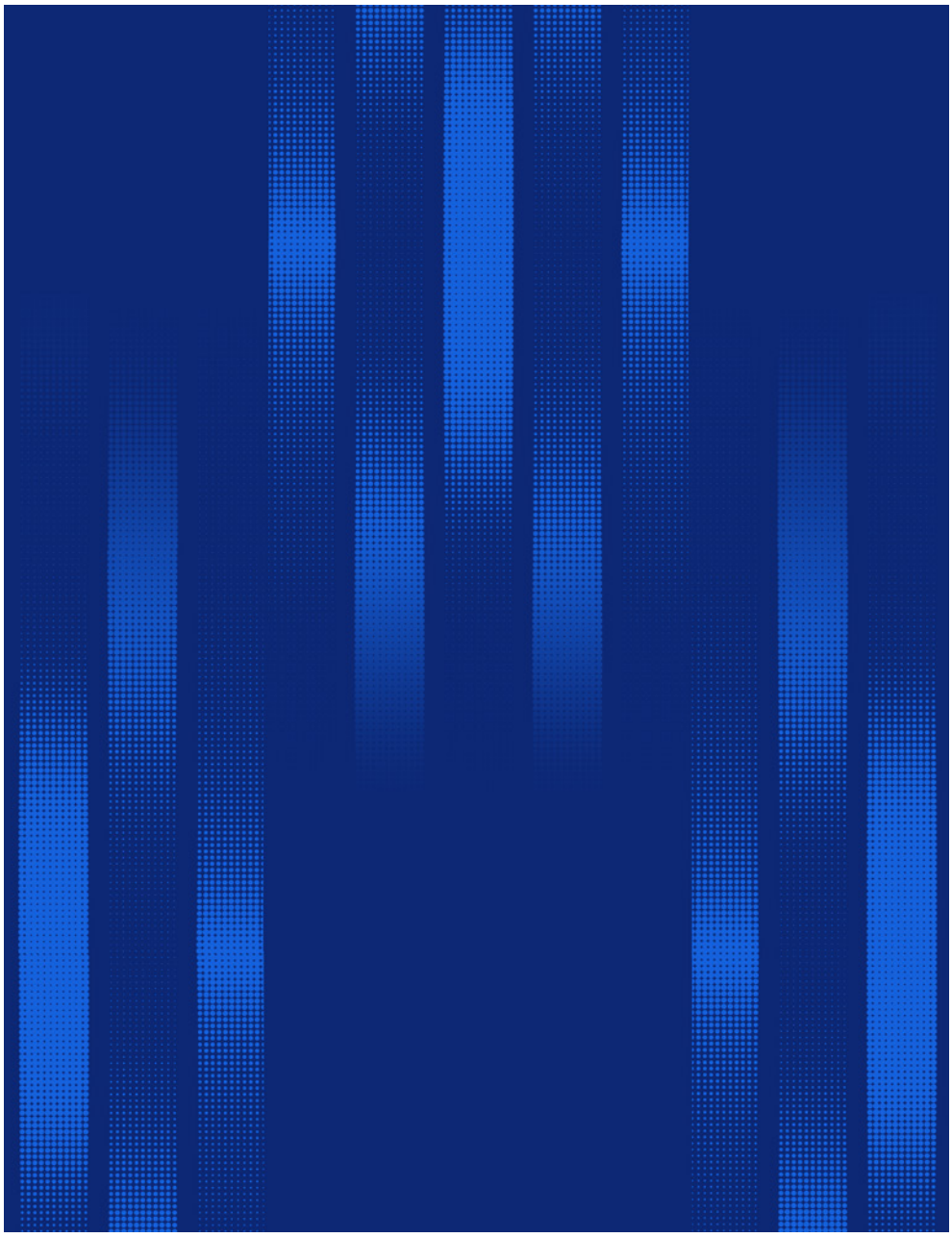
Whitepaper

September 2022

A Comprehensive Guide for Your Workforce Identity Maturity Journey

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



okta

Ubiquitous identity and access management

IT leaders today must stay on top of emerging technologies to help their businesses move faster, execute on priorities, and drive sustained growth. Cloud-first strategies are key to reaching these strategic goals, as they deliver greater flexibility. This is especially true for distributed, dynamic workforces that include contractors and business partners, for whom data regulation and privacy are top concerns. Organizations that deliver the secure and frictionless experiences demanded by today's digital-first workforces will separate themselves from the pack.

