RISE 2030

Identity First

The Roadmap to Modern Security & Access at FSU

Presented by Jose Rodriguez and Martin Schaefer

80% of all Cyber Attacks Involve Compromised Digital Identities

2025 Crowdstrike Global Threat Report:

- 79% of cyberattack detections were malware-free.
  - This signals tactics like credential abuse and hands-on-keyboard attacks.
- Identity based intrusions consisted of 35% of cloud incidents.
  - Facilitated by access broker markets which grew 50% year-over-year.
- Iran Hacks Stryker in Michigan (March 11, 2026)
  - Admin Identity was hacked
  - Over 200,000 devices remotely wiped
    - Laptops, servers, and smart phones

RISE 2030

Your FSU Digital Identity

Consists of information like:

- SSN
- Home address
- Bank information
- Personal Information

May have access to:

- Administrative/Financial Systems
- Confidential Data

It represents who you are online to other institutions

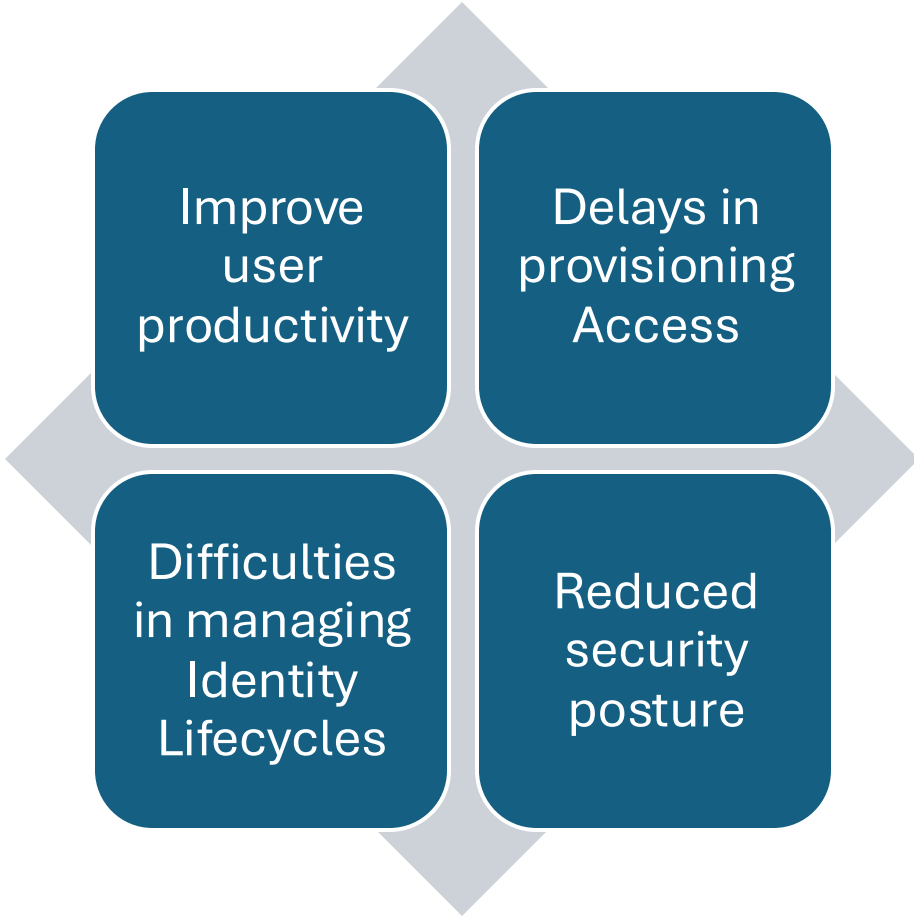
- It determines your reputation

A breach of identity also puts the University's finances and reputation at risk.

