SailPoint

SOLUTION BRIEF

6 Tips for Building Your Cloud-based Identity Governance Strategy

When starting any new project, especially one as critical to your organization's security as an identity governance project, there are certain aspects you must think about. Have you thought about what the entire organization needs for identity governance versus a single department? What about the types of pain points the business is experiencing with compliance, productivity and visibility?

As your business evaluates moving critical business technologies such as identity into the cloud, there are some factors to consider on how to evaluate and select the best governance solution for your organization.

Since identity needs to be at the center of your IT operations and security strategy, you must think about how it will affect the organization as a whole.

Tip #1: Think Holistically About Your Identity Needs

Whether you are implementing identity governance for the first time or transitioning from an on-premises solution, you should consider all your business requirements and how they should be addressed. Common business drivers for identity include:

- Protecting the organization from internal and external security threats
- Meeting regulatory compliance requirements
- Enabling the business with convenient access services
- Lowering operational costs

It may be tempting to start your identity governance program with a tactical solution like single sign-on (SSO) to provide convenient services to business users; it does offer the potential for great efficiency gains. While tools like SSO address a major pain point with users, it does not address the governance needs your organization has related to security and compliance requirements. Rather than focus on what hurts the most right now, take a step back and consider holistically what you want your ideal system to look like and how it would function. There are a range of identity services you need to consider, including:

- **User Provisioning:** to automate processes for granting, changing, and removing access securely and cost-effectively throughout a user's lifecycle within your organization.
- **Password Management:** to help enforce the consistent use of strong password policies while reducing IT and help desk costs.
- **Access Certifications:** to ensure that access is appropriate for a user's job role, conforms to corporate policy, and meets audit and compliance requirements.
- **Access Request:** to delegate application access requests and permissions to individual departments and users.

In order to meet your security, compliance and business enablement goals, you should have an explicit plan for how you will deliver all the critical identity governance services your organization needs. You should look for solutions that provide most, if not all, of the services you need. And if you plan to implement multiple products to meet your goals, then you will need to find complementary products so you don't assume the burden of integration. Taking an all-encompassing approach will ensure you don't face any underlying issues later on down the road.

A prioritized approach to deploying individual solutions in an identity program can be a lifesaver in terms of budget and time, but without a solid foundation of governance these solutions can become more of a burden.

Tip #2: Build a Governance Foundation

Experience shows that it's best to start your identity project with the right foundation – one that will make later phases of your implementation run more smoothly. For these reasons, you should strongly consider beginning with identity governance.

Starting your project with identity governance will allow you to build a baseline of the current state of user access within the organization, aggregating and correlating identity data across cloud and on-premises resources. This centralized visibility will enable your organization to inventory, analyze and understand the access privileges granted to users – in short to know "who has access to what?"

Identity governance will help you to establish a centralized governance model that describes who should have access to what and what that means (e.g., what data can be accessed, which files can be shared), defines clear ownership and approval processes for provisioning, and define access and password policies. Once your organization has a governance model in place, you can determine on an ongoing basis if user access privileges are appropriate or if they violate security or compliance policy.

By embedding identity governance policy and controls throughout all identity processes, your organization can achieve ongoing, sustainable compliance and reduce the need for after-the-fact remediation and expensive manual processes. Beginning your project with well-governed identities will underpin and strengthen all your solution components as you deploy them.

Even if your organization has already begun investing in an identity program, it's not too late to establish your governance foundation. In fact, it's probably more even more important. For example, if your organization has begun standardizing access management as part of a platform-as-a-service (PaaS) offering, it doesn't eliminate the need for identity governance. Rather, it increases the need to move quickly to establish "who should have access" based on business need and organizational policy. By tying an existing access management deployment to a strong governance model, you can ensure the right users have the right access at the right time.

Just as you must think about how identity will affect the entire organization, you must also procure a solution that will connect to your entire organization's resources.

Tip #3: Say No to Management Silos

While you may be struggling with your organization's rapid adoption of cloud and SaaS apps, you should not lose sight of the need to govern and control access across your entire organization. By leveraging a unified system to manage access to both on-premises and cloud-based resources, you can stay in control of identity no matter where an application is deployed.

The fact is, to effectively reduce risk and to make your workplace secure, you need the big picture. Who has access to what and does that access conform to policy? You can't govern without centralized visibility. And you need consistent enforcement of access policies across all your IT resources and identity processes such as provisioning and password management.

For these reasons, you should look for a cloud-based identity governance vendor with rich connectivity to both cloud and data center resources, and avoid cloud-only vendors that require expensive and time-consuming customization to connect to and manage on-premises resources. You should also ensure that all communications between your identity governance solution and any on-premises resources is handled reliably, securely and conforms to the highest enterprise IT security standards.

In order to secure your organization and ensure compliance with regulatory mandates, you need cloud-based identity solution that can:

- See everything – you need visibility to information about all identities, across all resources – no matter where they are located, what devices they may use, or whether the application is on-premises or in the cloud.
- Govern everything – continuously monitor user access and apply preventive and detective controls to enforce policy and ensure compliance.
- Empower everyone – automated and self-service options that ensure users have the right access at all times.

The world never stands still and technologies are always changing; your identity governance solution should be flexible enough to adjust to the needs of your business now and in the future.