In this context, identity and access management (IAM) has become both a necessity and a ubiquitous enabler for any modern business. IAM enables people to work from anywhere with seamless and secure access to critical tools and resources. Behind the scenes, IAM also helps IT teams support this dynamic workforce by simplifying user management, automating key identity processes, and protecting against identity-centric cyberattacks.

Although the need for a robust, holistic approach to identity is clear, progress varies when it comes to addressing security, efficiency, scalability, and other challenges to identity maturity. Many organizations are making headway towards a successful identity implementation and strategy, but the journey is rarely straight or narrow for any company.

The journey towards modern workforce identity

Often, teams lack the right tools, skills, or approach to establish a sustainable identity fabric that effectively balances user experience with security. To help you determine the best ways to mature your IAM, we've collated the most successful practices and patterns across thousands of Okta customers.

In this companion piece to our **customer identity maturity guide**, we'll focus on how to advance traditional IAM strategies for workforce users such as employees, contractors, and partners. Below, we lay out our comprehensive maturity model, exploring evaluation criteria and the optimal journey for all your identity needs. Read on for guidance about specific steps that simplify identity administration and strengthen your identity posture, so you can get on the path towards delivering new digital experiences, protecting against security threats, and improving operational efficiencies with modern IT infrastructure.

What is an identity maturity model?

Okta's Identity Maturity Model (IMM) is a framework for assessing the current state of your identity capabilities and effectiveness, creating a plan to improve them, and measuring ongoing success and value at each stage. By understanding your IAM landscape and evaluating the identity and security capabilities required to achieve your organization's long-term business objectives (i.e. where you're at and where you're going), you'll learn how to best focus your efforts and investments. This will ultimately position your business to more easily scale in response to new identity and security requirements, as well as shifting end-user demands.

5 areas of assessment for identity maturity

The first step on this journey is to conduct a thorough and realistic assessment of your company's existing approach to identity, including key capabilities and challenges. This evaluation should examine five critical categories: agility, experience, security, reliability, and strategy.

Agility

Ability to deploy, manage, and develop identity-related services and flows

Experience

Ability to deliver effective, desirable, and convenient experiences to end-users

Security

Ability to proactively and effectively mitigate and remediate security risk and incidents

Reliability

Ability to provide a resilient, high-performing, future-ready identity service at any scale

Strategy

Ability to plan and deliver holistically, intelligently, and with a focus on innovation

Specifically, as it relates to **workforce identity maturity**, you should assess the following:

1. **Agility** in deploying and managing identity-related services and flows

- Does your identity service provide modern IAM across the entire IT stack (from cloud-based SaaS applications and infrastructure to legacy systems and on-premises resources)?
- Can you accelerate the adoption of any custom-built or best-of-breed technology at the pace your business requires without compromising security?
- Do your administrators have an intuitive and centralized console for managing profiles and governing the lifecycle of all identities?
- Does your identity provider offer automation and orchestration capabilities to easily extend and customize your IT stack?

2. Delivery of a seamless and convenient **employee experience**

- Can employees self-serve to request applications and resolve authentication-related issues?
- Do you provide them with seamless and secure remote access that drives productivity across the hybrid work environment?
- Do you automatically provision “birthright applications” for employees by their first day of work?
- Can your organization automate identity-based processes to boost employee productivity and agility, without writing code?

