WHITE PAPER

SECUREAUTH




# NAVIGATING A SUCCESSFUL IAM CLOUD MIGRATION

A practical approach for assessing and planning a migration strategy for your identity and access management program

**March 2020**

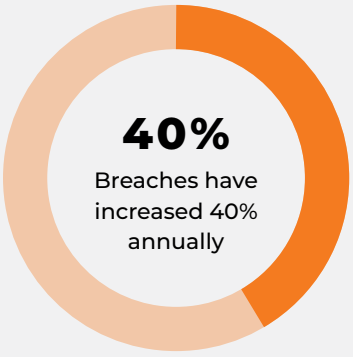
# TABLE OF CONTENTS

**Introduction** ..... **2**
**Where Are You on the Identity Maturity Scale?** ..... **3**
The SecureAuth Identity Framework ..... 3
The SecureAuth Identity Scale ..... 3
**The Primary Questions to Ask When Making A Choice** ..... **4**
What Are My Skill Sets? ..... 4
Do I Want A Single Vendor or A Set of Vendors? ..... 4
Do I Have Regulatory or Other Restrictions on Sharing Identity Information? ..... 4
Do I Need the Ability to Customize the User Experience and Authentication Workflow? ..... 4
**Deployment Freedom** ..... **5**
Extensibility ..... 6
Flexibility of Choice ..... 6
Management and Responsibility ..... 6
**Planning Your IAM Program** ..... **8**
Assess Your Current State ..... 8
Determine Where You Want to Go ..... 8
**Developing an IAM Program Adoption Plan** ..... **9**
Requirements and Business Outcomes ..... 9
Design and Deliver ..... 9
**Conclusion** ..... **10**
**Appendix** ..... **11**

# INTRODUCTION

**WHY WOULD YOU MOVE TO THE CLOUD?** Sure, enormous benefits exist for your business but have you taken the time to understand the risks as well. Your reasoning cannot be simply a "move to cloud for cloud sake" decision. It will need to be a decision that considers the technology, the process changes, the new governance model and the personnel required to implement and maintain the move.

SecureAuth was built on-prem where Identity was born and raised. As the leading vendor for managing authentication into legacy 3rd party technology, we have established our expertise developing secure authentication workflows and exceptional user experience across all systems from Mainframes to Cloud apps. From that established base, we have successfully migrated ourselves to a Cloud model and that experience allows us to help others understand the requirements and processes that need to be addressed as part of the decision when planning the future of Identity and Access Management (IAM).




Breaches continue to litter the headlines and have increased 40% annually. Yet on average, organizations protect roughly 60% of resources with multi-factor authentication (MFA) thus leaving roughly 40% of their resources protected with only a password. The unintended result is Identity has fast become the primary security weakness for most organizations. And with cyber attackers increasingly bypassing MFA, it's time to better protect your workforce and customer identities and secure the access control gap.

The framework in the following paper is intended to help you plan your own internal assessment and identify the next steps in your IAM journey. The goal of the paper is to help you identify what gaps exist today and what items will need to be addressed along the way. We recommend starting the assessment process on your own – and engage with an experienced partner as a next step to review and refine the assessment with your team and provide leadership as your guide to help you navigate your IAM journey.

# WHERE ARE YOU ON THE IDENTITY MATURITY SCALE?

## The SecureAuth Identity Framework

As your organization progresses in its decisioning maturity from Tactical through Strategic and into the Transformational stage, you can see in the "Secure" column the dependency on a Central Identity and a reliance on identifying the right people, devices and services required to achieve a reliable Security model. Understanding where your organization resides in the maturity model will help level-set items such as the scale, level of effort, objectives, and aspiration for your project.

