ForgeRock®

Identity Cloud Checklist

Top 10 Considerations and Best Practices for Your Identity Cloud Strategy

Digital transformation, competitive advantage, and saving money are driving factors for any organization moving to the cloud. Unfortunately, even organizations already in the cloud can't keep up with the pace of new business demands, like modern capabilities, better experiences for users, or addressing audit and regulatory pressures. As a result, organizations need to not only modernize legacy identity and access management (IAM) infrastructure for the cloud, but also support existing and new cloud initiatives while ensuring enough resources are still focused on cloud modernization.

A comprehensive cloud IAM platform can greatly help organizations simplify access, save money, and grow revenue. According to Forrester Research, organizations can reduce their IT operations and development costs by up to 80% by using cloud IAM solutions. Labor costs are also 80% to 90% lower for initial and ongoing maintenance and development of a cloud IAM solution.

As your organization grows, your IAM platform should grow with it. To plan for your organization's future in the cloud, you need a comprehensive, enterprise-grade identity platform that supports your priorities with a combination of usability, customizability, and operational cost savings. You also need a range of configuration options so that you can choose the functionality you need. This checklist highlights the top 10 considerations and best practices for your identity cloud strategy.

1 Forrester Research, "Making The Business Case For Identity And Access Management," 2019

Identity in the Cloud Strategy Checklist: 10 Considerations and Best Practices

CONSIDERATION 1:

Use Cases for Any Identity

- ☑ Define which use cases will be supported at rollout. Is the focus on simple single sign-on (SSO) and adaptive and multi-factor authentication (MFA) or on more comprehensive identity and access management (IAM) capabilities like user and identity lifecycle management or provisioning?

- ☑ Determine how the cloud identity platform will integrate with your current investments. For example, will the implementation be completely independent and new, or will it be an augmentation of existing IAM tools?

- ☑ Understand that the cloud IAM platform should be capable of managing multiple types of identities within a single implementation, including customers, partners, workforce, citizens, gig economy workers, and “non-person” identities, such as devices, bots, APIs, and microservices.

- ☑ Have a roadmap for future growth and use cases based on your organizational needs. The platform should have a flexible data model that is object based and provides the ability to define many different schema and attributes and the relationships between each.

CONSIDERATION 2:

Migration

- ☑ Review current deployment and all customizations. The platform should provide options to migrate identities in bulk as a one-time exercise (including password hashes from on-premises directories), continues sync with multiple authoritative systems, and just-in-time (JIT) migration (including the ability to capture user credentials during authentication).

- ☑ Devise a migration plan and strategy, such as replacement versus coexistence. Be on the lookout for ways to add value during all the phases of implementation and rollout.

- ☑ Execute migration plans, including deploying in the cloud, syncing users, migrating apps, and decommissioning legacy apps.

- ☑ The platform should be capable of migrating apps group by group or individually, so you can plan and execute cloud migration at your own pace.

- ☑ The cloud platform should provide DevOps-friendly ways to integrate your agile continuous integration/ continuous delivery (CI/CD) methodologies to seamlessly move changes from lower environments to production.

CONSIDERATION 3:

Coexistence

- ☑ The cloud platform should support multiple protocols like SAML, OAuth 2.0, and WebAuthN to enable integrations with legacy and modern applications quickly.

- ☑ The cloud platform should coexist with other legacy IAM solutions by supporting federation or native integrations where possible, and augment legacy or home-grown applications to give you the time you need to execute on your cloud migration and security strategy.

- ☑ The cloud platform should support bidirectional identity sync between legacy solutions and the cloud in order to maintain a consistent user identity store.

- ☑ The cloud platform should have the ability to secure applications running on premises or in public or private clouds with web agents, a gateway-based architecture or leverage modern protocols and integrations for the new generation of SaaS applications.

CONSIDERATION 4:

Deployment Flexibility

- ☑ The platform should have capabilities that can be deployed to secure applications on premises, in the cloud with a public cloud provider of your choice or through a hybrid or multi-cloud approach.

- ☑ Deployment architecture options should be a combination of private and public clouds, infrastructure as a service (IaaS), and platform as a service (PaaS).

- ☑ The IAM architecture should have feature parity across cloud and on premises so that your team doesn't have to make a tough choice between capability and deployment options.

CONSIDERATION 5:

User Experience

- ☑ Plan for the platform to secure and orchestrate seamless omnichannel user journeys for your users, regardless of what device they are on for easy access.

- ☑ Evaluate to make sure that the platform can support multiple access and self-service scenarios based on your users' preferences using an easy to use drag-and-drop user interface (UI) for configuration.

- ☑ Ensure the platform is easy to configure for administrators who are new to the platform with smart defaults and a simple wizard UI, yet flexible enough for advanced use cases when needed.

CONSIDERATION 6:

Capabilities

- ☑ Look for a platform that enables you to consume the service without sacrificing rich features and extensibility. This way, you can reap the benefits of the cloud while maintaining the depth and breadth of a full-featured IAM platform.

- ☑ The platform should be designed to solve a majority of customer use cases with a single offering. This includes identity management, access management, and directory services capabilities.

- ☑ The cloud platform should include a gateway to integrate legacy applications, APIs, and microservices to bridge legacy applications and modern services.