3. Mitigation and remediation of **security** risks and incidents:

- Does your IAM solution enable secure access to resources for employees, as well as for your entire information supply chain of business partners (suppliers, resellers, distributors, and affiliate organizations such as subsidiaries and franchises)?
- Do you embed contextual insight and intelligence on behavioral patterns in your policies to prevent access under anomalous conditions?
- Are you able to quickly uncover and resolve identity-related security incidents, and have you established security service-level agreements (SLAs) around these processes?
- Have you implemented a Zero Trust, identity-based security model to reduce your attack surface and mitigate threats?

4. Ability to provide a **reliable**, high performing identity service at any scale

- Do you experience outages that impact employee productivity, particularly in revenue-generating business functions?
- Is your identity service able to handle demand fluctuations without interruptions, even when unexpected?
- Are you able to scale your identity service to grow with your dynamic workforce?

5. **Strategic** focus and vision for future identity needs and innovations

- Is your identity strategy aligned and unified across all of your regions and business units?
- Do you have a clear, holistic vision of how to evolve your identity service to meet business needs?
- Is it fully-funded, multi-year, and supported by executive buy-in?
- Can you proactively measure and maximize the return on investment (ROI), total cost of ownership (TCO), and business benefits of your identity service?

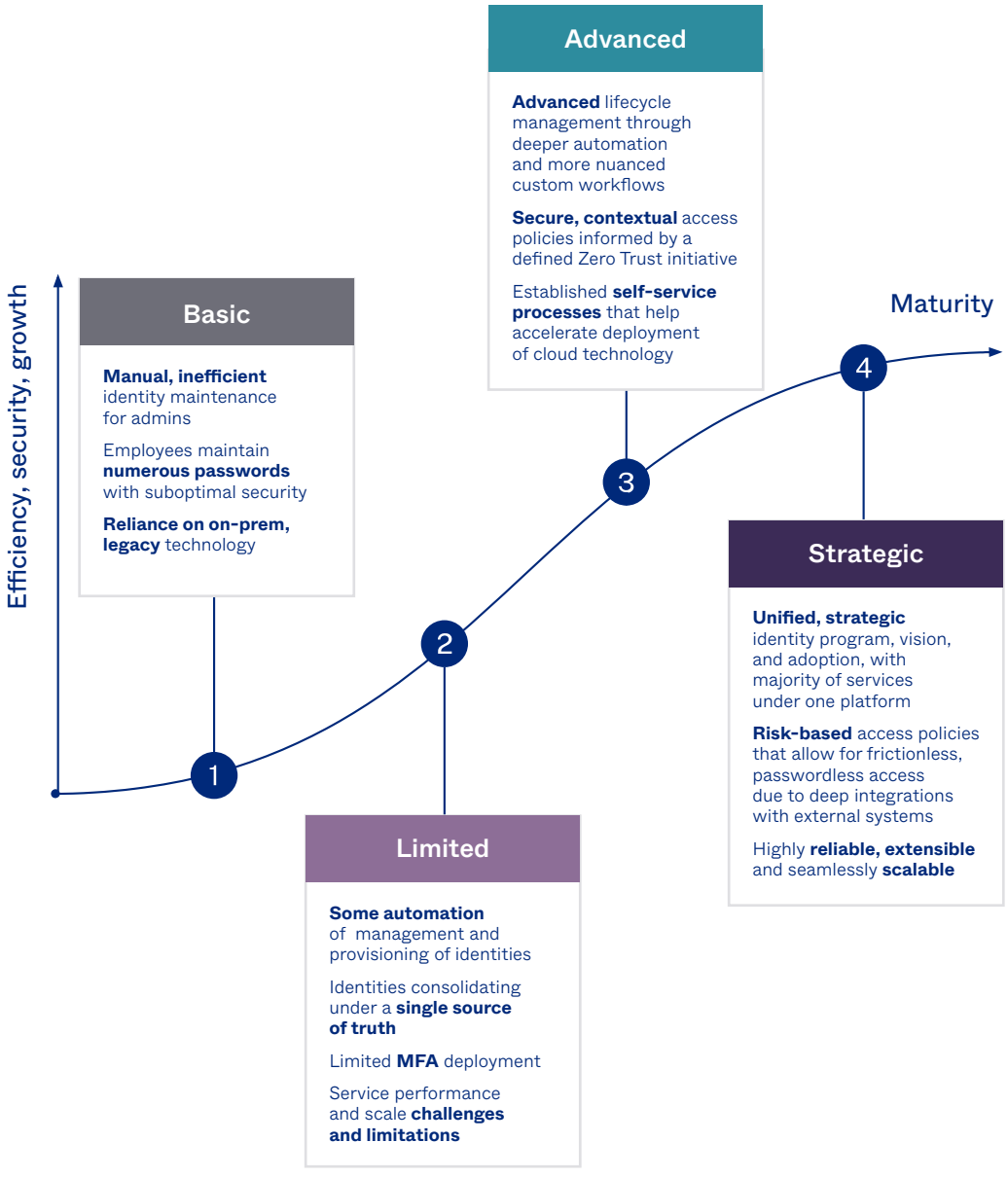
Mapping the way to workforce identity maturity