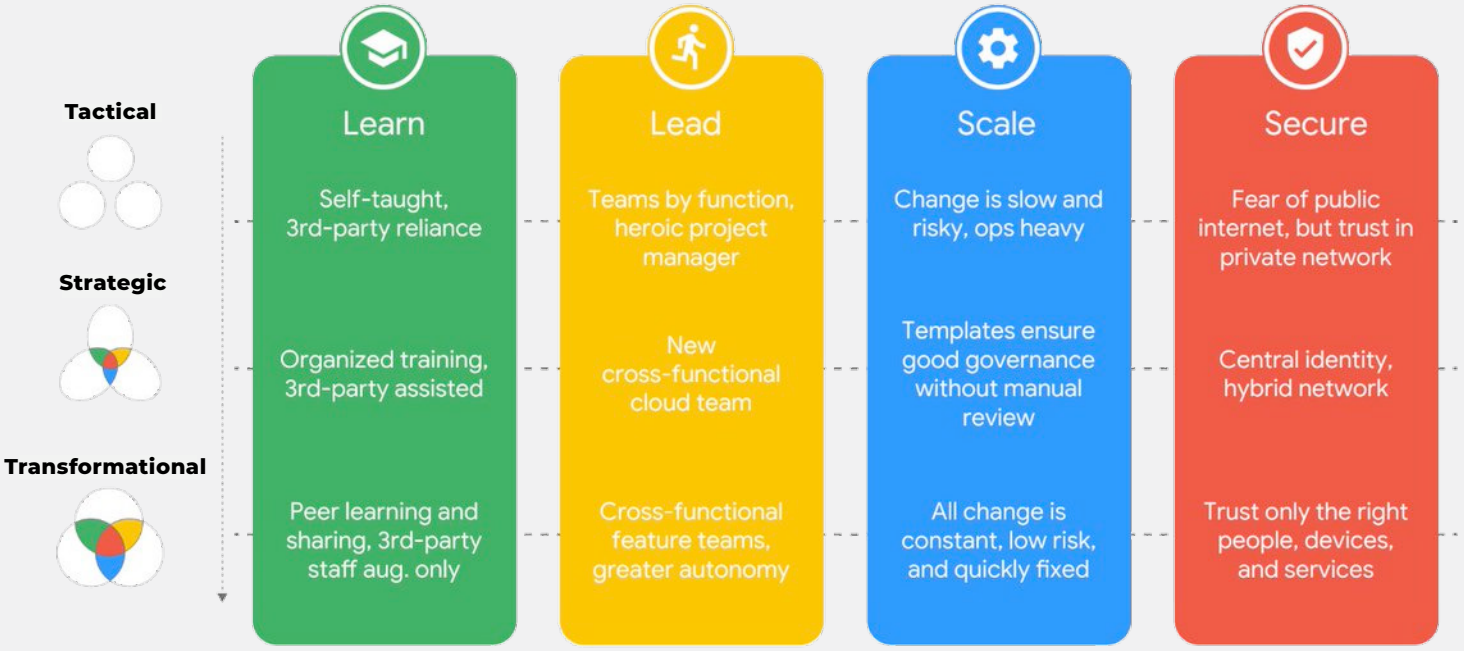



Fig. 1 The GoogleCloud Maturity Scale

## The SecureAuth Identity Scale

An IAM solution is an evolving service and at its foundation is a process which requires consistent evaluation and updates to function and perform optimally. As such, organizations continuously strive to enable new capabilities to drive security and enhance the user experience. Identifying where your organization is on the Access Maturity scale will help develop your objectives and desired future state.

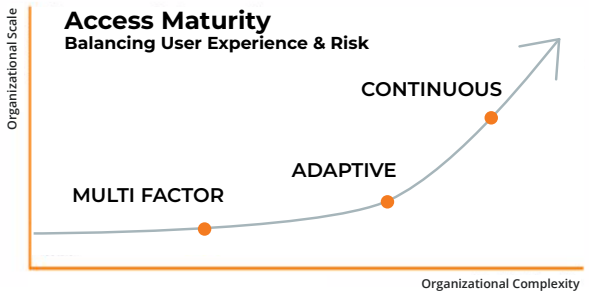



Fig. 2 SecureAuth Identity Scale

# THE PRIMARY QUESTIONS TO ASK WHEN MAKING A CHOICE

## What Are My Skill Sets?

Do I have the personnel to implement, manage and maintain home built solutions? And On-prem?

## Do I Want A Single Vendor or A Set of Vendors?

According to Gartner most SaaS-delivered IAM vendors still do not have solutions to support legacy applications with proprietary authentication interfaces, other than by password vaulting and forwarding. Many of these vendors are working to improve their legacy application support through developments, partnerships or acquisitions. SecureAuth has this functionality built in. There is no need to try an integrate with another vendor, SecureAuth provides the complete package. When planning, Organizations that need support for legacy applications should focus their vendor evaluations and proofs of concept on ensuring that access management tool vendors can support all target applications.