Tip #4: Buy Open, Extensible Solutions

Because identity governance is a critical foundation for managing identity, it's important to select a solution that facilitates interoperability with complementary tools and technologies. An open architecture allows identity governance solutions to work in a complementary fashion with other security, infrastructure and operational components, to make policy-based decisions about how access is granted and changed, to fulfill access and password changes on target resources, and to provide enterprise-wide visibility to user access.

Identity governance can augment complementary identity management services, such as access management solutions, with critical functions such as:

- Role-based policies to control how access is granted and maintained
- Auto-provisioning of tiles on application launchpads
- Fine-grained provisioning on target resources
- Self-service access request for new applications
- Password reset, synchronization, and policy enforcement

One step further than a solution with integrations is a true open identity platform. With official plugins, open APIs and the ability for the community at-large to collaborate and share their own extensions with each other, an open identity platform can significantly lower costs, deployment times and minimize your project risk with identity. You should look for identity governance providers that provide rich integration options and tools, and foster a partner ecosystem with proven integrations and extensibility.

Identity governance is complex, no matter how it is deployed. Cloud-based identity governance utilizes years of best practices to make identity accessible for every enterprise.

Tip #5: Configure, Don't Customize

If there is one consistent lesson learned by organizations over the past 20 years of identity history, it's that customization is costly. While customization may allow you to mold software to your unique business requirements, it can significantly delay your deployment, increase implementation costs exponentially and be very difficult to upgrade or adjust as your requirements change.

Avoiding customization is one of the key principles of next-generation SaaS solutions. For this reason, true cloud-based identity governance solutions are designed to minimize customization by being highly configurable. This means you have many choices on how to deploy and run your software, but you don't spend months writing custom policies and workflow, redesigning user interfaces or hard-coding rules.

Make sure that the cloud-based identity governance solution you select can be used out-of-the-box and provides a catalog of configuration choices that are designed to meet the needs of many organizations. By providing a set of default best practices that are ready to go on day one, the right solution will give your organization immediate value and avoid time-consuming customizations that can slow down projects. When you choose a solution with most capabilities ready to go "out of the box," you can shorten deployment times and speed time-to-value.

When choosing a vendor, take a peek behind the scenes and make sure what you're getting is a true cloud-based identity governance solution.

Tip #6: Ensure Your Solution Will Truly Lower TCO

One of the primary reasons that organizations choose to go for a cloud-based solution is the lower total cost of ownership (TCO). With SaaS solutions, you pay a monthly or annual subscription fee for as long as you use the solution, allowing you to significantly lower your initial acquisition and project deployment costs.

Because all infrastructure costs, maintenance and upgrades are handled by the SaaS provider, your organization can completely eliminate the cost of platform software and hardware, network infrastructure, third-party monitoring tools, test tools and security products. You will also save both time and money by eliminating the need to hire skilled personnel to operate, monitor and maintain the application since all those costs are transferred to the software vendor and amortized across all the customers on the platform.

Another area of savings is software updates. With a true cloud-based solution, the provider regularly updates the software, which means you will always be running the latest version of the software without any downtime. Your organization will no longer be responsible for software upgrade projects, which can be expensive and time-consuming.

As important as cost management is to your organization, you will need to compare your options carefully when it comes to TCO. Unfortunately, not all "cloud" identity governance products are created equal, and to get the benefits for which you are looking, you need to choose a native SaaS solution built on a multitenant architecture.

Instead of your software instance living on an individual server that could fail – this is one of the larger drawbacks of a hosted on-premises solution – multitenancy shares the load of all customers across all resources to ensure a near 100% uptime. It also ensures that every customer is on the same version of the software, and is what allows your vendor to pass cost savings on to you.

Because a multitenant identity governance provider's resources are focused on maintaining a single, current version of the application, rather than supporting multiple software versions for individual customers, the annual total cost of ownership is much lower. Vendors that claim to offer a cloud-based solution, but actually offer single-tenant hosting (where each customer's software is a separate implementation), do not offer the same cost savings potential. Because these vendors must support,

maintain and upgrade different versions of the software with unique customizations made by each customer, they incur very high deployment and operational costs, and those costs are inevitably passed on to you, the customer.

Identity at the Speed of Cloud™

Today's enterprises are cloud enterprises. They're adopting the cloud at an ever-increasing rate, and Gartner estimates even that 90% of enterprises will have a hybrid environment in the next few years. The cloud is changing how we work – employees can now work wherever they want, and on whatever device they want to work – but it's also presenting new challenges. These users – identities – are who access the sensitive information in an organization, and it's them around which we must center our security.

Identity is what powers the cloud and it is what enables organizations to securely adopt new technologies while still being able to have full visibility and control over who has access to what sensitive information. When identity governance is delivered from the cloud itself, it grants the crucial security, compliance and automation that organizations need while also offering all the benefits of a cloud-based solution.

But it's also more than just security. Once enterprises know that through their efforts, the business is safer, more efficient and better protected. They are free to do what they set out to do in the first place: improve the organization. Whether that means gaining a competitive advantage, chasing new opportunities for growth, or providing a better experience for its customers, the empowerment organizations gain with identity governance is what allows them to be confident, fearless and unstoppable.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.

SB1121-1710