



The Okta Identity Maturity Model

Your roadmap for strengthening security and compliance through Zero Trust, improving end-user experiences, and increasing operational agility with identity

Links

Strengthening security —
and so much more



Authentication



Identity Stores



Risk Assessments



Access Management



Visibility and Analytics



Automation and Orchestration



Governance



Conclusion



Strengthening security — and so much more

Identity and Access Management (IAM) was once a service that primarily managed usernames and passwords. Now, it's so much more, empowering your organization to securely engage with your workforce, customers, and partners — wherever, whenever, and on whatever device.

When identity is strong:



Security tightens,
and governance, risk,
and compliance
(GRC) is simplified



Operations move
faster, with extensive
automation and
fewer errors



Users can more easily
access the resources
they need, when they
need to

But identity's reach, impact, and complexity can make it hard to know where to start, to assess where you stand today, and to create a roadmap to get your organization where it needs to be.

The Okta Identity Maturity Model (IMM)

Based on patterns and collective best practices we've observed across more than 19,450 Okta customers, the **Okta Identity Maturity Model (IMM)** is a value-driven framework that provides both a roadmap and evaluation criteria for achieving business outcomes. This framework builds upon the foundation laid by other technology-based frameworks to address how identity can be the driving force behind organization-wide business outcomes.



Within the IMM, four progressive stages map identity capabilities along the maturity journey:



Fundamental

Meeting essential identity needs while creating a strong, reliable foundation for maturation



Scaling

Expanding a consolidated identity footprint to new apps, services, use cases, and users



Advanced

Increasing automation and integration to elevate experiences, improve agility, and strengthen security



Strategic

Gaining a strategic advantage through initiatives that empower the workforce, optimize efficiency, and leverage identity to detect and respond to threats in real time

The table below demonstrates how maturing through these stages delivers meaningful, measurable outcomes across the critical value pillars of Security & Compliance, Operational Agility, and End-User Experience.



okta



Stage 1: Fundamental

Organizations often struggle to enable applications and users while preventing identity-based attacks. To mature, they must consolidate and simplify their identity infrastructure.



Stage 2: Scaling

With fundamental identity functions in place, focus shifts to refinements that help underlying/enabling operations scale. This requires layering security controls and expanding automation.



Stage 3: Advanced

Organizations have established a broad range of identity systems, focusing on advancing high-impact, easily achievable controls through automation or strengthened security policies.



Stage 4: Strategic

This final, ongoing stage is largely about extending controls and automation to as much of the organization as possible, and reaching a steady state characterized by refinements and optimization.

Value Pillar

Example Outcomes

Security & Compliance

- Proactively mitigate and remediate identity threats
- Achieve and maintain critical compliance certifications
- Streamline and secure end-user access with principles of least-privilege access

Increase defense against identity attacks by implementing basic single sign-on (SSO) and multi-factor authentication (MFA) with role-based access control (RBAC) policies.

Initiate early stages of a Zero Trust architecture with dynamic access policies.

Implement risk-aware and phishing-resistant authentication and authorization.

Employ intelligent, contextual, and continuous authentication and authorization that can keep pace with modern-day intrusions.

Operational Agility

- Increase operational efficiency / reduce operational costs
- Increase employee efficiency
- Streamline merger and acquisition integrations

Move away from manually managing users and apps.

Automate across the user lifecycle and provisioning

Employ advanced lifecycle management (LCM), with automation for common tasks such as access requests and approvals and app provisioning.

Fully automate policy, user LCM, and identity-related IT and security operations workflows across cloud apps and services.

End-user Experience

- Improve the end-user's digital experience
- Increase sign-up and login conversions

Establish an inventory of all applications and secure login flows with baseline protections like MFA, bot detection, and strong password policies.

Expand SSO and MFA to all user types, introduce early passwordless options like FastPass and passkeys, and standardize self-service access for common needs.

Expand passwordless access across devices and channels, support seamless self-service, and use identity signals to personalize access in real time.

Deliver fully passwordless and personalized access across all touchpoints using advanced capabilities like verifiable credentials, adaptive policies and real-time session control.

Note: This table is meant to convey the breadth of identity's reach. It is not a comprehensive representation of characteristics and behaviors that define each stage or the business outcomes.



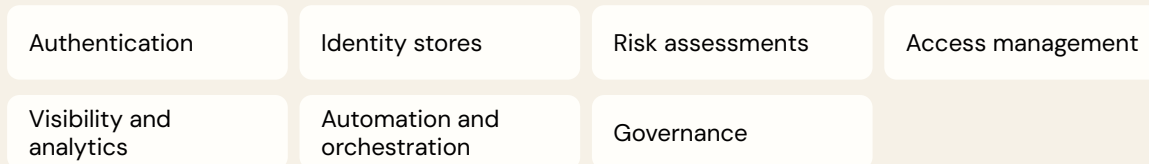
About this document

We created the Okta Identity Maturity Model to give organizations practical, value-based, and outcome-oriented guidance for building and improving their identity strategy.

This approach makes the IMM distinct from technology-based frameworks and maturity checklists, which tend to describe functions or prescribe technologies — but that omit detailed examination of value or outcomes.

Likewise, the fact that the IMM extends beyond security (and compliance) distinguishes it from these other resources.

Nevertheless, recognizing that security is often the key reason identity projects begin, this guide examines identity maturity through the familiar lens of the four identity functions and three cross-cutting capabilities within the popular CISA Zero Trust Maturity Model (ZTMM):



Along the way, we'll:



Provide insights and real-world context



Occasionally compare and contrast with the ZTMM



Suggest Okta solutions that can help your organization reach its identity maturity goals

Identity maturity and Zero Trust

Identity is the first of five key pillars within the [Zero Trust Maturity Model \(ZTMM\)](#) developed by the [Cybersecurity and Infrastructure Security Agency \(CISA\)](#).