## Do I Have Regulatory or Other Restrictions on Sharing Identity Information?

For example, a B2C full cloud solution would require the sharing of Customer Identities with a 3rd party. Do I need Opt-In, what are my obligations (GDRP, CCPA etc.)? Some software buyers can be risk-averse regarding having a third party manage their authentication and authorization services and hold personal information, and so these buyers may stick to their traditional software deployment. Is a Hybrid solution better for me and can the vendor handle that seamlessly?

## Do I Need the Ability to Customize the User Experience and Authentication Workflow?

According to Gartner, IAM leaders must also evaluate the risks of moving to SaaS-delivered IAM along with the reduced ability to customize:

- Data security, especially credential (password) security
- Service and data residency (depending on the legal restrictions)
- Service availability and business continuity
- Other security controls

Knowing more about the identities accessing your systems can stop attackers from gaining entry with stolen credentials and bypassing MFA. By analyzing multiple characteristics around device, location, IP address, and behavior, it becomes clear if an identity is known or unknown and the appropriate access decision can automatically ensue. If you want to employ phone- based authentication for example, it's critical to check the carrier, phone type, and porting status to ensure an attacker hasn't compromised it. The more you know, the more you can trust and when trust is high you can safely remove authentication disruptions like MFA steps.

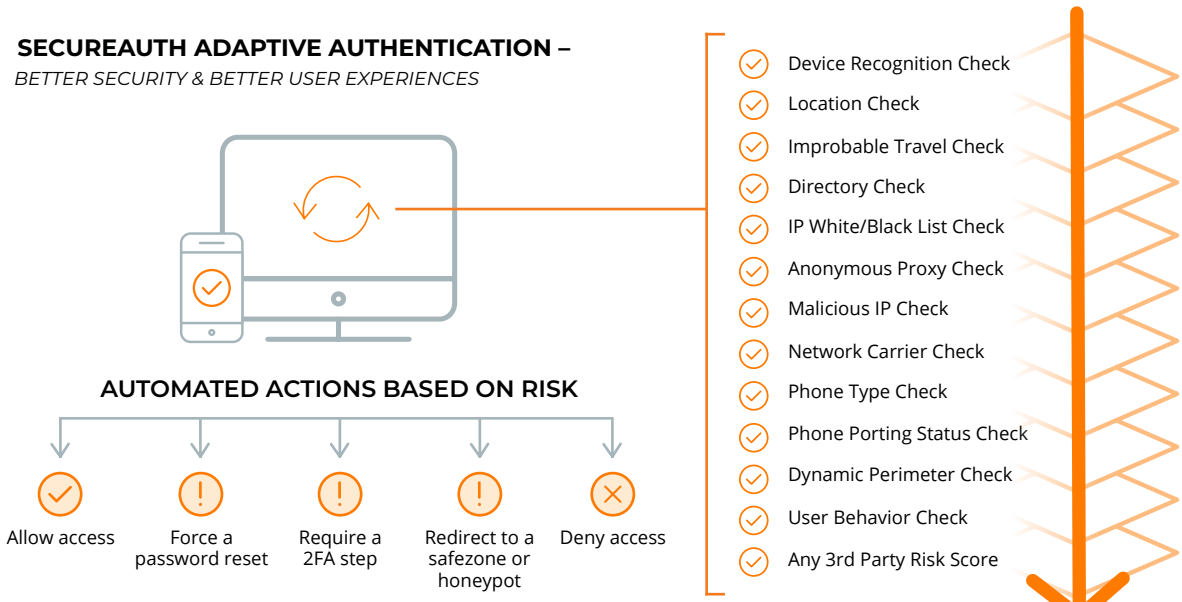



Fig. 3 Adaptive Authentication Model

## DEPLOYMENT FREEDOM

**KNOWING MORE ABOUT THE IDENTITIES** accessing your systems can stop attackers from gaining entry with stolen credentials and bypassing MFA. By analyzing multiple characteristics around device, location, IP address, and behavior, it becomes clear if an identity is known or unknown and the appropriate access decision can automatically ensue. If you want to employ phone- based authentication for example, it's critical to check the carrier, phone type, and porting status to ensure an attacker hasn't compromised it. The more you know, the more you can trust and when trust is high you can safely remove authentication disruptions like MFA steps.

