SailPoint

SOLUTION BRIEF

The 6 Elements of a **Cloud-based Identity Governance Deployment**

If your organization is considering deploying cloud-based identity governance, it pays to do your homework. While in many ways simpler than traditional on-premises identity governance deployments, cloud-based identity governance projects still require careful planning and preparation. There are important differences from traditional deployment models that can catch your organization by surprise – and there are aspects of the deployment that are no different from an on-premises deployment. Either way, it pays to know what to expect.

Here are the six elements of a cloud-based identity governance implementation to help you prepare your deployment.

What's Different about Cloud-based Identity Governance?

There are three main areas that organizations find cloud-based identity governance deployments to be distinct from traditional on-premises deployments.

Configuration, Not Customization

In order to capture the full advantages of cloud-based identity governance, your organization will need to embrace standard, out-of-the-box business processes, instead of customizing the software to fit your existing processes.

It may take strong leadership to steer business groups away from doing things the way they always have done, but there are numerous benefits to that tradeoff.

Using default settings, pre-built configuration options and out-of-the box templates, cloud-based identity governance solutions deliver choice and flexibility, while significantly reducing the time spent setting up and deploying the solution.

By providing a selection of configuration options that do not require custom coding, cloud-based identity governance solutions can be up and running in a few short months, allowing users to manage changes to their access privileges, reset passwords and perform access certifications.

To help your organization avoid the customization trap, remind key stakeholders of the lessons learned in the past from over-customizing identity solutions. Customization is expensive and time-consuming. It can significantly delay deployments and increase complexity. It can also result in your organization running a "one-off" version of the software that is difficult to upgrade. By embracing the cloud, your organization can pave to the way to fast time to value, greater ease of use and effortless upgrades in the future.

The Project Pace

Many organizations are attracted to cloud-based identity governance solutions because of the shorter deployment time and faster time to value. However, the faster pace of a cloud deployment has the potential to catch your organization by surprise.

A compressed project deployment brings its own challenges and requirements.

Business and technical users who are accustomed to the lengthy deployment cycles of on-premises software may think they have more breathing room than they do. With cloud-based identity governance, stakeholders will find that they need to get involved in the project right away. Application and data owners need to be consulted almost immediately and end users may be required to begin acceptance testing within a few weeks.

You can ensure that the deployment stays on pace by establishing a communication and onboarding plan for end users before you begin deployment. Remember that it is people who will drive the success or failure of your project, so you need to ensure that technical resources are committed and prepared and that end users are trained and understand what is coming. It is also important to have a strong project manager who can troubleshoot any issues that arise, so that you don't delay the progress of the deployment and risk losing stakeholder support. Finally, in order to benefit from the full visibility and control provided by identity governance, it's critical that the cloud-based solution connects to and manages both on-premises systems and cloud environments.

"Continuous" Updates
One of the biggest differences between cloud-based identity governance and conventional on-premises solutions is how software updates are handled. For many on-premises applications, software upgrades can be a disruptive and time-consuming job that most organizations tackle once or twice per year, delaying the availability of the latest functionality.

With cloud-based identity governance, your cloud solution provider handles all upgrades, with no need to take the application offline. Your organization seamlessly receives updates and new features as soon as they are ready. However, because these upgrades happen more frequently and incrementally, they typically result in reduced user acceptance testing and training costs.

Another key difference is that your organization and all of the solution provider's customers run the same version of the software and receive updates concurrently.

Cloud-based identity governance means your organization is always up-to-date and can take advantage of new functionality within the application more quickly.

When your users participate in user groups and other forums, they can share experience and tips about the exact same version of the software.

Despite its many advantages, the "continuous" update process may require more preparation, so that you are tracking the rollout of releases – minor ones that happen more frequently and major ones that happen less often. As part of providing feedback to your identity governance solution provider, you'll want to monitor updates and adjust your requirements and feature requests to keep pace with what has been delivered and what is scheduled to be delivered.

What Hasn't Changed with Cloud-Based Identity Governance?

Not everything about a cloud-based identity governance deployment is new and different. Here are three aspects of identity deployments still hold true, even for cloud-based solutions.

Resource Connectivity
One of the primary benefits of cloud-based identity governance is the ability to centrally manage and control all identities across all systems – on-premises and in the cloud. In order to make this enterprise-wide view possible, you will need secure connectivity to your cloud applications and to systems in your data center.

You should look for identity governance vendors with rich integration capabilities, and avoid vendors that require expensive custom integrations. By using pre-built connectors and packaged integrations, you can reduce the time required to connect, but be aware some project management and technical oversight is generally needed to gain the permission and/or assistance of data owners to access certain resources and to ensure that all systems are properly integrated.

With a cloud-based identity governance solution, it's also important to ensure that your integration approach meets your organization's security requirements. Most companies have regulatory and security obligations when transmitting data outside their network. A remotely managed virtual appliance for integrating to on-premises systems is a good approach to ensure that your integration meets security and scalability requirements.

Data Aggregation and Correlation

The foundation of identity governance is the ability to see and manage user access privileges across the organization. This centralized visibility and control requires creating a single repository for identity and access information by aggregating data from your authoritative source(s) and target resources.

Once you have aggregated your identity data from various sources across the organization, you can move on to step two – the correlation process – which will help you resolve the inconsistencies between the various sources of identity data and create a 360˚ view of "who has access to what." Your organization's data owners and technical staff will need to invest time to work with your service provider to map and correlate data across the organization so every account held by a unique individual is identified and mapped to that person. They will also need to troubleshoot any issues that arise based on missing, incomplete, or inaccurate data.

Bear in mind that without consistent and accurate data, no identity governance application can work effectively.

Missing or erroneous data undermines that ability of the solution to help your organization detect policy violations and inappropriate access, and it can potentially disrupt identity business processes, discouraging user adoption. Starting your project with clean and accurate data provides the foundation for effectively governing identities and securing the enterprise.

The Right Staffing

Assembling the right deployment team is a critical success factor for any identity governance project, whether cloud-based or traditional on-premises deployment. The right implementation team understands the technical and business requirements of the project and has the appropriate skills and experience to get the job done.

While cloud-based solutions don't need the same system administration and operations staff as on-premises applications, they do require some upfront architecture and integration work, especially in the area of connectivity and data integration. And staffing the team with the right business and executive stakeholders can make or break a project.

Here are sample profiles of key personnel needed to ensure the success of your cloud-based identity governance project:

- **Business Lead:** understands business processes, has executive direction, and can make critical decisions and tradeoffs.
- **Technical Lead:** has technical security or identity knowledge, as well as skills in the areas of infrastructure design and requirements/gap analysis.
- **Project Manager:** owns day-to-day management of the project, requests and assigns resources, resolves issues, and manages vendor communications.
- **Source/Application Administrator:** provides subject matter expertise for connectivity to target systems on an as-needed basis.

Last but not least, don't forget your end users. It's vital to communicate and involve them early in the deployment as user acceptance testers, to ensure that the project meets business requirements.

By keeping these six elements in mind when preparing for your cloud-based identity governance implementation, your deployment will be a smoother process and your organization can greater utilize all the benefits and features of a cloud-based solution.

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 a wide range of industries, including: 6 of the top 15 banks, 4 of the top 6 healthcare insurance and managed care providers, 8 of the top 15 property and casualty insurance providers, 5 of the top 15 pharmaceutical companies, and six of the largest 15 federal agencies.

SB1129-1710