The identity subsection of the model specifically notes that U.S. agencies should:

- Ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access.
- Integrate identity, credential, and access management solutions where possible throughout their enterprise to enforce strong authentication, grant tailored context-based authorization, and assess identity risk for agency users and entities.
- Integrate their identity stores and management systems, where appropriate, to enhance awareness of enterprise identities and their associated responsibilities and authorities.

While developed for U.S. agencies, the technology-based ZTMM is used by many private sector organizations. The CISA model complements the architectural guidance of the [NIST Zero Trust Architecture \(SP 800-207\)](#), which outlines principles like continuous verification and least privilege. However, the CISA' guide is more descriptive than prescriptive, leading countless Okta customers to ask us how to mature their identity practice in accordance with the CISA ZTMM.

For that reason, within this guide, we specifically reference particular aspects of the CISA ZTMM to illustrate the alignment between the Okta IMM and CISA's model.

[Learn more](#) about how the Okta Identity Maturity Model supports Zero Trust for regulated industries.



Authentication

Authentication confirms the identity of a user or entity requesting access to an application, service, or other resource, ensuring they are who they claim to be.

Threat actors commonly target authentication, using methods including:

- Brute force to try many credential combinations
- Social engineering to trick users into providing credentials
- Infostealers to steal credentials, cookies, and tokens
- SIM swapping and adversary-in-the-middle attacks to bypass susceptible forms of MFA

Authentication is clearly an important element of security, but it also influences user experiences and workforce productivity, with potentially significant consequences.

For example, the [Auth0 Customer Identity Trends Report 2025](#) revealed that nearly a quarter of users always (6%) or often (17%) abandon an online purchase due to issues with signup or login processes, and a further 40% report sometimes doing so. Likewise, a worker unable to access an application or information is unable to do their job.

A mature authentication function combines strong, phishing-resistant security (including incorporating risk signals) with ease of use. It makes it extremely difficult and costly for bad actors to gain access, while still providing convenient access to genuine users.

Moreover, a mature authentication function doesn't just assess risk once (i.e., when the user logs in), but does so continuously to guard against session hijacking and similar post-login threats.

Authorization

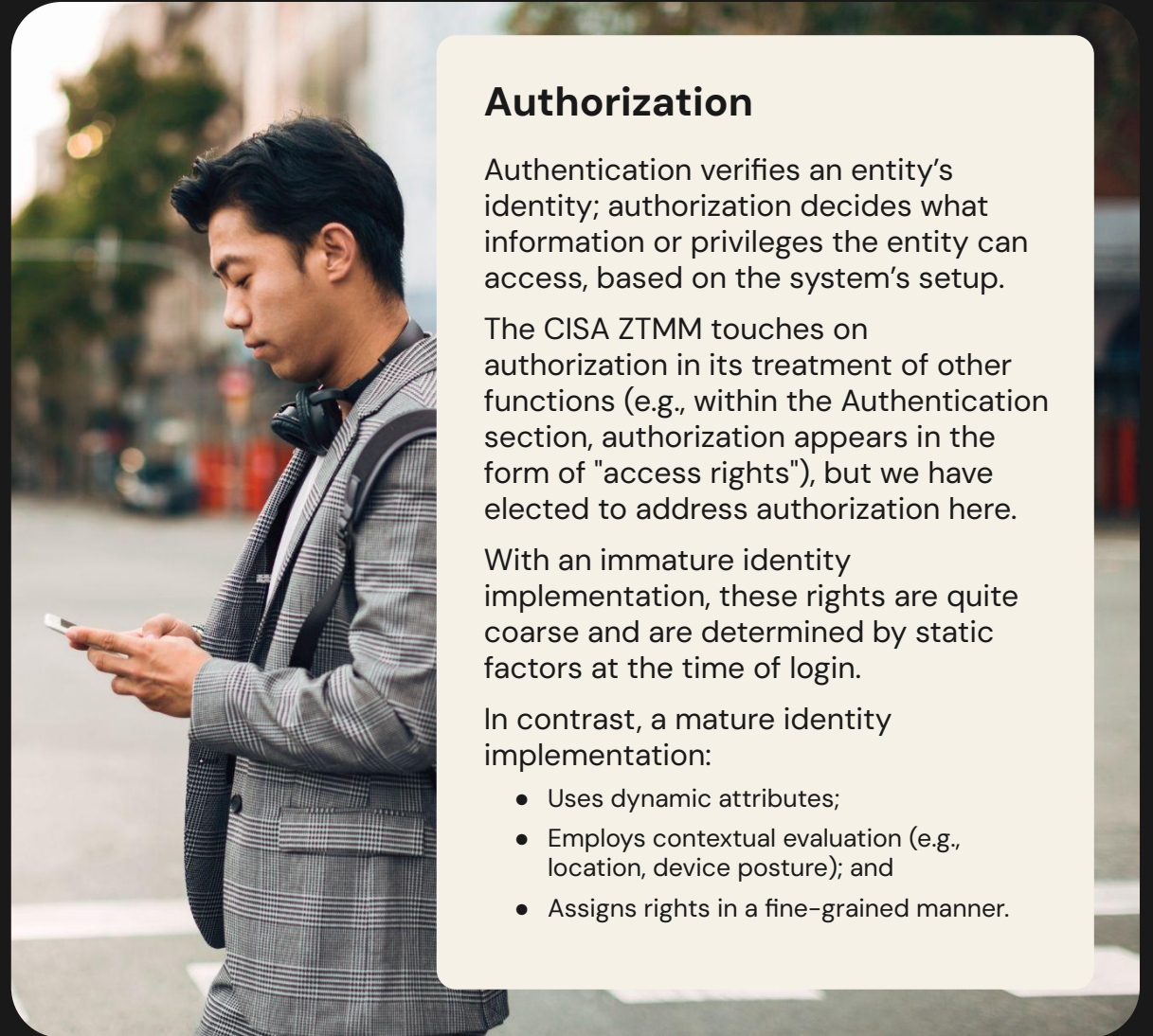
Authentication verifies an entity's identity; authorization decides what information or privileges the entity can access, based on the system's setup.