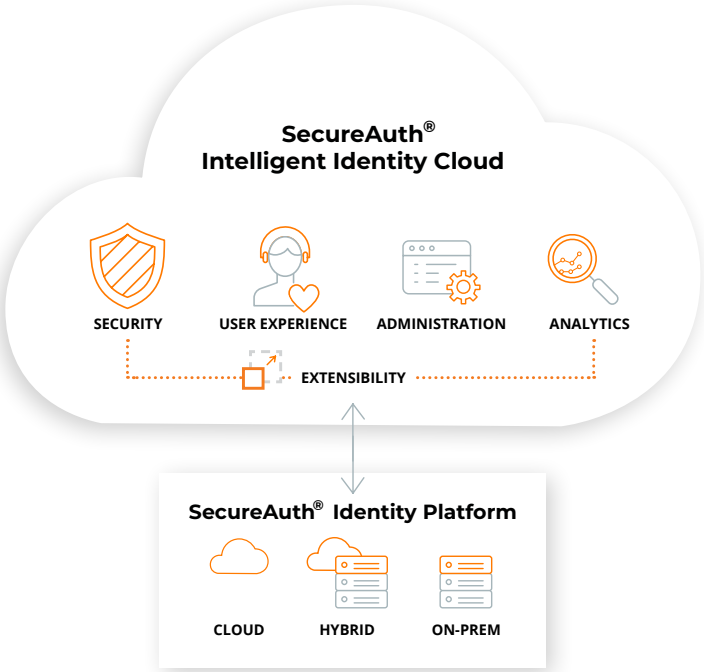



Fig. 4 SecureAuth Intelligent Identity Cloud

## Extensibility

The ability to leverage existing investments in threat intelligence and other security solutions, such as PAM, SIEM, IGA, and UEBA, is key to enhancing and strengthening your IAM solution. Through APIs and pre-built integrations, valuable intelligence can be integrated into the SecureAuth solution to improve analysis in the adaptive authentication process leveraging your own data from industry specific risk and threat intelligence providers. Extensibility expands your ability to separate legitimate users from bad actors and protect your organization and the identities that connect to it.

## Flexibility of Choice

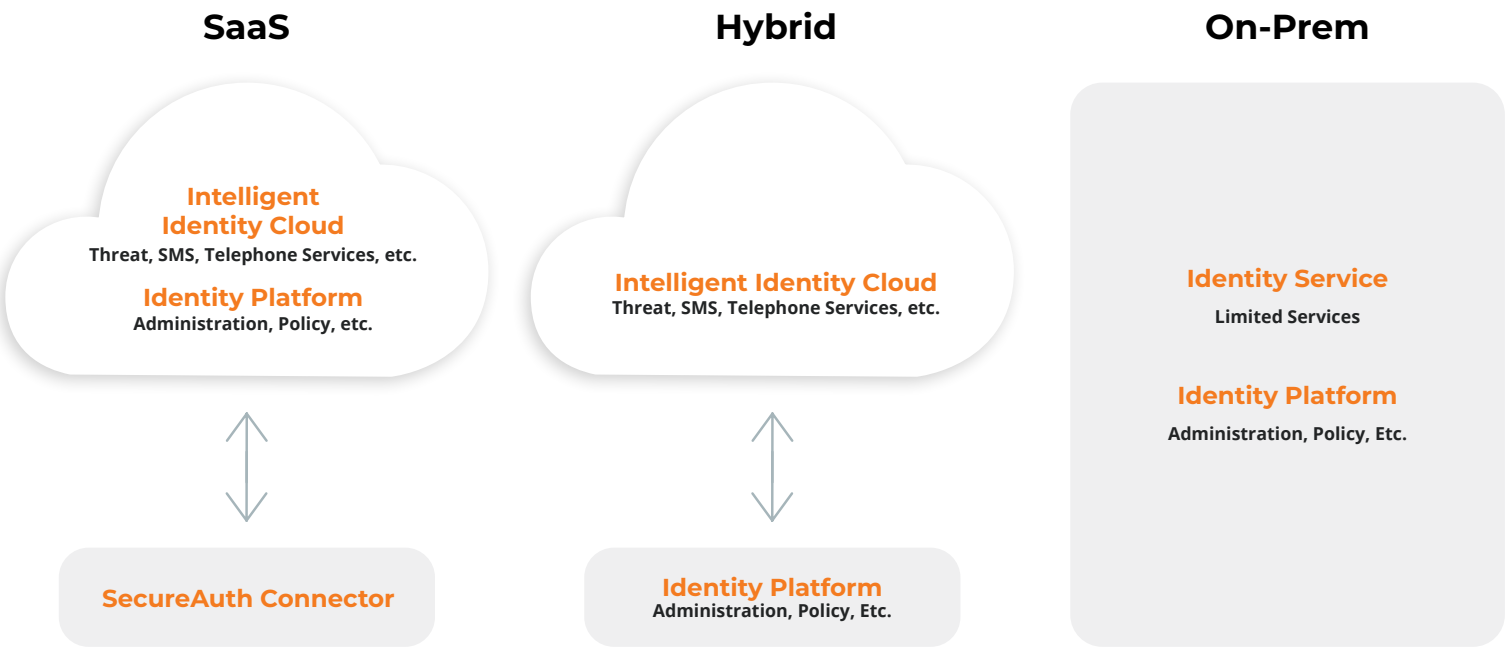
The convenience to manage the same solution regardless of the deployment option provides the ultimate flexibility for your business to continue its digital transformation journey. Because the IAM solution is the same product, the ability to migrate from a hybrid deployment to a SaaS model is a simple migration. You can choose the deployment option best suited for your organization now - knowing that you can migrate in either direction at your own pace. Product consistency, regardless of the deployment model, is a factor which should be considered when implementing an enterprise IAM solution.