RISE 2030

IAM Modernization Project

Project Drivers



Conducted an Identity Assessment (KeyData)

- We engaged within ITS and with our Campus Partners
  - We conducted over 100 workshops
    - Architecture
    - Challenges
  - We engaged with 39 unique groups at FSU

RISE 2030

Participating Partners

- Admissions
- Athletics
- Business Services
- Campus Recreation
- Career Center
- Center for Global Engagement
- Chief Auditor
- College of Arts and Sciences
- College of Medicine
- College of Nursing
- Compliance and Risk
- FAMU/FSU College of Engineering
- Florida High (High schools)
- Foundation
- FSU Controller's Office
- FSU Health
- Human Resources
- General Counsel
- Graduate School
- Housing
- Institutional Research
- Information and Security Policy Office
- ITAPP/CEHHS
- ITAPP/Facilities
- ITAPP/International Programs
- ITAPP/Law
- ITAPP/Panama City/ PC School
- Information Technology Services
- Mag Lab
- Office of Compliance and Ethics
- Office of Research
- Police Department / Ccure
- RAMP / Research
- Registrar Research Development
- Ringling
- Student Affairs
- Undergraduate Studies
- University Centers and Institutes
- University Health Services

Identity Assessment Findings (KeyData)

- Lack of Business-Driven Roles and Central Governance
- Manual Provisioning Processes
  - Access is given after someone has access to their account
- Decentralized Identity Management
  - Residual Access for Separated Employees
- Inefficient Access Certification/Recertification

RISE 2030

IAM vs IGA

What is the difference?

Identity and Access Management (IAM)

- Focused on Real-time Access
- Logging In (Authentication)
- Granting Access (Authorization)

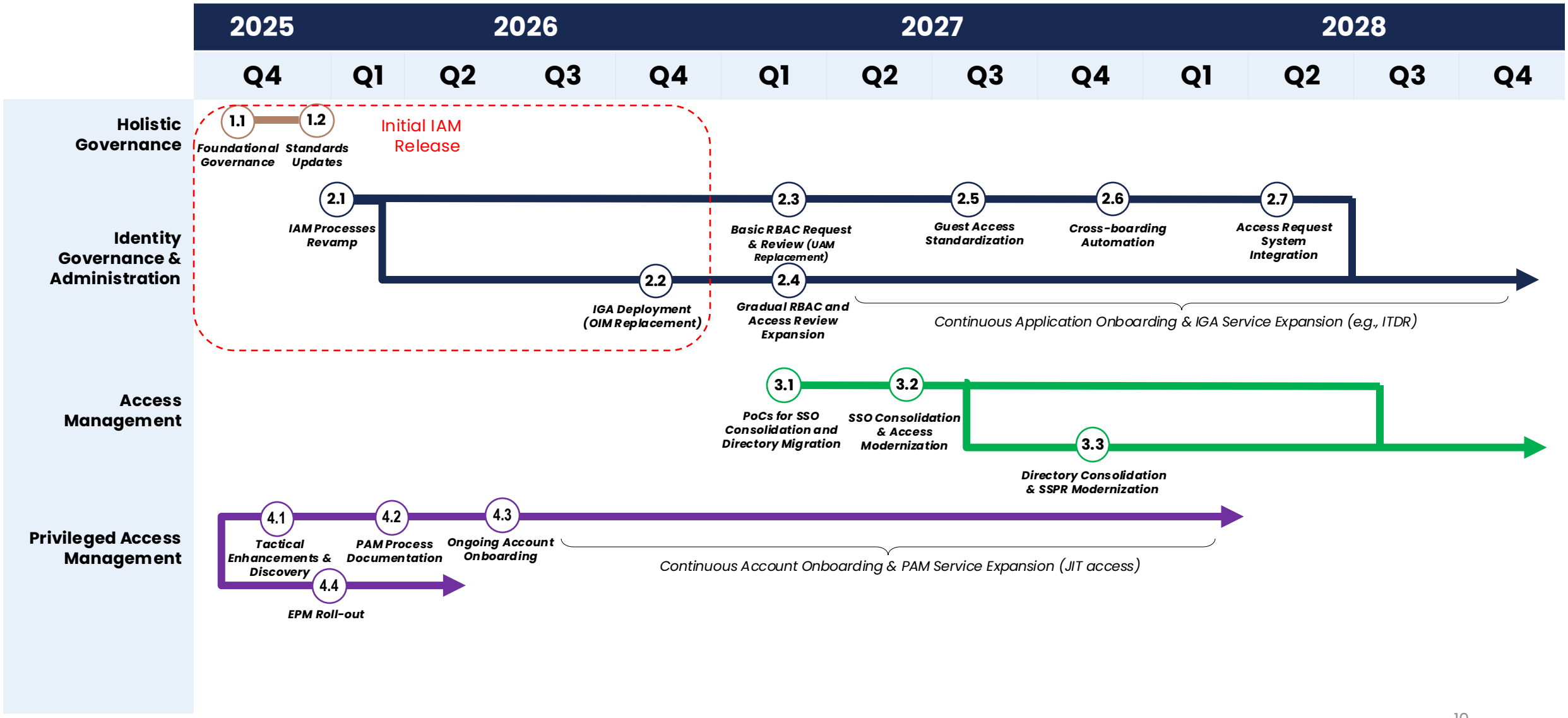
Identity Governance and Administration (IGA)