The CISA ZTMM touches on authorization in its treatment of other functions (e.g., within the Authentication section, authorization appears in the form of "access rights"), but we have elected to address authorization here.

With an immature identity implementation, these rights are quite coarse and are determined by static factors at the time of login.

In contrast, a mature identity implementation:

- Uses dynamic attributes;
- Employs contextual evaluation (e.g., location, device posture); and
- Assigns rights in a fine-grained manner.



Stage

Description

Supporting Okta Solutions



Fundamental

In this high-risk stage, authentication primarily relies on username and password pairs. There may be some use of MFA, but it isn't required for the entire workforce and may employ phishable techniques (e.g., SMS, email). Additionally, authorization is predefined and fixed, and does not take into account real-time or contextual conditions.

- [Multi-Factor Authentication](#)
- [Adaptive Multi-Factor Authentication](#)
- [Single Sign-On](#)
- [Universal Directory](#)



Scaling

The organization enforces MFA for all entities, with security strengthened by the introduction of possession and inherence factors that may be phishing-resistant. Coupled with single sign-on (SSO), authentication is now stronger and more convenient.

Simplified and centralized user stores enable more efficient and effective authorization management. Role- or attribute-based access controls (RBAC or ABAC) are in place, and incorporate dynamic factors that can be used to assess risk, such as entity location, local time, and device type.

- [Adaptive Multi-Factor Authentication](#)
- [Single Sign-On](#)
- [Universal Directory](#)
- [Fine-Grained Authorization](#)



Advanced

The organization starts to phase out passwords, one-time passwords/passcodes (OTPs), security questions, and push notifications.

Phishing-resistant MFA is scaled across the organization and includes implementations of passwordless MFA via FIDO2 or, where applicable, a secure government credential like Personal Identity Verification (PIV).

Relationship-based access control (ReBAC) enables precise and dynamic authorization. Access management and MFA are extended to how users log in via computers.

Authentication flows are decoupled for secure and passwordless initiation by trusted systems, like call centers, service kiosks, or AI-powered agents, eliminating the need for security questions, OTPs, or PINs.

- [Adaptive Multi-Factor Authentication](#)
- [Single Sign-On](#)
- [Universal Directory](#)
- [Identity Threat Protection](#)
- [Okta FastPass](#)
- [Fine-Grained Authorization](#)
- [Okta Device Access](#)
- [Client-Initiated Backchannel Authentication \(CIBA\)](#)



Strategic

All identity is validated with phishing-resistant and passwordless authentication. Access controls extend from device login to application sign-in for integrated security that also simplifies the user experience.

Access rights are now evaluated continuously, using dynamic variables, to enable detection of post-authentication threats.

Sensitive customer actions — like high-risk transactions or profile changes — are authenticated and protected through real-time confirmation mechanisms that add security without disrupting the journey.

Behind the scenes, customer communication channels and data exchanges are hardened to financial-grade standards, preventing tampering or interception throughout the end-to-end customer journey.

- [Adaptive Multi-Factor Authentication](#)
- [Single Sign-On](#)
- [Universal Directory](#)
- [Identity Threat Protection](#)
- [Okta FastPass](#)
- [Fine-Grained Authorization](#)
- [Okta Device Access](#)
- [Strong Customer Authentication](#)
- [Financial-Grade APIs \(FAPI\)](#)



Identity Stores

An identity store is a repository of user and entity data, such as names, roles, and attributes, used to enable authentication, certificate verification, and lifecycle management for the identities of employees, partners, contractors, customers, services, and other third parties. Identity stores now also encompass non-human identities (NHIs), such as service accounts, devices, bots, and AI agents.

Most organizations begin with a self-managed, on-premises identity store, only to quickly run into limitations related to scalability, visibility, and security.

As organizations grow or deploy more applications, it becomes difficult to maintain a single source of truth. Identities — both human and non-human — proliferate across disconnected systems, leading to “identity sprawl.” This condition complicates administration and makes it harder to enforce consistent policies, slowing operations and introducing security risks.

By consolidating and synchronizing identities, organizations can create a single source of truth, establishing a necessary foundation for fully automating secure access, reducing risk, and ensuring efficient lifecycle management.



Stage

Description

Supporting Okta Solutions



Fundamental

The organization uses only self-managed (e.g., planned, deployed, and maintained) identity stores like Active Directory or LDAP. These stores typically focus on human users, with NHIs like service accounts often unmanaged or tracked informally.

- [Single Sign-On](#)
- [Universal Directory](#)



Scaling

Organizations begin unifying identity stores — both self-managed and cloud-hosted — to reduce identity sprawl and associated risks, while applying consistent governance to both human and NHIs created through automation and infrastructure as code.

Additionally, organizations synchronize across directories, standardize lifecycle management practices, and begin formally tracking NHIs. These steps lay the groundwork for reducing duplication, thereby improving visibility and setting up automated workflows that scale.