| | Identity Platform Deployment Environment | Identity Platform Hosted By | Identity Platform Maintained By | Intelligent Identity Cloud Hosted & Maintained by |
|---|---|---|---|---|
| **SaaS** | **SecureAuth Cloud** | **SecureAuth** | **SecureAuth** | **SecureAuth** |
| **Hybrid** | **Public Cloud** (i.e. AWS, Azure, GCP) | **Cloud Provider** | **Customer** | **SecureAuth** |
| | **Managed Private Cloud** (i.e. AWS VPC, Rackspace) | **Cloud Provider** | **Customer** | **SecureAuth** |
| | **Corporate Private Cloud** (i.e. HPC Helion) | **Customer** | **Customer** | **SecureAuth** |
| | **Corporate Data Center** (i.e. VMWare) | **Customer** | **Customer** | **SecureAuth** |
| **On-Prem** | **Air Gapped Custom Env.** (VMWare, Bare Metal) | **Customer** | **Customer** | **Customer*** |

**Fig. 5 SecureAuth Deployment Matrix**

## Management and Responsibility

Identifying the resources, skillsets, and time your organization has available to administer and manage your IAM solution will provide excellent data points for selecting the appropriate deployment model. Depending on the results of your assessment and your desired business outcomes, a SaaS, Hybrid, or On-premises model can support and meet your requirements.




### Fully Managed by SecureAuth

**Solution hosted and maintained** by SecureAuth, requiring only a lightweight connector to interface with customers' data store and directories

**Single-tenant** Identity Platform for enhanced security.

**Benefits**

- Always On, always Current
- Faster feature update
- Lower operating cost and higher productivity

### Mixed Management

**Intelligent Identity Cloud hosted and maintained** by SecureAuth; Identity Platform hosted[1] and maintained by customers.

**Reduced security exposure** and risk

**Benefits**

- Supports legacy on-prem application
- Provide more flexibility for customization

### Fully Managed by Customer

**Solution hosted and maintained** by customers with potentially reduced features.

**Air gapped** for maximum security

**Benefits**

- Maximum security and regulation compliance.

1. Identity Platform can be deployed to on-prem data center, or Closed Service Providers including Amazon Web Services, Microsoft Azure, or Google Cloud Platform.

Fig. 6 SecureAuth Deployment Freedom

# PLANNING YOUR IAM PROGRAM

## Assess Your Current State

Gather the appropriate team from multiple departments and identify your gaps and stack rank them against your business objectives. Be sure to include reviewing processes and workflows as well as performance expectations as part of your review. Your analysis will provide the data points you need to develop a go-forward plan to help strengthen your IAM program.