After assessing the maturity of your current workforce identity capabilities, it's helpful to familiarize yourself with the four primary stages of Okta's IMM:

- Basic
- Limited
- Advanced
- Strategic

Each step along this path unlocks more value for your organization by advancing IAM sophistication.

The workforce identity maturity journey



Our model provides guidance for launching an extensible identity strategy, with a starting point to evolve your organization from manual, inefficient, and fragmented identity functions to automated, intelligent, and scalable ones. That said, keep in mind that each individual business may require a different level of maturity, and not all organizations will elect to reach Stage 4.

Key metrics for evaluating IAM success

As you journey through the four stages of maturity, it's important to think about how your organization is investing in key business outcomes. By consistently measuring key performance indicators (KPIs), such as the ones below, in each of the five identity maturity categories, you'll be able to show progress over time.

Agility KPIs

FTE hours dedicated to identity administration, time to adopt and deploy apps, cost or time spent maintaining legacy infrastructure

Experience KPIs

Volume of tickets related to access or requests for apps, employee satisfaction scores, time spent authenticating, getting access to new apps, or onboarding new users

Security KPIs

Number of identity-related security issues, time to detect (and respond), cost of a security breach, time spent on audits and reporting, employee adoption of advanced authentication

Reliability KPIs

Average minutes and cost of unplanned downtime per month, number of incidents that led to lost productivity or employee complaints

Strategy KPIs

Annual investment in identity-related technologies, term of fully-funded identity program, identity service ROI and TCO

To see an example of how you can calculate ROI for your IAM solution, visit **https://www.okta.com/roi/**

Your stage-by-stage maturity guide

This next section provides an overview of each maturity stage, including common goals and challenges we've observed throughout the Okta community. We also recommend key ways to advance your identity capabilities in each phase, so you can improve operational efficiencies, eliminate security gaps, and deliver even more value along the way.

Stage 1: Basic

Goals & challenges

Over time, many companies accumulate multiple disconnected identity stores, with IT teams managing fragmented identities across a mix of disparate applications on-premises and in the cloud. This is made more complex by departments outside of IT acquiring and leveraging apps and tools for their own business needs — solutions that need to be tracked and united under a single IAM program. Since IT organizations often lack deep expertise or insight around how identity should fit into their broader business strategy, you may find yourself spending significant time and resources on building and maintaining even rudimentary identity services.