- [Single Sign-On](#)
- [Universal Directory](#)
- [Lifecycle Management](#)
- [Workflows](#)



Advanced

Identity stores are consolidated, and governance policies are applied across human and non-human identities, reducing identity sprawl and contributing to more secure and efficient identity operations (e.g., SSO) and administration (e.g., provisioning, LCM).

Service accounts, APIs, and bots are onboarded and tracked more formally. Visibility improves, and identity lifecycle events become centralized.

- [Universal Directory](#)
- [Single Sign-On](#)
- [Lifecycle Management](#)
- [Workflows](#)
- [Okta Identity Governance](#)
- [Okta Privileged Access](#)



Strategic

Identity stores are unified across all environments, minimizing the number of identity stores in use and enabling automated LCM between them.

NHIs — now including emerging AI agents — are governed alongside human users. The organization enables adaptive policies, automated LCM, and posture management across a shared identity fabric.

- [Universal Directory](#)
- [Single Sign-On](#)
- [Lifecycle Management](#)
- [Workflows](#)
- [Okta Identity Governance](#)
- [Okta Privileged Access](#)
- [Identity Security Posture Management](#)



Risk Assessments

Okta takes a broad view of identity risk, defining it as “any vulnerability in an organization’s Identity and Access Management processes.”

This expansive definition includes both the risk attached to individual identities and those associated with:

- Weak IAM hygiene (e.g., orphaned accounts, overprovisioning)
- Misconfigurations resulting in security gaps
- The use of outdated technologies.

As organizations mature towards the Strategic stage, they must prioritize capabilities that harden their security posture and dynamically reduce identity risk by ingesting and analyzing security signals across the environment, including identity, endpoint, network, and device posture.

These real-time signals help inform adaptive policies and enable organizations to proactively reduce the identity attack surface and improve security through:

- **Detection:** Uncovering hidden threats and misconfigurations across identity providers, SaaS, and cloud infrastructure (IaaS).
- **Prioritization:** Discovering and prioritizing vulnerabilities like MFA bypass, overprovisioned users, and improper offboarding.
- **Remediation:** Gaining actionable security insights to drive quick remediation.
- **Continuous Monitoring:** Receiving ongoing, continuous analysis of the organization's identity security exposure with rapid deployments, and enabling risk-based monitoring against security, IAM, and compliance standards (e.g. NIST, CIS, ISO, SOX, and PCI-DSS).



Identity risk

The CISA ZTMM definition of *identity risk* is limited to the “likelihood that an identity is compromised”, which is narrower than Okta’s definition.¹

Consequently, the model focuses on helping organizations quickly and accurately detect compromised identities. For example, it detects anomalous behavior—such as a service account accessing sensitive resources it has never interacted with before—and flags it for further investigation.

While the CISA ZTMM doesn’t explicitly link the risk assessment and authentication function, they are closely connected, and Okta helps bridge that gap. For instance:





- If a process assesses with high probability that an identity has been compromised, that entity may be denied authentication.
- If an entity’s behavior during authentication is suspicious, observing this could feed into risk assessments.

Okta expands on this relationship by continuously assessing risk throughout the identity lifecycle, not just during login, by monitoring real-time behavioral and contextual signals from other threat surfaces enabling swift responses, such as policy-based session termination/logout or adaptive step-up authentication, helping contain threats as they emerge.



[1] CISA. Zero Trust Maturity Model, Version 2.0. April 2023, p. 14. Retrieved June 9, 2025, from https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

These capabilities overlap with the CISA ZTMM's Access Management function and three cross-cutting capabilities (Visibility and Analytics, Automation and Orchestration, and Governance).

Stage	Description	Supporting Okta Solutions
 Fundamental	Organizations in this stage have a very limited ability to assess and incorporate identity risk into access policies. Any assessment that does exist is likely based upon static attributes, and associated policies are simplistic (e.g., binary).	<ul style="list-style-type: none">• Multi-Factor Authentication• Adaptive Multi-Factor Authentication
 Scaling	Policies are slightly richer, with assessments that can incorporate authentication telemetry at login. Nevertheless, assessments remain comparatively basic and vulnerable to identity attacks due in part to continued reliance on manual methods and static rules.	<ul style="list-style-type: none">• Adaptive Multi-Factor Authentication
 Advanced	Assessments leverage automation and dynamic rules, making use of a multitude of authentication signals (perhaps including those from device assurance and management solutions) when making access decisions. However, assessments are still predominantly performed only at login, and are not revisited during the lifetime of a user's session.	<ul style="list-style-type: none">• Adaptive Multi-Factor Authentication• Identity Threat Protection• Identity Security Posture Management
 Strategic	Risk assessments are performed continuously, in real time, and leverage dynamic context and a rich array of signals from identity infrastructure and ancillary security and IT systems. Identity Threat Protection with Okta AI Moreover, automation and integration enable appropriate responses and policy enforcement, including immediate secure logout and the activation of security or IT operations workflows to protect the organization and compromised users.	<ul style="list-style-type: none">• Adaptive Multi-Factor Authentication• Identity Threat Protection• Identity Security Posture Management• Workflows

