How Okta's Identity Maturity Model supports higher education

A guide for navigating identity-related policies through the lens of three categories: operational agility, end-user experience, and security and compliance.

Introduction

The frameworks mapped in this guidebook serve as a blueprint for those operating in highly regulated industries looking to modernize their IT infrastructure and ensure secure, efficient access to multi-cloud services. At minimum, each framework's core principles emphasizes why adopting a risk-based approach to strong authentication, granular access controls, and continuous monitoring aligns with the broader push for Zero Trust security. The guidebook also references the Okta Identity Maturity Model as a base model.

In each section you'll find:

- Alignment to key stakeholders
- Metrics for evaluating identity success
- Potential savings with Okta

To keep up to date with launch milestones please reference the Okta US Public Sector resource page.

Links

Higher Education - NIST CSF 2.0

Okta on Okta examples

okta

Higher Education - NIST CSF 2.0

Higher education institutions align with the NIST Cybersecurity Framework (CSF) for foundational identity services, managing cybersecurity risks to identities, access, and data. They uniquely grapple with diverse user populations, enabling collaboration, securing research data and ensuring student privacy (e.g., FERPA). Modern IAM provides a secure, flexible foundation for their core activities and digital transformation.

View the framework →

Potential Savings with Okta

- Lowers costs associated with manual account management and custom integration development.
- Reduces administrative burden through automated lifecycle workflows.
- Optimizes resource allocation by consolidating identity infrastructure.
- Minimizes delays and associated productivity loss during onboarding/offboarding peaks.

okta

Higher Education - NIST CSF 2.0

	Description: Ability to	Stakeholder Support	Metrics for Evaluating Identity Success
Operational Agility	Manage complex and dynamic user lifecycles (students, faculty, staff, alumni, affiliates, researchers) efficiently; integrate diverse campus applications (LMS, SIS, HR, research platforms); support inter-institutional collaboration and federation (e.g., InCommon); adapt to evolving remote/hybrid learning models.	Provosts, Deans, IT Leadership (CIO/CISO), Research Administration, and Registrars Office collaborate to define identity needs across teaching, research, and administration, leveraging Okta for automation, integration, and streamlined lifecycle management across diverse user populations and affiliations.	• Reduced time/effort for user provisioning/deprovisioning during peak periods (start/end of term) (Okta Lifecycle Management, Workflows). • Faster integration of new academic/research applications (Okta Integration Network, APIs/SDKs). • Decreased IT overhead managing multiple identity silos (Okta Universal Directory). • Improved efficiency in managing affiliate/researcher access (Okta Lifecycle Management, Delegated Admin).
End-user Experience	Provide a consistent, secure, and user-friendly login experience across campus resources (web portals, applications, Wi-Fi via eduroam); enable self-service for password resets and profile updates; support multiple user affiliations (e.g., student also being an employee) seamlessly.	Campus IT, Student Affairs, Faculty Support Services, and Communication teams work together using Okta to provide intuitive self-service tools, unified login (SSO), and reliable access appropriate to user roles and affiliations, minimizing friction for students, faculty, and staff.	• Improved user satisfaction (students, faculty, staff) with access processes (Okta SSO, MFA Self-Service). • Reduction in help desk calls related to password resets and access issues (Okta Self-Service Password Reset, MFA). • Increased adoption/usage of campus digital services due to simplified access (Okta SSO, Universal Directory for profile mastering). • Reduced time spent by users managing multiple credentials or dealing with login issues (Okta FastPass, Passwordless).
Security & Compliance	Protect sensitive student data (FERPA), research data (NIST SP 800-171/CMMC), and institutional assets; enforce strong authentication and authorization policies; implement least privilege access; manage risk associated with third-party collaborators; support audit and reporting requirements.	CISOs, Compliance Officers, Research Integrity Officers, and Internal Audit teams leverage Okta's security features (MFA, Adaptive Policies, ThreatInsight), governance capabilities (Okta Identity Governance), and audit logs to enforce security policies, meet compliance mandates (FERPA, NIST), mitigate risks, and streamline audits.	• Reduction in identity-related security incidents (e.g., account compromise, unauthorized access) (Okta MFA, Adaptive MFA, Identity Threat Protection). • Demonstrated compliance with FERPA, NIST SP 800-171 controls related to identification, authentication, and access control. • Increased adoption of MFA across all user populations. • Effective enforcement of least privilege access through regular reviews and automated controls (Okta Identity Governance). • Reduced time and effort for audit preparation and response (Okta Reports, Audit Logs).