At the beginning of the IAM maturity journey, businesses tend to rely primarily on manual processes and bare essential capabilities to manage users and applications. As companies work on gaining more control of employees and members of the extended workforce at this stage, some typical goals include:

- Minimizing orphaned accounts and unmanaged roles, groups, and apps
- Increasing remote access for a hybrid workforce
- Decreasing the numerous (most likely insecure) passwords users have to remember
- Reducing the burden on IT to manage password resets and account lockouts
- Addressing security vulnerabilities

Our recommended steps and capabilities

If your organization is at this stage, we recommend implementing the following workforce identity solutions and capabilities in order to proceed to the next level of maturity:

Agility

- User repository consolidation and synchronization (with custom scripts) across legacy directories and systems of record, which may include Active Directory (AD) domains, LDAP servers, HR systems, etc.
- Basic identity administration user interface (UI) for user and policy management (although you may still be highly reliant on manual execution from IT teams)

Experience

- Basic single-sign-on (SSO) deployment and end-user authentication, which may include delegated authentication support for AD/LDAP users and a single multi-factor authentication (MFA) policy for all (including privileged accounts)
- Simple self-service functions, such as credential reset and password recovery (although frequent help desk assistance may still be required)

Security

- Authorization server compliant with modern standards (e.g., OpenID Connect (OIDC), Open Authorization (OAuth) 2.0, Security Assertion Markup Language (SAML)
- Basic role-based access policies that reflect user group needs and network zones

Reliability

- Identity infrastructure with basic high-availability architecture, failover, and disaster recovery capabilities, SLA standards, etc.

Strategy

- Comprehensive inventory of all on-premises and cloud apps used by your workforce to clarify app ownership and reduce the risk of unknown business IT (i.e., shadow IT)
- A business case to secure budget allocation and executive support for identity improvements

Stage 2: Limited

Goals & challenges

Once companies graduate from Stage 1, they are on their way to consolidating all identities under a centralized single source of truth and management plane. They've also reduced password sprawl and increased secure access to applications by deploying SSO and limited MFA.

Your next focus is likely easing the IT administrator burden by automating high-volume, low-complexity employee joiner, mover, leaver tasks — an effort that's made easier with an intuitive identity admin portal and centralized, low-touch user lifecycle management. Businesses at Stage 2 usually begin to recognize the many benefits of an automated and intelligent IAM service, while at the same time unearthing more security gaps they need to fill.

Our recommended steps and capabilities

In order to proceed to the next level of maturity, we recommend organizations implement the following customer identity solutions and capabilities:

Agility

- Unified user directory, retiring legacy technologies (ADs and other on-premises services)
- Limited automated lifecycle management for onboarding and offboarding employees and provisioning of downstream application acces

Experience

- Extended SSO capabilities, providing simpler access for employees, contractors, and partners, such as the support of third-party identity providers (IdPs)
- More fully operational self-service functions for employees that lessen the IT team's burden

Security

- MFA with at least two assurance factors (e.g., SMS, email) and enforcement of access policies across applications (although MFA may still be limited in terms of devices, methods, and use in app access)
- Initial solutions and steps towards a Zero Trust architecture, such as applying dynamic access policies to apps
- Auditing and monitoring tools to regularly evaluate security irregularities

Reliability

- Expanded identity infrastructure to support performance and reliability at scale
- A plan for bursts / spikes that often require ad-hoc investments and manual intervention

Strategy

- Alignment and communication between business units leveraging IAM technologies, with specific areas of ownership and responsibilities defined
- Realistic evaluation of IAM gaps and requirements to drive remediation and investment plans

Stage 3: Advanced

Goals & challenges

Organizations at this stage are building a strong foundation to support and scale increasingly dynamic workforces of employees, contractors, and partners who work remotely and in offices. This requires IT teams to deliver simple and seamless access (e.g., one set of credentials for each individual to access key applications and systems, which may include multiple clouds), while safeguarding data security and privacy and adhering to increasingly rigorous compliance and audit requirements.

Perhaps you're starting to improve security posture through contextual access policies based on rich signals about who each user is and where they are, which application they are trying to access, and their current device and network security risks. With different user types and access rights, it is critical to address any risks posed by privileged accounts, eliminating standing privileges as needed.