- ☑ The platform should enable you to easily design user journeys, from registration and authentication, to how users prefer to access services (MFA, passwordless, one-time password, magic link, and others), to self-service flows, such as password resets, forgotten usernames, and preferences.

- ☑ Developers should be able to integrate user access journeys with any home-grown, legacy, or custom access management, fraud, or risk solution to meet the needs of the business.

- ☑ The platform should be able to manage all identities, password policies, groups, and roles.

- ☑ The platform should support bidirectional identity provisioning between on-premises and cloud or bulk import of users..

- ☑ The platform should support identity reconciliation with standards-based connectors to ensure that user identity data, including passwords, are always accurate across all managed applications.

- ☑ The platform should provide the ability to sync password changes from Active Directory or other standard LDAP directory servers to the cloud in order to ensure users always have a seamless experience.

- ☑ The platform should support software development kits (SDKs) that can be embedded into your applications to provide seamless user experiences and also provide dedicated apps for capabilities like MFA and one-time password (OTP).

- ☑ Advanced use cases should also be supported, such as contextual and fine-grained authorization, continuous risk monitoring, social identity registration and login, personalization, delegation, user dashboards, privacy, and consent features.

CONSIDERATION 7:

Security, Privacy, and Compliance

- Ensure your data is never commingled with other customer data. This not only prevents accidental data spillage, but also “noisy” and “nosey” neighbors impacting your performance or accidentally or maliciously accessing your data.

- All data should be encrypted at rest and in transmission to prevent unauthorized access and data breaches.

- The platform should enable you to manage data residency requirements by allowing you to place data in the region of your choice.

- Ensure compliance certifications are in place, such as ISO 27001 and SOC 2.

- Ensure the platform addresses international and national privacy regulations, such as The General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

- Have a detailed and well-documented incident response (IR) plan to detect, contain, eradicate, and recover from any potential incidents.

- Conduct automated vulnerability scanning of internet-facing systems on a regular schedule, along with manual penetration testing, both by internal security engineers as well as external experts.

- Have a dedicated secrets management system for each customer that is used to securely store passwords, private keys, API keys, and other secrets. The secrets should be strongly protected at rest and in transit, and the cryptographic keys used to encrypt the secrets should be regularly rotated.

- Use industry best practices to continuously monitor vendor-managed cloud identity platforms.

- Ensure that network communications within a customer environment are strictly controlled by using role-based access control (RBAC) and enforced via network policies.

- The platform should have protections against common threats like network flooding or denial of service attacks including Layer 3 and Layer 4 attacks.

- All cloud endpoints should require TLS 1.2 or higher and should be anchored by a digital certificate.

- The platform should have full tenant isolation so that if an attacker compromises a customer’s credentials, it does not impact others. If an entire customer environment is compromised in a worst case scenario, none of the identities would be valid in other customer environments or the service control plane.

CONSIDERATION 8:

Availability and Predictability

- The cloud platform should have multi-region availability to ensure that you get data isolation and to satisfy data residency laws for regional regulatory requirements.

- The platform should have the ability to provide zero downtime upgrades so that a patch or upgrade does not impact service level agreements (SLA).

- The platform should have the ability to restore your specific environment from an encrypted backup, within an acceptable SLA, in case of a mishap or misconfiguration.

- The cloud platform should provide seamless scaling to meet your needs in case of sudden or seasonal traffic growth.

- The cloud platform should not impact any business by throttling or stopping any legitimate business transactions because of sudden surges in activity beyond the subscription level.

CONSIDERATION 9:

Vendor Support

- ☑ The vendor should have a dedicated customer success team for onboarding the service, with an end-to-end deployment strategy for your success.
- ☑ The vendor should have 24/7 support with a global presence with well established response times for critical issues.
- ☑ The vendor should support agile software development methodologies and DevOps tools. This way, developers don't have to spend long cycles building their own tooling to move configurations between environments.
- ☑ The vendor should have extensive IAM maturity to assist you in your roadmap and future plans.

CONSIDERATION 10:

Cost

- ☑ Look for an IAM platform that offers one subscription, giving you complete flexibility to consume it as a service, and also allows you to deploy it anywhere – whether in your data center, private or public cloud, or in a hybrid configuration.
- ☑ Pricing should be predictable. That includes unlimited annual usage per user with surplus user coverage that protects you as your business grows or as you experience spikes in demand.
- ☑ Look for an IAM platform that offers pricing that covers most use cases rather than charging you for every feature.
- ☑ Development, testing, and production environments should be included in one subscription, at one cost.

Meet All Requirements With ForgeRock Identity Cloud

ForgeRock Identity Cloud is the industry's most comprehensive, fully customizable, and extensible identity platform as a service. With ForgeRock Identity Cloud, you can plan for your current and future business needs with a more attractive, predictable cost model and focus more on your business. You will reduce operational risks by relying on a trusted software vendor, simplify your infrastructure footprint, and better align with your cloud strategy.

Get Started On Your IAM Cloud Strategy Today

Cover all your specific IAM requirements in the cloud today and tomorrow. We're here to help. Contact us to learn more about IAM cloud best practices and the ForgeRock Identity Cloud today.

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com** or follow ForgeRock on social media.

Follow Us