**"Is a SaaS, Hybrid, or On-premises deployment the best option today based on your technical and business requirements?"**

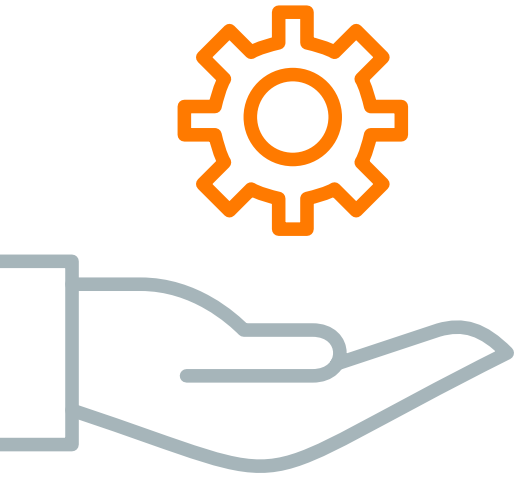
## Determine Where You Want to Go

As you review solution options, it is important to assess the flexibility of the solutions to ensure the capabilities map to your vision and strategic roadmap. Is a SaaS, Hybrid, or On-premises deployment the best option today based on your technical and business requirements. And will you potentially need to pivot your deployment model if business or technical requirements change. Will your IAM solution adapt if or when you need it to?

# DEVELOPING AN IAM PROGRAM ADOPTION PLAN

## Requirements and Business Outcomes

We recognize not all businesses are the same and requirements from one organization to another often vary based on resources, business needs, and security requirements. Ensuring all business units, departments, and stakeholders are included in the overall IAM process is critical to driving success. During the early planning stages understanding the needs, wants, and desires of the overall company ecosystem will strengthen alignment across the business and help fortify a vision for the IAM program. And a constant we acknowledge for any strategic corporate initiative is ensuring a certified Project Manager is engaged early to support and manage the end-to-end-initiative. The ability to manage timelines and expectations is an essential responsibility for every IAM initiative.



## Design and Deliver

For organizations to design and deliver an IAM solution, whether it is deployed in the Cloud, On-Prem, or Hybrid, requires the involvement of multiple stakeholders to ensure alignment throughout the organization on the following:

- Vision of the IAM Program
- External Factors Influencing Success
- Organizational Structure Requirements
- The Governance Structure
- The Program Approach
- The Program Implementation Framework
- The Program Implementation and Delivery

# CONCLUSION

**A CLOUD OR SAAS IDENTITY AND ACCESS MANAGEMENT SOLUTION** is a viable option for your business. As your organization considers a move to the cloud, be sure to avoid the failure to implement a cloud strategy. Doing so can prove to be a competitive disadvantage over time. As you evaluate the technical requirements and the company's business objectives, you will have a choice to make when it comes to deployment options. Your selection will ultimately come down to the balance between Management and Responsibility – what is your appetite for adopting a fully managed solution versus a shared responsibility model. Your choice will depend on business process complexity, your appetite for change, and the economy of scale that makes sense for your business.

Over the past decade, Identity and Access Management has transitioned from an IT-centric administration and compliance tool to a critical security component in the modern digital enterprise. Protecting the business and supporting a rapidly expanding definition of users, a modern IAM solution must secure valuable resources, support multiple use cases, be easy to use for both administrators and users, provide intelligence, and manage the authentication of multiple user types - the workforce, contractors, partners, and customers. Identity and Access Management is a requirement in today's digital world to secure, protect, automate, and enhance an organization's business operations.

However, Identity and Access Management is not a one-size-fits-all proposition. Many companies both large and small struggle with IAM as a program of ongoing integration. Key to long-term success is understanding the strategic value of an IAM solution in the context of your business operations. With a clear view of how your IAM solution supports the business, you can apply resources for measured success and push continuous improvement.

Wherever your organization may find itself in your assessment and planning process for your IAM solution, SecureAuth understands the challenges and can help your team develop an approach to ensure success. Our team of experts will engage and collaborate with your team to develop a roadmap and deployment plan to deliver the IAM program your business requires.

Together, we will secure and protect your valuable data, applications, and resources while simultaneously enabling your users with an exceptional user experience.

# APPENDIX

## Definitions:

### Access Management*

***Objective:*** *Ensuring that only the right people, devices and services are authorized to perform the right actions on the right resources*

Good access management applies the principle of least privilege without stifling those users and resources from legitimately accessing the resources they require to perform their jobs. SecureAuth Intelligent Identity Cloud Service relies on Adaptive Authentication.

### Architecture*

***Objective:*** *providing the best practice recommendations and forward-looking view for the appropriate Identity and Access management choices*

Cloud architecture ensures that applications take full advantage of the cloud platform capabilities and future-proofs the investment in a cloud migration by selecting appropriate compute and storage choices. For example, to achieve elastic scalability, cloud application architecture favors stateless (micro) services that are separated from persistent storage. Cloud infrastructure architecture employs software-defined, immutable components to assure repeatability and security by eliminating manual patching and maintenance.