Another focus is speeding new employee productivity, in part by more deeply integrating identity with HR sources to streamline and automate complex lifecycle tasks. Stage 3 IT teams aim to enhance backend identity systems and infrastructure by introducing more advanced automation and process efficiencies. Overall, your objective is to minimize IT intervention where possible, which reduces the chance of human error and frees your team up for more strategic priorities that help move the business forward.

Our recommended steps and capabilities

At this stage, we recommend organizations implement the following IAM solutions and capabilities in order to proceed to the next level of maturity:

Agility

- Advanced automations to codify a majority of user lifecycle management business rules and minimize the need for manual developer and IT intervention
- Out-of-the-box integrations with HR systems for deeper automation that quickly surfaces lifecycle changes

Experience

- Day-one access to key systems and apps for a seamless new employee experience
- Complete employee self-service for popular app requests, password management, and MFA factor changes
- Some adoption of passwordless technology, bolstered by an access policy that only prompts users for a second factor during risky login attempts

Security

- MFA with adaptive features that leverage a variety of high assurance factors and behavioral inputs to assign risk and step-up authentication only when needed
- Some out-of-the-box integrations with third-party tools / systems to capture and manage security events and signals
- A defined Zero Trust initiative, discrete context-based policies that maintain least privilege, and secure access extensions to APIs and servers

Reliability

- Built-in service resiliency with redundant servers, load balancers, and high-availability infrastructure

Strategy

- Formal and ongoing processes, plans, and organizational ownership for identity posture
- Ability to track and quantify a variety of identity-related KPIs / metrics to demonstrate measurable improvement
- Trained, dedicated IAM experts in-house

Stage 4: Strategic

Goals & challenges

Every business may require a different level of maturity, and not all will need or choose to reach Stage 4. Businesses that have reached this point have typically embraced a dynamic workforce and recognized the associated need to ensure teams can work efficiently without friction, no matter where they are. At this level, organizations view identity as pivotal to their success, and have achieved a robust and sustainable IAM implementation. Stage 4 reflects a continuous journey of incremental optimization and improvements, rather than an end state.

By this point, your employees enjoy modern digital access that optimizes for both user experience and security, while empowering IT administrators to tackle more strategic initiatives. You've embraced a cloud-native approach to IT and security, a holistic Zero Trust security strategy, and no-code/low-code solutions that enable any line of business or geography to build custom workflows for localized requirements.

At Stage 4, businesses must continue to innovate and enhance digital workplace tools with rich, up-to-date IAM features. This is the time to prioritize the next level of fine-grained, risk-based access policies, passwordless authentication, and data-based risk management. Look for modern technologies that can understand your risk tolerance and weigh data-based considerations in a way humans just can't.

Our recommended steps and capabilities

In order to optimize identity's impact at this stage, we recommend organizations implement the following IAM solutions and capabilities:

Agility

- Full automation of identity and security policy management, user lifecycle management, and complex identity-related business workflows
- A centralized, intuitive admin UI with a unified view of all users and their entitlements

Experience

- Highly extensible and frictionless employee, contractor, and partner access experiences, across all devices
- Widespread adoption of passwordless login that uses strong MFA factors

Security

- Risk-based, fine-grained access control for continuous and adaptive authentication and authorization
- Intelligent MFA engine with the ability to ingest and analyze risk signals from a variety of sources
- Fully automated security workflows that support incident response and identity orchestration

Reliability

- Resilient infrastructure that seamlessly and dynamically scales with demand spikes, including during unforeseen, highly trafficked events

Strategy

- Fully-funded, multi-year identity program with executive buy-in
- Diverse internal stakeholder teams collaborating on identity strategy and program like a well-designed machine