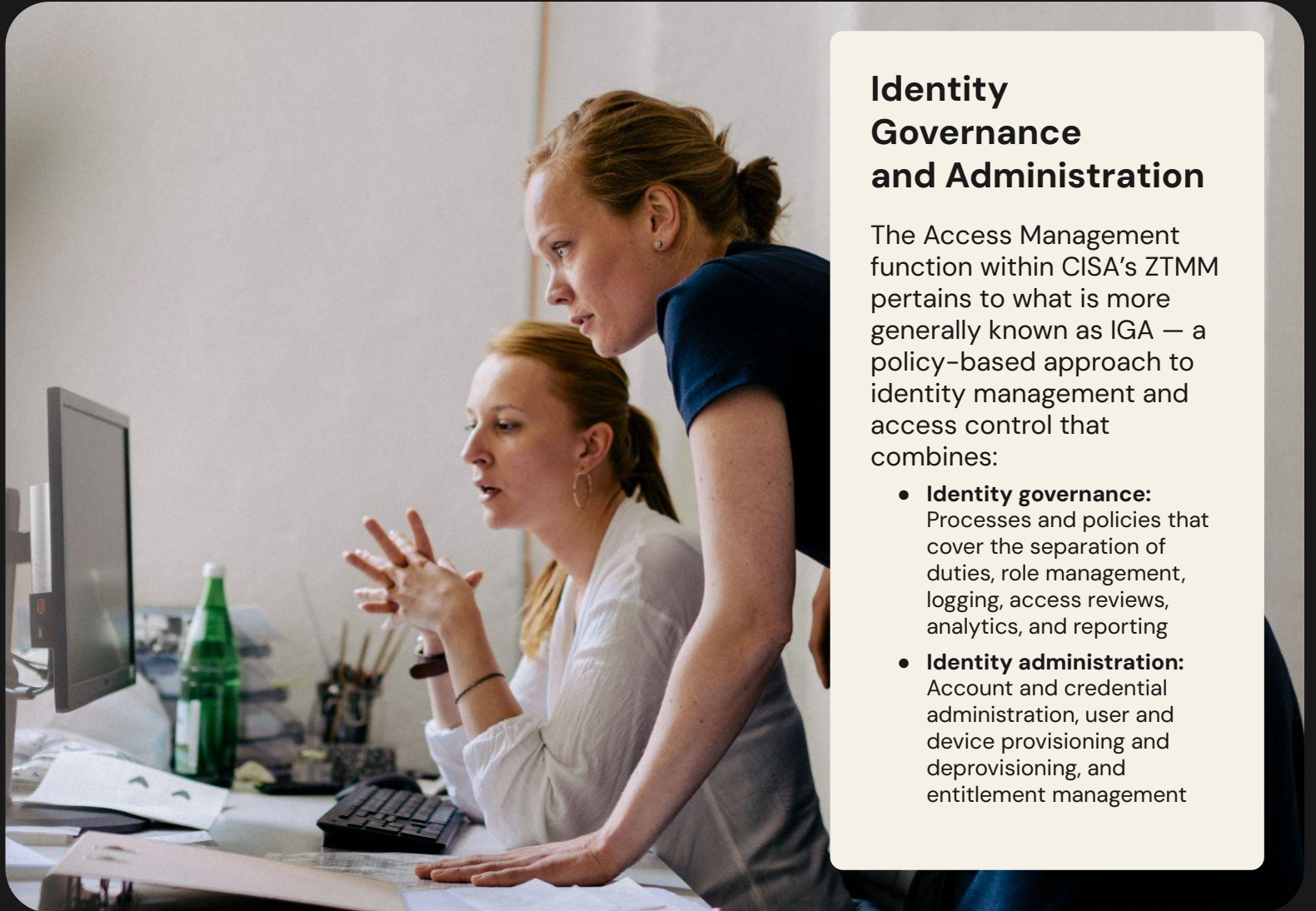


Access Management

In accordance with the Identity Governance and Administration (IGA)-focused meaning of Access Management within the CISA ZTMM, the four stages describe implementation and process maturity, rather than addressing technical solutions. Nevertheless, an organization's ability to implement IGA policies requires that certain capabilities be in place.

Broadly speaking, an immature organization will have manual access review processes, very long-lasting access privileges, and very coarse authorization. This combination typically results in vastly overprovisioned access and toxic combinations (e.g., a single user can both request and approve a privilege escalation), providing ample opportunity for abuse. Moreover, it simply doesn't scale.

In contrast, a mature organization makes maximum use of automation, grants access only when needed, with zero standing privileges, and grants access in an extremely precise manner in accordance with the principle of least-privilege access.



Identity Governance and Administration

The Access Management function within CISA's ZTMM pertains to what is more generally known as IGA — a policy-based approach to identity management and access control that combines:

- **Identity governance:** Processes and policies that cover the separation of duties, role management, logging, access reviews, analytics, and reporting
- **Identity administration:** Account and credential administration, user and device provisioning and deprovisioning, and entitlement management



Stage

Description

Supporting Okta Solutions



Fundamental

In this stage, which is likely more common for smaller organizations, access for both privileged and standard accounts is authorized on a permanent basis, subject only to periodic review. Access is not contextual, enforcement is limited, and access is likely tracked manually (e.g., in a spreadsheet).

- [Okta Identity Governance](#)
- [Identity Security Posture Management](#)



Scaling

Access for privileged and standard accounts is tracked via automated review. The main difference in the Scaling stage is that access expires with automated review, unless otherwise extended. The information used to make access decisions remains limited, perhaps based upon role rather than needs or past access logs, which can result in long-standing access. Entities may also become overprivileged due to limited granularity of access control.

- [Okta Identity Governance](#)
- [Identity Security Posture Management](#)
- [Okta Privileged Access](#)
- [Fine-Grained Authorization](#)



Advanced

Access is managed on a need- and session- basis, tailored to actions and resources, and revoked automatically — applying principles of least privilege with time-bound and just-in-time (JIT) passwordless access, especially for critical infrastructure like servers. This also extends to how access is managed for device login, which is risk-based and policy-driven. Enforcement incorporates granular conditions based on device posture, network, and behavioral risk signals.