- Focused on Governance
- Central User Management
- Policies
- Compliance & Audits

Identity Assessment Recommendations (KeyData)

- Implement a Modern Identity Governance & Administration (IGA) Solution
  - Central Identity Warehouse –Gives visibility over all identities
  - Enables centralized role management
  - Allows automating on-boarding, off-boarding, and cross-boarding based on source triggers.
  - Automated access reviews
  - Single pane of glass for metrics, KPIs, and KRIs around identity
  - Centralized audit trail for all user
- KeyData helped us develop an Identity Road Map

RISE 2030


2025
2026
2027
2028
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Holistic Governance
Identity Governance & Administration
Access Management
Privileged Access Management
1.1
Foundational Governance
1.2
Standards Updates
Initial IAM Release
2.1
IAM Processes Revamp
2.2
IGA Deployment (OIM Replacement)
2.3
Basic RBAC Request & Review (UAM Replacement)
2.4
Gradual RBAC and Access Review Expansion
2.5
Guest Access Standardization
2.6
Cross-boarding Automation
2.7
Access Request System Integration
Continuous Application Onboarding & IGA Service Expansion (e.g., ITDR)
3.1
PoCs for SSO Consolidation and Directory Migration
3.2
SSO Consolidation & Access Modernization
3.3
Directory Consolidation & SSPR Modernization
4.1
Tactical Enhancements & Discovery
4.2
PAM Process Documentation
4.3
Ongoing Account Onboarding
4.4
EPM Roll-out
Continuous Account Onboarding & PAM Service Expansion (JIT access)

RISE 2030

IGA Implementation

Road Map

RISE 2030

We Purchased an IGA Solution

CDW

- Our Contract is through CDW
- Established relationship with FSU
- CDW will perform project management and business analyst role

Fischer Identity

- 20+ Years of IAM Expertise with Higher Ed
- First IGA provider in the cloud(2006)
- 80% of their customers are in higher education
- 97% Customer Retention Rate
- Offered the best prices and the most complete package
- They had some of the best customer referrals.

CDW | Education

FISCHER IDENTITY

RISE 2030

IGA Sets the Foundation

- **Sets the Foundation for FSU's Identity Management Roadmap**
  - Provides the strategic control to simplify our environment and deliver on future roadmap goals.
- **Establishes a Unified Identity Fabric**
  - Delivers true extensibility through 100+ native connectors and a no-code configuration platform—enabling us to seamlessly integrate with our entire ecosystem, from PeopleSoft and Canvas to Salesforce, without custom development.
  - Provides actionable insights and reporting capabilities for identity governance.
- **Centralized Role Management**
  - Allows defining and managing roles and policies centrally ensuring consistency across the organization.
  - Can recommend optimal roles based on what similar users have, leveraging user pattern analysis.
- **Enables Automated Lifecycle Management**
  - Integrates with source systems like our HR and Student systems and can use data to automate on-boarding, change-boarding, and off-boarding.
- **Facilitates Automated Access Reviews**
  - Automated campaigns are possible and should be easier to manage and track.
  - Allows delegation of review to the appropriate owners while still providing full visibility.
- **Comprehensive Audit & Compliance**
  - Captures every access decision, approval, and lifecycle event.