Stage 1: Basic	Stage 2: Limited	Stage 3: Advanced	Stage 4: Strategic
Goals & challenges			
– Moving away from manually managing users and apps – Reducing the number of passwords – Minimizing orphaned accounts and unmanaged roles, groups, and apps – Understanding how identity fits into business strategy	– Consolidating identities under a centralized single source of truth – Reducing password sprawl – Easing IT administrator burden – Improving security posture	– Scaling and speeding efficiency for a dynamic workforce – Improving security posture through contextual access policies – Minimizing IT intervention with advanced automations and process efficiencies	– Optimizing for user experience and security – Embedding continuous and intelligent authentication and authorization – Simplifying the task of customizing identity processes
Our recommended steps and capabilities for each maturity level			
Agility			
– Consolidate and synchronize user repositories across legacy directories and systems of record – Basic identity administration UI for user and policy management	– Unified, modern user directory – Retire legacy systems – Partially automate user lifecycle management and provisioning	– Advanced lifecycle management and automations – Out-of-the-box integrations with HR systems	– Fully automate policy, user lifecycle management, and identity-related business workflows – Centralized, intuitive admin UI
Experience			
– Basic SSO deployment and end-user authentication – Simple self-service functions (password recovery, etc.)	– Extended SSO capabilities for employees, contractors, and partners w/ support for 3rd party IdPs – More fully operational self-service functions	– Day-one access for new employees – Complete employee self-service for popular app requests, password management, etc. – Passwordless bolstered by contextual access policies	– Highly extensible and frictionless workforce and partner access experiences, across all devices – Widespread adoption of passwordless login
Security			
– Authorization server compliant with modern standards – Basic MFA and role-based access policies that reflect user group needs and network zones	– Limited MFA with access policies across apps and at least 2 factors – Initial steps towards Zero Trust, (e.g., dynamic access policies) – Audit and monitoring tools	– Adaptive MFA – Least privilege; secure access to APIs and servers – Some out-of-the-box integrations with 3rd party tools to capture security events – Defined Zero Trust initiative	– Intelligent MFA able to analyze risk signals from various sources – Fully automated processes supporting incident response and orchestration – Risk-based, fine-grained access control
Reliability			
– Basic high-availability architecture, failover, disaster recovery capabilities, SLA standards, etc.	– Plan for bursts/spikes often requiring ad-hoc investments and manual intervention	– Redundant servers, load balancers, and high-availability infrastructure	– Resilient infrastructure that scales seamlessly and dynamically
Strategy			
– Comprehensive inventory of all on-premises and cloud apps – Identity business case to secure budget and executive support	– Alignment and communication between BUs – Evaluation of gaps and requirements to drive investment plans	– Formal and ongoing processes for evaluating identity posture – Identity-related KPIs – Identity experts in-house	– Multi-year identity program with executive buy-in – Diverse stakeholder collaboration on identity strategy

Benefits of identity maturity

This IAM maturity model drives several valuable business outcomes, such as:

- **Increased identity management effectiveness and ROI,** with each stage of maturity delivering more value than the last.
- **Improved employee experience,** thanks to IT efficiencies from intuitive tools for centralized identity administration and process automation.
- **Revenue acceleration** via increased employee productivity and business agility through rapid deployment of cloud technology that unlocks new business opportunities.
- **Brand reputation protection** by mitigating security risks and recovering promptly when incidents do occur.
- **A cohesive, forward-looking identity strategy** that grows with the business and positions it for success.