- [Okta Identity Governance](#)
- [Identity Security Posture Management](#)
- [Okta Privileged Access](#)
- [Fine-Grained Authorization](#)
- [Workflows](#)
- [Okta Device Access](#)



Strategic

Least privilege and JIT access authorization policies are now automated, tailoring access to individual actions and resource needs — resulting in zero standing privileges. Access enforcement is fully adaptive, responding to real-time signals across the tech stack. Authentication and session decisions are based on continuous evaluation. Risk-based step-up authentication and other actions are automated and operate in real-time, enhancing user experiences while maintaining security posture.

- [Okta Identity Governance](#)
- [Identity Security Posture Management](#)
- [Okta Privileged Access](#)
- [Fine-Grained Authorization](#)
- [Workflows](#)
- [Okta Device Access](#)



Visibility and Analytics

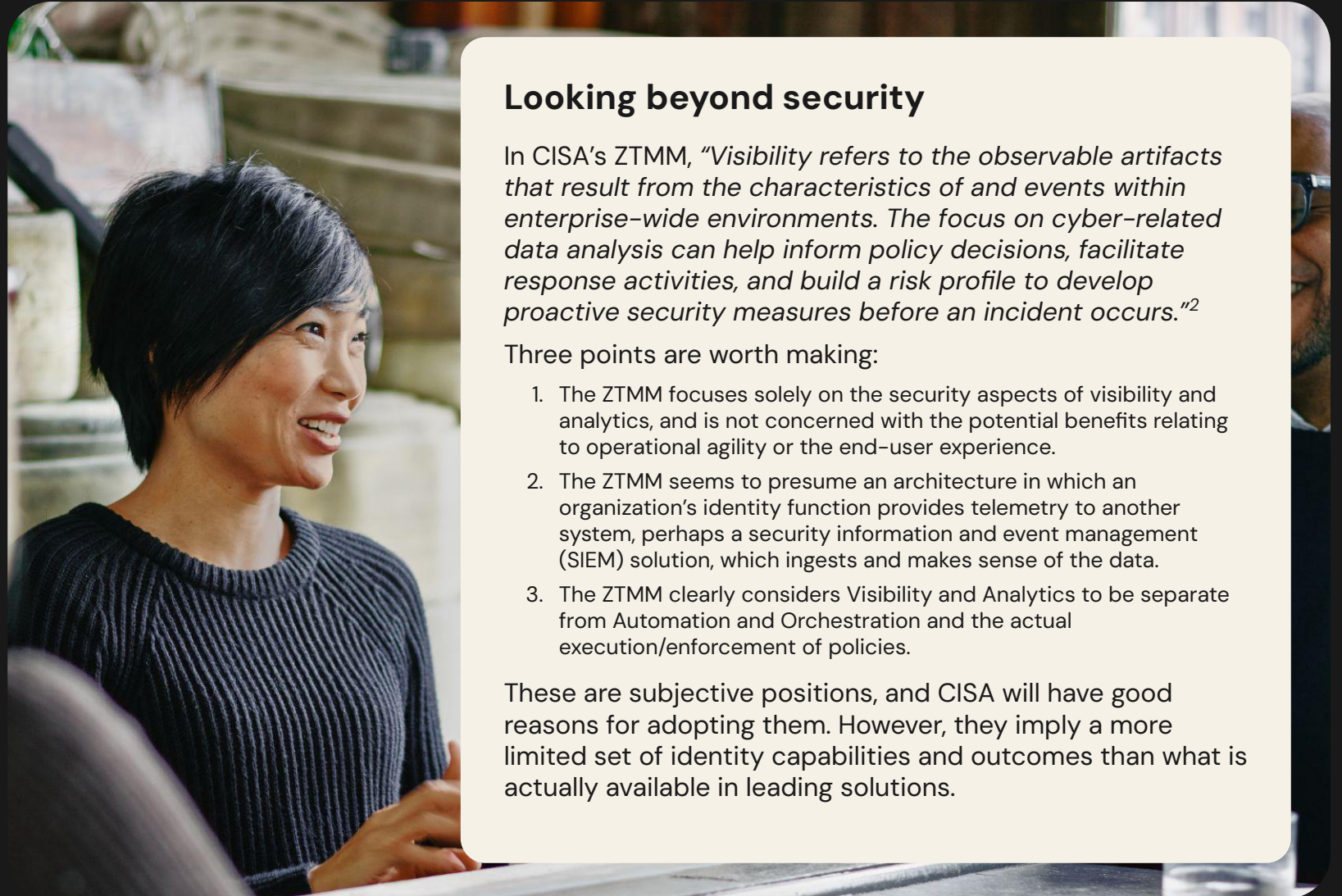
The more an organization understands how entities use identity systems, the more they can:

- Improve operational agility (e.g., by automating workflows)
- Optimize user experiences (e.g., by refining access management policies)
- Strengthen security (e.g., by implementing prevention, detection, and response capabilities)

Some identity solutions can detect risks in real time, often faster and more accurately than general security tools, without needing to send data to a SIEM. Importantly, local analysis can complement external systems.

Certain identity solutions also directly enforce policies in response to threats such as preventing authentication or logging out compromised users. With real-time detection offered by the same solution, this tight coupling mitigates threats quickly, strengthening the organization's security posture.