Higher Education - NIST CSF 2.0

	Description	Benefits to NIST CSF 2.0
Workflows & Lifecycle Management	Automates joiner, mover, leaver processes essential for managing high-volume, time-sensitive student/staff turnover. Enables no-code automation for tasks like role changes, group memberships, and access provisioning/deprovisioning based on SIS/HR triggers. Addresses EDUCAUSE emphasis on automation and efficiency.	• Automates aspects of **GV.RR (Roles, Responsibilities, and Authorities)** by ensuring access assignments align with predefined roles from authoritative systems. • Manages **PR.AA-01 & PR.AA-05 (Identity Management & Access Control)** by automating the identity lifecycle (creation to deletion) and enforcing least privilege access. • Facilitates **RS.MA (Mitigation)** by enabling the rapid disabling of user accounts or immediate revocation of access privileges in response to security incidents
Universal Directory	Centralizes identity data for diverse populations (students, faculty, staff, alumni, affiliates) from various sources (SIS, HR, AD). Provides a flexible profile and supports managing complex affiliations and attributes needed in higher education.	• Supports **GV.RM (Risk Management Strategy)** by providing a clear view of identities, aiding in understanding identity-related risks. • Fulfills **ID.AM (Asset Management)** by serving as a central inventory for user identities and their associated attributes **(ID.AM-01).** • Underpins **PR.AA-01 (Identity Management**) by providing a centralized platform to manage all user identities throughout their lifecycle.
Single Sign-On & MFA	Provides secure, seamless access to campus applications, cloud services, and federated resources (e.g, via InCommon). Enforces strong, adaptive authentication (including phishing-resistant options) critical for protecting diverse users and meeting NIST guidelines.	• Enhances **PR.AA-03 (Authentication)** by providing robust primary authentication (SSO) layered with strong, adaptive, and phishing-resistant multi-factor verification (AMFA). • Enforces **GV.PO (Policy)** through AMFA's capability for central definition and consistent application of risk-based access policies across the institution. • Improves security posture and user adoption under **PR.AT (Awareness and Training)** through a combination of user-friendly SSO and convenient, context-aware AMFA prompting.
Identity Governance	Enables automated access requests, certifications/reviews, and reporting. Crucial for enforcing least privilege, managing entitlements across complex roles/affiliations, and demonstrating compliance with FERPA and NIST SP 800-171 access control requirements.	• Aligns with NIST CSF **Govern (GV.PO)** function and **Protect (PR.AC)** access control families. • Provides mechanisms for regular access reviews needed for FERPA and sensitive data protection. • Helps enforce least privilege in complex higher education environments with many roles/systems. • Delivers audit trails essential for compliance reporting.

Leading by Example

As part of our Okta Secure Identity Commitment, we believe in leading by example. That means using our own identity platform to protect our workforce, validate our product innovations, and demonstrate best-in-class identity practices.

"Okta on Okta" isn't just dogfooding- it's how we pressure test our capabilities at scale, uncover insights for product improvement, and build trust with customers who rely on us to secure their most critical assets.

Identity Verification

Okta customized our Identity verification process to include country verification to ensure legal alignment to relevant restrictions, limiting the access of Okta's products in jurisdictions where US import controls or economic sanctions laws are in effect.

Learn more →

Identity Governance

Okta Identity Governance was deployed across ~75 non-SOX and 2 SOX applications—including Okta itself and its Support User instance—to strengthen access controls, improve audit readiness, and ensure the right people have the right access at the right time.

Learn more →

Device Access

Okta Device Access (ODA) is used internally to deliver secure but user-friendly access controls at device login touchpoints, enabling consistent security policies at all authentication moments from devices to applications.

Learn more →

Identity Security Posture Management

Okta's Identity Security Posture Management, now generally available, has strengthened Okta's own least privileged & Zero Trust approach to security through continuous internal monitoring and validation of our identity security posture.

Learn more →

Partner Integrations

Okta extends its value through integrations with key security partners. For example, Okta integrates with Yubico for phishing-resistant MFA, Persona for enhanced Identity verification, Jamf for device trust, and CrowdStrike + Palo Alto for threat signal correlation. CallerVerify adds another layer of voice-based authentication for high-risk actions.

Learn more →

okta