It is an essential consideration for any business that wishes to achieve a step change in the scalability, availability, and affordability of their self-developed applications, data warehouses, and pipelines, and that seeks to increase development velocity as well.

### Continuous Integration and Delivery*

***Objective:*** *automating changes to the system through a CI/CD process pipeline, so that all changes can be tested, audited, and deployed with minimal interruption.*

In a large, distributed system, there are a lot of unknowns, dependencies, and ownerships, which create uncertainty about whether identity or workflow changes will work as intended. For businesses, uncertainty leads to risk and slows down adoption. A continuous software release process that validates every change — continuous integration (CI) and continuous deployment/delivery (CD) — builds confidence that any identity or workflow change will work as intended.

### Identity Management*

***Objective:*** *reliably authenticating users' or services' identity and guarding against loss of credentials and attempts at impersonation*

Establishing a person's or device's identity with absolute confidence is core to the modern security model in which no single factor is trusted -- not the password, not the certificate, and most certainly not the IP address — and yet, by combining many factors, can be trusted from anywhere on any network.

## Instrumentation*

***Objective:*** *logging events, as well as tracing, profiling, and debugging workflows, so that the behavior of a user Identity can be examined under any circumstance and service-level objectives can be quantified.*

Comprehensive instrumentation, while essential in any IT operating model, plays an even more important role in Identity and Access Management. It provides crucial insights to help triage whether SecureAuth's services or your own application is the root cause for an observed poor performance or degraded service. Finally, comprehensive logging provides a gapless and immutable audit trail of who performed which action to which resource or configuration, which in turn helps make your organization's operations inherently more secure.

## People Operations*

***Objective:*** *defining the required organization structures and aligning the delivery and operations with the right role, skill and performance measures to help them fulfill their new tasks and duties*

Alignment of the organizational structure, people, and performance measures ensures that teams are set up to receive the change and embrace their new duties.

It is also important to ensure that cloud adopters are incented for executing their new responsibilities and behaviors (e.g., collaboration, transparency, acceptance of failure, trust) through the performance management process and incentive structures.

Finally, it is critical to set organizational goals that are both measurable and able to be influenced by the journey that the organization is on. Misaligned goals and initiatives will have a negative impact on the success of Identity and Access Management adoption.

## Sponsorship*

***Objective:*** *passionately and continuously demonstrating executive support for the IAM strategy, so that early adopters have a widely recognized mandate for change.*

Sponsorship refers to the active and visible support that executives and team leaders give to the IAM initiative or project within the organization. Enterprise Identity and Access Management is complex. Strong sponsorship is vital when organizations make the decision to go forward with organization-wide deployments whose intent is to add value and drive organizational collaboration and velocity.

As the most influential individuals within an organization, executives must passionately and continuously demonstrate executive support for the IAM strategy, so that early adopters have a widely recognized mandate for change.

## User Experience*

***Objective:*** *ensuring the continued satisfaction of the user in the day to day performing their role or function. Identification should not be a concern for them, it should be a concern for the business. The organization should implement methods that make the user identification as simple as possible for the user and as robust as necessary for the business unit.*

The one constant in Security is the understanding that if Security creates too much friction in the user experience, the user will find a way around the security. Access controls must be a balance between Risk and Usability. The level of risk accepted must be based on the risk appetite of the company.

## Upskilling*

***Objective:*** *investing in learning, so that the incumbent staff may combine their existing in-depth knowledge about the business and the current state of IT with learnings about the new best practices.*

Cloud computing marks a paradigm shift in IT the likes of which the industry has not seen since the introduction of virtualization. These new principles and best practices can be studied in many ways to suit your teams' individual learning styles, ranging from instructor-led training courses to self-serve interactive courses.

Upskilling is about more than just understanding the technical theory. It's about applying the learning on the job, self-sufficiently researching solutions to issues online, or reaching out to SecureAuth Support and sharing lessons learned with peers, to nurture a culture of continuous learning and to grow institutional knowledge.

## References

**Figure 1. Google Cloud Maturity Scale**
The scale references the model presented by Google in the Google Cloud Adoption Framework
**https://services.google.com/fh/files/misc/google_cloud_adoption_framework_whitepaper.pdf**

* Definitions are based on the language used by Google in the Google Cloud Adoption Framework
**https://services.google.com/fh/files/misc/google_cloud_adoption_framework_whitepaper.pdf**

SECUREAUTH