The outcomes achieved, however, will vary depending on the identity platform and its telemetry capabilities



Looking beyond security

In CISA's ZTMM, *"Visibility refers to the observable artifacts that result from the characteristics of and events within enterprise-wide environments. The focus on cyber-related data analysis can help inform policy decisions, facilitate response activities, and build a risk profile to develop proactive security measures before an incident occurs."*²

Three points are worth making:

1. The ZTMM focuses solely on the security aspects of visibility and analytics, and is not concerned with the potential benefits relating to operational agility or the end-user experience.
2. The ZTMM seems to presume an architecture in which an organization's identity function provides telemetry to another system, perhaps a security information and event management (SIEM) solution, which ingests and makes sense of the data.
3. The ZTMM clearly considers Visibility and Analytics to be separate from Automation and Orchestration and the actual execution/enforcement of policies.

These are subjective positions, and CISA will have good reasons for adopting them. However, they imply a more limited set of identity capabilities and outcomes than what is actually available in leading solutions.



Stage

Description

Supporting Okta Solutions



Fundamental

At this point, the organization collects identity activity logs, with special attention paid to privileged credentials. While log analysis may be performed as a matter of routine, it is done manually. As a result, such analysis is comparatively unable to identify risks in a timely manner, or to identify advanced threats.

- [Universal Directory](#)



Scaling

In addition to manual log analysis, the organization now has some automated analysis. However, while the automated analysis improves the organization's ability to detect threats in a timely manner, limited correlation between log types still hampers detection of advanced threats.

- [Universal Directory](#)
- [Workflows](#)



Advanced

Analysis is now entirely automated (or almost so), with correlation between log types, although not all user and entity log types are included. Identity logs are also linked with other sources, closing visibility gaps and providing more holistic threat detection capabilities.

- [Universal Directory](#)
- [Workflows](#)
- [Identity Threat Protection](#)



Strategic

The organization achieves and maintains comprehensive visibility through automated analysis of all user and entity log types, linked with other sources.

- [Universal Directory](#)
- [Workflows](#)
- [Identity Threat Protection](#)

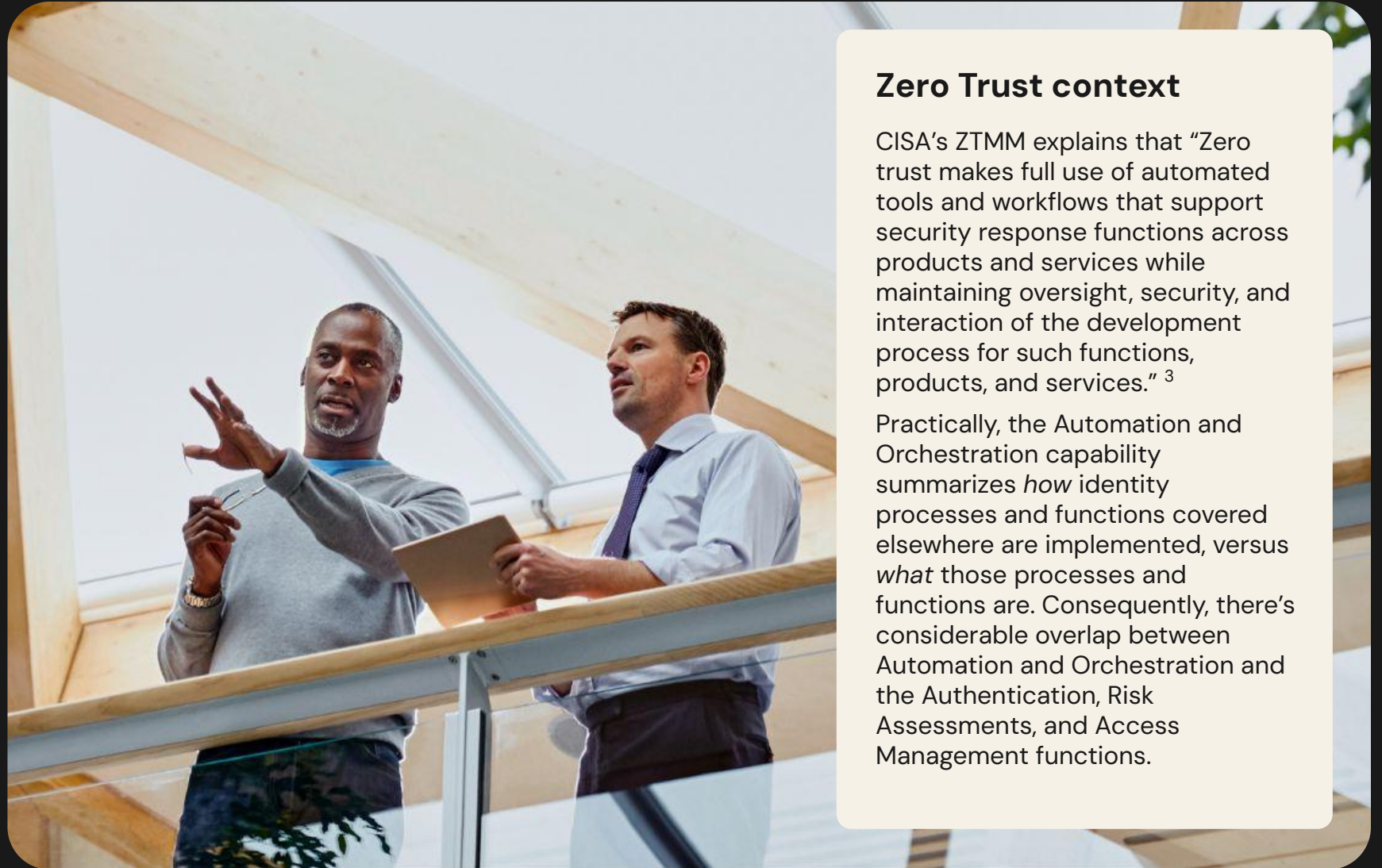


Automation and Orchestration

The degree to which an organization can mature its identity automation and orchestration capabilities is hugely dependent upon the identity platforms and products it deploys.