Implementation and Road Map

Implementation

Road Map 2.2

Current versus New

Building the Foundation

Enhancing Existing Functionality

Improving User Experience

- "Lift and Shift" +

- Extensible Framework
- Building a richer dataset
- Collecting Use Cases

- External User Intake
- Attribute and Role Based Provisioning
- Enhanced Approvals and Workflows
- Certifications and Audits

- Activation and Password Management
- User Self Service and User Management
- Helpdesk Features

RISE 2030

RBAC Request and Review

Road Map 2.3

Attribute Based
and
Requestable Roles

Where are we today?

- Case management
- e-ORR

Fischer Features

- Supports **hybrid RBAC + ABAC** models using authoritative identity attributes (HR, SIS, ERP)
- Dynamic role assignment driven by **identity attributes** such as job code, department, affiliation, location, and status
- Role lifecycle management (create, modify, retire roles) with approval workflows
- Policy-based access rules evaluated continuously, not just at provisioning time
- Requestable roles with ability to provision just-in-time or with limited lifetimes
- Role simulation and impact analysis prior to deployment

Value Provided

- Accelerates onboarding by automatically assigning correct access based on attributes
- Ensures access aligns with **least privilege** and **business intent**
- Reduces role sprawl while preserving flexibility through attribute-driven access
- Improves scalability as populations grow or change frequently (students, employees, contractors)
- Simplifies audits by clearly mapping access to business rules and attributes

RISE 2030

RBAC Request and Review

Road Map 2.3 (supporting ongoing initiative)

Elevated Privilege Accounts and Privileged Account Management (PAM)

Features

- Identification and governance of **privileged, admin, and service accounts**
- Separation of standard user identities from elevated privilege identities
- Workflow-driven request and approval for elevated access
- Time-bound and purpose-based assignment of elevated privileges
- Integration with directories (AD, LDAP) and privileged groups
- Certification campaigns targeting privileged access specifically

Value Provided

- Reduces risk associated with standing administrative privileges
- Improves compliance with security and audit requirements
- Provides visibility into **who has elevated access and why**
- Supports segregation of duties (SoD) for high-risk functions
- Enables faster incident response by clearly identifying privileged identities

RBAC Request and Review

Road Map 2.3

AD/Entra Group Management and Automation

Features

- Automated creation, update, and removal of directory and application groups
- Attribute-driven and role-driven group membership rules
- Lifecycle-aware group management (joiner, mover, leaver)
- Approval workflows for manual or exception-based group assignments
- Synchronization with Active Directory, LDAP, and application-specific groups
- Group ownership and accountability tracking

Value Provided

- Eliminates manual group maintenance and associated errors
- Ensures group membership always reflects current business context
- Improves operational efficiency for IT and application teams
- Reduces over-provisioning and orphaned access
- Enhances transparency and accountability for group-based access

RISE 2030

Access Management

Road Map 2.4

Certification and Auditing

Features

- Scheduled and event-driven **access certification campaigns**
- Role, entitlement, group, and privileged access reviews
- Reviewer delegation and escalation support
- Attestation tracking with reviewer comments and decisions
- Automated remediation for revoked access
- Comprehensive audit logs and reportin

Value Provided

- Demonstrates compliance with regulatory and institutional policies
- Reduces audit preparation time through centralized evidence
- Ensures ongoing validation of access appropriateness
- Improves accountability by involving business owners in access decisions
- Lowers risk of toxic access combinations and access creep

RISE 2030

Directories and SSO Consolidation

Road Map 3.1, 3.2

Todays Architecture

- Active Directory
- Oracle LDAP
- Entra / CAS
- Not a unified login experience
- Supporting legacy systems

Future Architecture

- Modern Standards
- Active Directory
- Entra

Systems Integrations

Road Map 2.7

Extending Security Across the Enterprise

- Connecting to downstream systems
- API
- File Integration
- Other Connections
- Administrative Provisioning to disconnected systems

How can you prepare?

Questions?

THANK YOU!

- How to Follow the Project:
  - https://its.fsu.edu/iam
- How to Reach the Project Team:
  - IAM-Project@fsu.edu