ForgeRock

# Identity Cloud Checklist

## Top 10 Considerations and Best Practices for Your Identity Cloud Strategy

The driving factors for any organization moving to the cloud invariably include digital transformation, gaining a competitive advantage, and saving money. Unfortunately, even organizations already in the cloud can't keep up with the pace of new business demands, like passwordless authentication, better experiences for users, or the need to address audit and regulatory pressures. As a result, organizations are facing the 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 remain focused on overall IT modernization.

A comprehensive cloud IAM platform can 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.[1]

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, such as 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 schemas and attributes and the relationships between each.

**CONSIDERATION 2:**

## Migration to Cloud

- 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), continuous 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 vs. 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.
- Require the cloud service to be capable of migrating apps group by group or individually, so you can plan and execute cloud migration at your own pace.
- Look for a cloud service that supports 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 with Legacy

- Support multiple protocols, such as SAML, OAuth 2.0, and WebAuthN to enable integrations with legacy and modern applications quickly.
- Plan for the cloud service to 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.
- Ensure the cloud service can provide bidirectional identity sync between legacy solutions and the cloud in order to maintain a consistent user identity store.
- Secure applications running on-premises or in public or private clouds with web agents or a proxy-based architecture, or leverage modern protocols and integrations for the new generation of SaaS applications.

**CONSIDERATION 4:**

## Hybrid IT

- Determine if the vendor has 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.
- Opt for an architecture with deployment options that include a combination of private and public clouds, infrastructure as a service (IaaS), and platform as a service (PaaS).
- Be sure that the IAM architecture has 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 easy access, regardless of what device users are on.
- Evaluate the platform to be sure it can support multiple access and self-service scenarios based on your users' preferences, and that it enables easy configuration with a drag-and-drop user interface (UI).
- Ensure the platform is easy to configure for administrators who are new to the platform, offering smart defaults and a simple wizard-driven UI, and that it's flexible enough for advanced use cases when needed.

**CONSIDERATION 6:**

## Capabilities

- Plan 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.
- Look for a cloud service that is designed to solve a majority of customer use cases with a single offering. This includes identity management, access management, and directory services capabilities.
- Ensure the cloud service includes edge security to integrate legacy applications, APIs, and microservices to bridge legacy applications and modern services.
- Plan for multiple user journeys.The cloud service should enable you to easily design user journeys, from registration and authentication, to the ways 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.
- Work with developers 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.
- Determine if the cloud service is able to manage all identities, password policies, groups, and roles.
- Make sure the cloud service supports bidirectional identity provisioning between on-premises and cloud or bulk import of users.
- Require the cloud service to support identity reconciliation with standards-based connectors to ensure that user identity data, including passwords, is always accurate across all managed applications.
- Plan for the cloud service to 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.
- Ensure the cloud service supports 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).
- Be sure it also supports advanced use cases, 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

- Work with your cloud service provider to 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.
- Ensure that all data is encrypted at rest and in transmission to prevent unauthorized access and data breaches.

- Ascertain that the cloud service enables 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.
- Address international and national privacy regulations with the cloud service provider, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).
- 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 using role-based access control (RBAC) and enforced via network policies.
- Be sure the cloud service has protections against common threats like network flooding or denial-of-service attacks, including Layer 3 and Layer 4 attacks. Ensure that all cloud endpoints require TLS 1.2 or higher and should be anchored by a digital certificate.
- Require the cloud service to have full tenant isolation so that if an attacker compromises a cloud 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.
- Have a detailed and well-documented incident response (IR) plan to detect, contain, eradicate, and recover from any potential incidents.
- Ensure that the vendor has a crisis management and communication plan that involves collecting, processing and dissemination of information required to address the crisis for impacted customers.

**CONSIDERATION 8:**

## Availability and Predictability

- Cover multi-region availability with the cloud service provider to ensure that you get data isolation and to satisfy data residency laws for regional regulatory requirements.
- Review the cloud service provider's upgrade process. There should be zero-downtime upgrades so that a patch or upgrade does not impact service-level agreements (SLAs).
- Seek out a vendor with an industry-standard 99.99% SLA and a history of exceeding that standard.
- Be sure the cloud service has the ability to restore your specific environment from an encrypted backup, within an acceptable SLA, in case of a mishap or misconfiguration.
- Ensure seamless scaling from your cloud service provider to meet your needs in case of sudden or seasonal traffic growth.
- Make sure the cloud service does 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

- Be sure the vendor has a dedicated customer success team for onboarding the service, with an end-to-end deployment strategy for your success.
- Ensure the vendor offers 24/7 support with a global presence and established response times for critical issues.
- Find a vendor that supports 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.
- Select a vendor with extensive IAM maturity to assist you in your roadmap and future plans..

**CONSIDERATION 10:**

## Cost

- Look for an IAM service 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.
- Seek predictable pricing. It should include 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 service with pricing that covers most use cases rather than charging you for every feature.
- Be sure that development, testing, and production environments are 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 that allows you to focus less on the need to right-size your identity platform 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.