The most powerful identity solutions will not only support automation and orchestration by integrating with the wider technology stack, but will also contain such capabilities within themselves.

These embedded capabilities allow the organization to create workflows to manage identity lifecycles, including joiner, mover, and leaver (JML) processes, to support strong governance, to carefully control privileged access, to enhance security posture, and so on, without requiring a generalized automation and orchestration tool.



Zero Trust context

CISA's ZTMM explains that "Zero trust makes full use of automated tools and workflows that support security response functions across products and services while maintaining oversight, security, and interaction of the development process for such functions, products, and services." ³

Practically, the Automation and Orchestration capability summarizes *how* identity processes and functions covered elsewhere are implemented, versus *what* those processes and functions are. Consequently, there's considerable overlap between Automation and Orchestration and the Authentication, Risk Assessments, and Access Management functions.



Stage

Description

Supporting Okta Solutions



Fundamental

In this stage, the organization works almost entirely with self-managed identities and manually executes lifecycle management processes, including onboarding and offboarding, doing so mainly via email, collaboration apps, service desk tickets, and similar utilities.

There is little integration between different systems, and reviews (e.g., for access privileges) are performed manually at some predetermined cadence.

- [Lifecycle Management](#)
- [Workflows](#)



Scaling

In this stage, the organization begins to implement some automation to orchestrate processes around non-privileged users and self-managed identities. User provisioning and deprovisioning are increasingly handled through automation.

The organization still orchestrates privileged identities manually, but now also manages external identities.

- [Lifecycle Management](#)
- [Workflows](#)
- [Okta Identity Governance](#)
- [Okta Privileged Access](#)



Advanced

In this stage, the organization has sufficient integration across all environments to enable automation and orchestration for internal and external identities. Privileged identities are still orchestrated manually.

Identity risk detection and remediation are automated, with capabilities to proactively identify and address potential threats.

- [Lifecycle Management](#)
- [Workflows](#)
- [Okta Identity Governance](#)
- [Okta Privileged Access](#)



Strategic

In the Strategic stage, all identity orchestration processes are automated, span all identities and environments, and are based on behaviors, enrollments, and deployment needs.

The organization has the flexibility to automate remediation responses by triggering downstream processes, tailored to their specific needs once risks are detected.

- [Lifecycle Management](#)
- [Workflows](#)
- [Okta Identity Governance](#)
- [Okta Privileged Access](#)



Governance

Identity governance refers to the definition and associated enforcement of an organization's policies, procedures, and processes, in support of its goals (e.g., implementing Zero Trust principles, improving efficiency, enhancing productivity) and compliance with regulations, frameworks, standards, and contractual obligations.

Maturity in the context of governance focuses on swapping siloed and manual approaches for holistic and automated ones. This includes unifying policies across both human and non-human identities (NHIs), applying role- and risk-based access controls, and scaling lifecycle and certification processes.

As organizations mature, governance expands from ad hoc controls to continuous, intelligent automation that applies equally to APIs, service accounts, and robotic processes. NHIs become first-class citizens in governance, subject to least privilege, access reviews, and compliance oversight at each stage of the identity lifecycle.



Stage

Description

Supporting Okta Solutions



Fundamental

Very little identity governance is in place, and any existing programs tend to be siloed (rather than aligned around shared business and governance goals) or standalone, focused only on human identities. There is no central oversight of NHIs, which often proliferate unchecked, increasing risk.

- [Lifecycle Management](#)
- [Workflows](#)



Scaling

The organization has simplified some aspects of governance and compliance by automating access reviews and access request flows.

Governance becomes more structured through role-based models. Provisioning and deprovisioning are automated based on lifecycle events, and access certifications are scheduled periodically.

Early-stage controls for NHIs may be introduced, typically via basic lifecycle automation for service accounts and bots.

- [Lifecycle Management](#)
- [Workflows](#)
- [Okta Identity Governance](#)
- [Okta Privileged Access](#)



Advanced

The organization has enforced governance and operational practices to ensure identity continually evolves to meet business needs and deliver value.

Access is governed by dynamic, policy-based controls that account for user attributes, risk levels, and business rules. Just-in-time and time-bound access is implemented. High-risk requests trigger human-in-the-loop approvals, and separation of duties is enforced to prevent conflicting access.

Governance over NHIs is introduced systematically, applying least privilege, reviews, and lifecycle controls similar to those applied to human users.

- [Lifecycle Management](#)
- [Workflows](#)
- [Okta Identity Governance](#)
- [Okta Privileged Access](#)



Strategic

The organization leverages AI to enable stronger identity security and governance, better user experiences, and easier configuration and development.

Governance is continuous and proactive. Access decisions are autonomous and risk-aware, driven by predictive analytics and unified policies across cloud, hybrid, and on-prem environments.

Certifications shift from periodic to event-driven, with NHIs fully integrated into adaptive governance processes.

Human-in-the-loop oversight is applied only to high-risk scenarios, ensuring adaptive governance that balances automation with intelligent intervention. Autonomous governance of NHIs — complete with risk scoring, access automation, and intelligent remediation — becomes a core capability.

- [Lifecycle Management](#)
- [Workflows](#)
- [Okta Identity Governance](#)
- [Okta Privileged Access](#)



Conclusion

While every organization's identity journey is unique — one of those clichés firmly rooted in truth — there are nevertheless recurring patterns.

By prioritizing identity maturity, an organization can benefit from a strengthened security posture, a more productive workforce, improved operational efficiencies, and continued business growth.

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements. © Okta and/or its affiliates. All rights reserved.

