management Services, the organization consolidated its administrative identity and access management silos into a common framework designed to reduce costs and complexity through the use of common, reusable standards-based components, technologies and services. And as a result, the company was better positioned to avoid and mitigate compliance risks.

Step 4: Take action now

While there are plenty of organizations today with longstanding strategies designed to help them protect their systems, applications and data from unauthorized access, the need for a truly comprehensive identity and access management strategy often continues to go unmet. But now that identity has clearly emerged as a new security perimeter—requiring controls to manage, enforce and monitor user entitlements and access activities—it's time to take action.

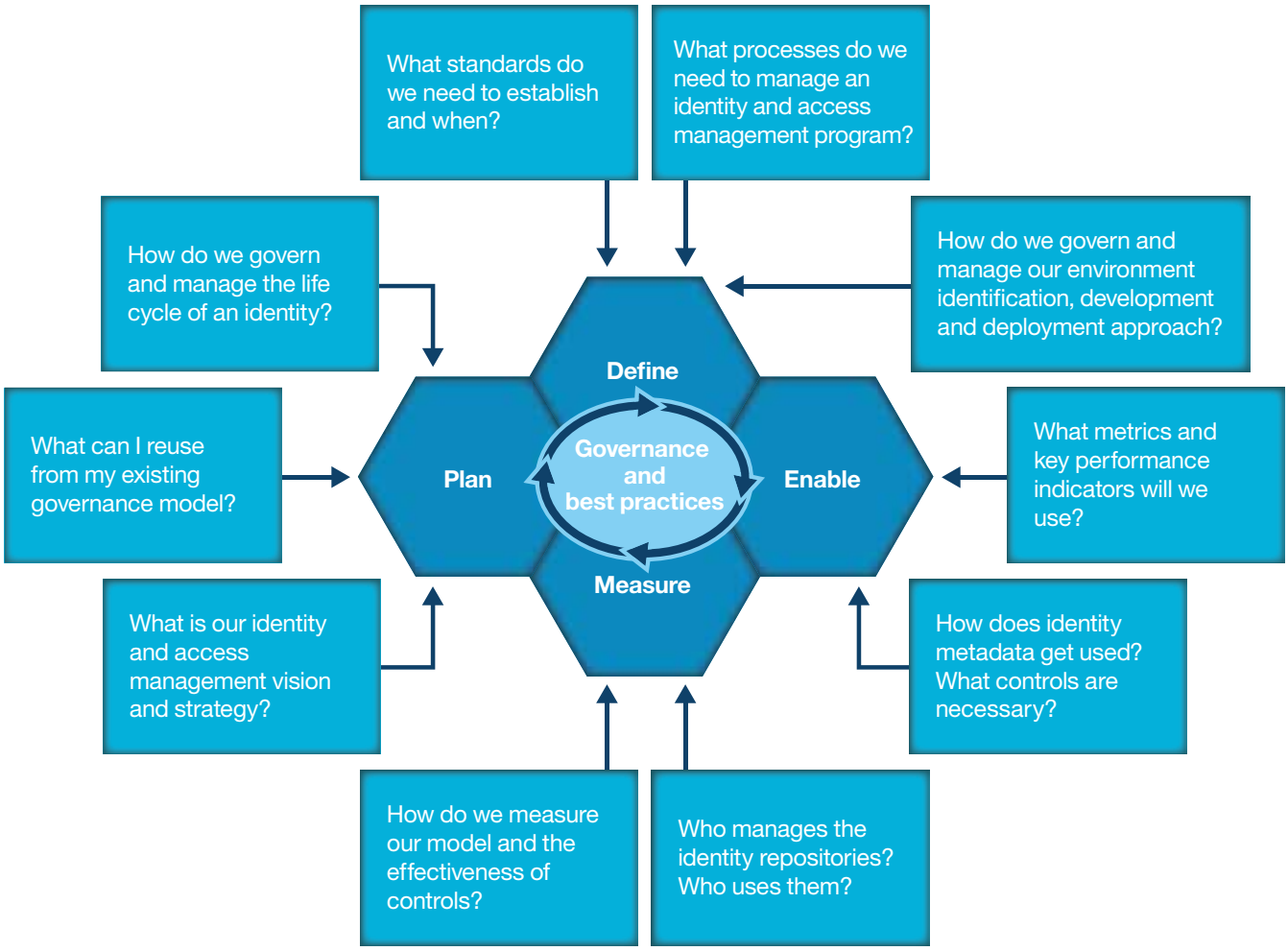


Figure 3. There are 10 key questions you need to ask as you develop an identity and access management program.

Companies today are embracing new business models that rely increasingly on cloud computing, mobile technology and social interactions for their success. And despite efforts to rein them in, insider threats continue to proliferate across the enterprise. The lack of an effective identity and access management strategy—and the expertise necessary to integrate the appropriate technologies into your environment—can result in risky implementations and expensive mistakes. That's why many organizations look to experienced service providers for assistance.

IBM Identity and Access Management Services can help you, with a comprehensive approach that leverages the services and technology that have gained IBM recognition as a leader in developing and delivering security solutions. Our identity and access management services focus on the key security challenges facing enterprise IT and line of business managers today, helping them to:

- Safeguard mobile, cloud and social interactions
- Prevent insider threat and identity fraud
- Simplify identity silos and cloud integrations
- Deliver intelligent identity and access assurance.

We offer professional and managed services that include:

- ***Identity and Access Management Assessment and Strategy Services***—Business and technology consulting to help clients develop a clear, business-driven, strategic roadmap for improving an organization's identity and access management maturity posture
- ***Identity and Access Management Design and Implementation Services***—Proven best-practice framework and methodology for designing and implementing solutions that help maintain security control over mobile devices, mitigate internal and external threats, reduce security risks in cloud environments and automate compliance
- ***Identity and Access Management Managed Services***—On-premises, hosted or cloud-based delivery models offering a full array of capabilities, including user provisioning, lifecycle governance, single sign-on, enterprise user registry services, federation and multi-factor authentication.

IBM has long been recognized as a security solutions thought leader—and is one of the few service providers offering these kinds of end-to-end identity and access management solutions, from strategy development, to design, building and management. Our security specialists work with you to address your specific needs and provide the solutions that fit with your business goals.

For more information

To learn more about how IBM Security Services can help you reduce costs and increase your protection against sophisticated threats, please contact your IBM representative or IBM Business Partner, and visit the following website:
ibm.com/services/security

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

Produced in the United States of America
January 2014

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 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.


Please Recycle

[1] IBM and Ponemon Survey of 265 C-Level Executives, Feb 2012, "The Source of Greatest Risk to Sensitive Data."
[2,3] IBM X-Force 2012 Trend and Risk Report.

SEW03038-USEN-00