The ultimate IAM benefit: business agility

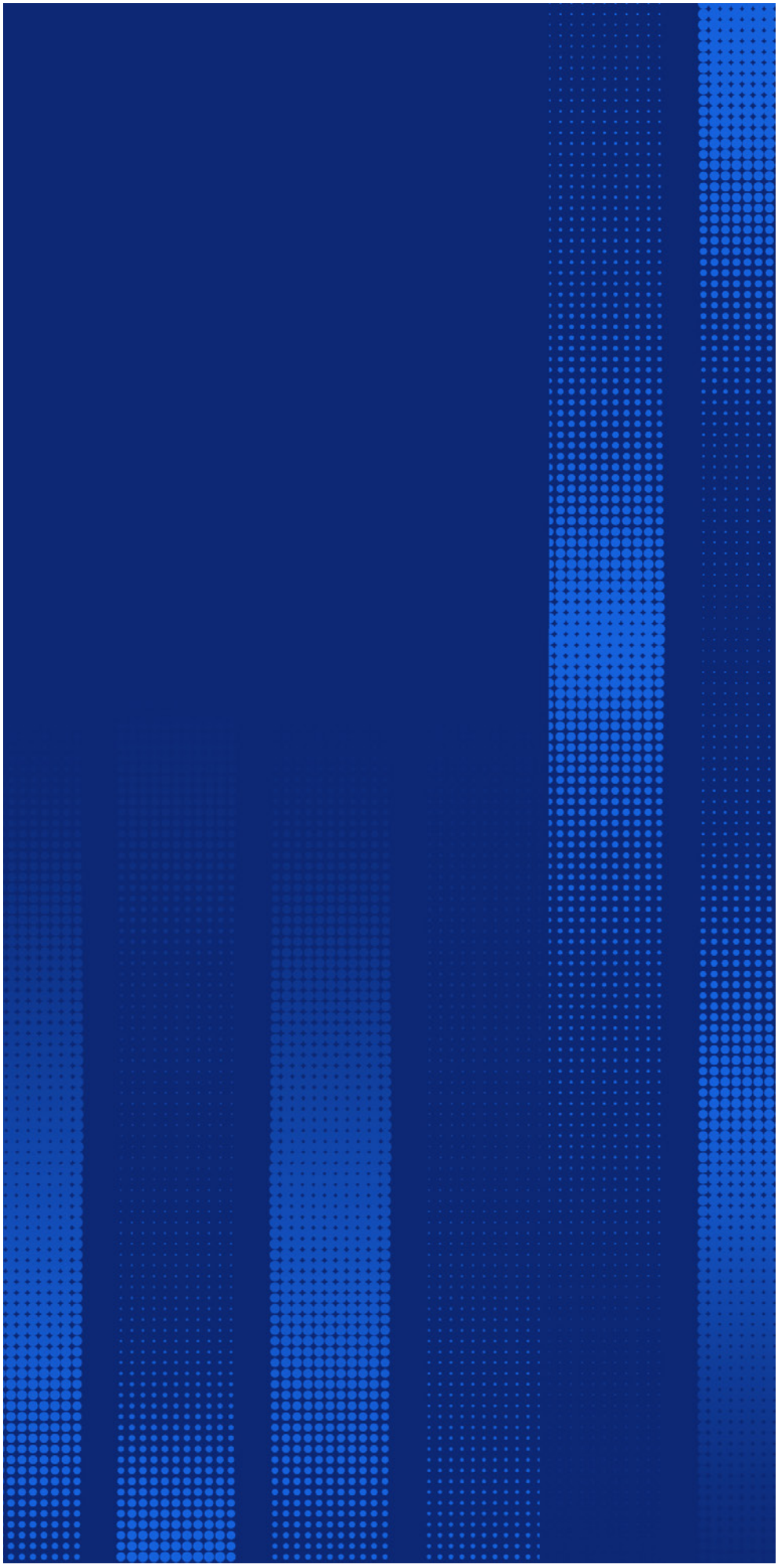
Okta's workforce identity maturity model offers insight into critical business and IT opportunities that will help differentiate your company. At each phase of your journey, it's important to reflect on your progress, consider next steps, and track success towards innovating the digital experience, strengthening security protections, and driving business growth.

In the next edition of this maturity guide, we'll share how maturing your workforce identity posture will map to real business capabilities that generate value for your company.

Industry leading solutions like Okta unleash this value by freeing up IT time and resources. As a result, your team can do their most meaningful work while we focus on staying ahead of identity and security risks and requirements. To learn more about how Okta's proven IAM solution can quickly get you on the path to workforce identity maturity, visit **okta.com/workforce-identity**.

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 16,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, and Teach for America, trust Okta to help protect the identities of their workforces and customers. For more information, go to **okta.com**.



okta