October 19, 2022

Office of Internal Auditing

Enterprise Identity Management Audit

(Assurance Project)

MINNESOTA STATE

Background

Students, faculty, staff, applicants, and others need identities, also known as StarID user accounts, to access enterprise systems, such as ISRS, and campus-specific systems at the colleges and universities, such as computer lab workstations.

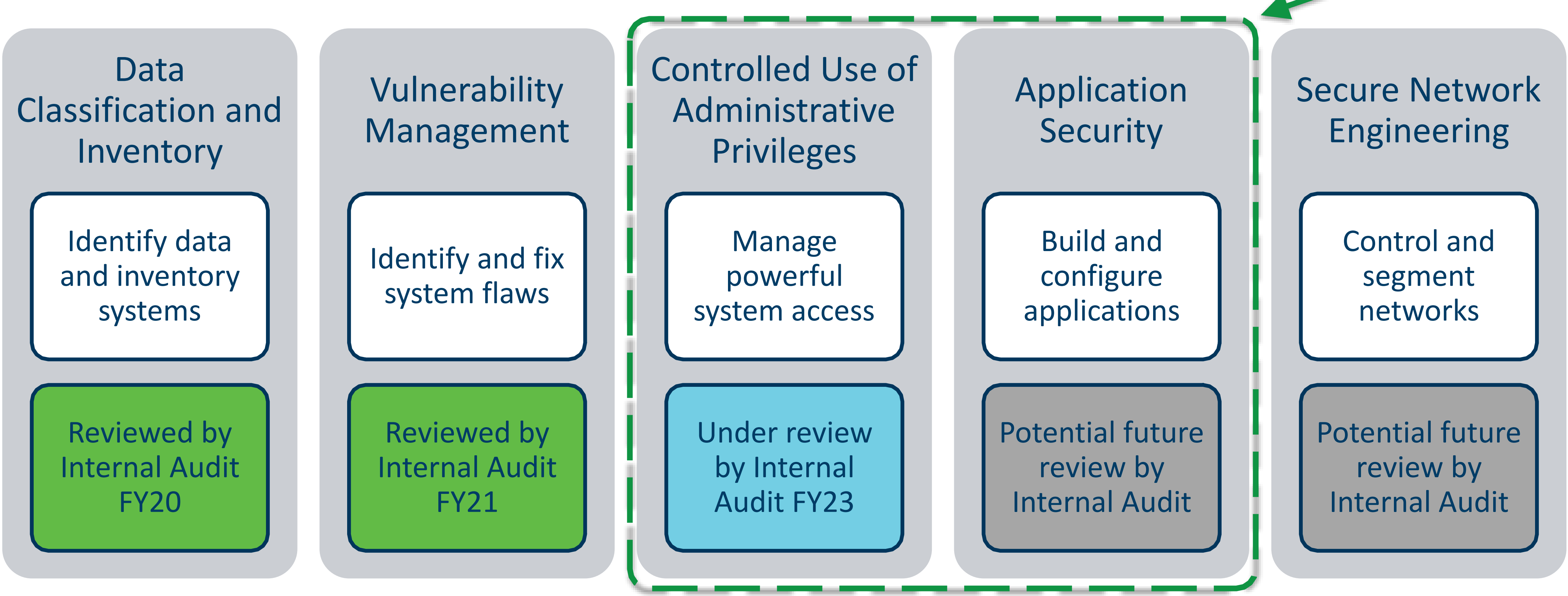
Minnesota State has a system-wide enterprise identity management program managed by the system office.

Program consists of processes and technologies that enable authorized access to systems.

Identity management is a key control for maintaining the security of data and enabling students, faculty, and staff to effectively use technology systems.

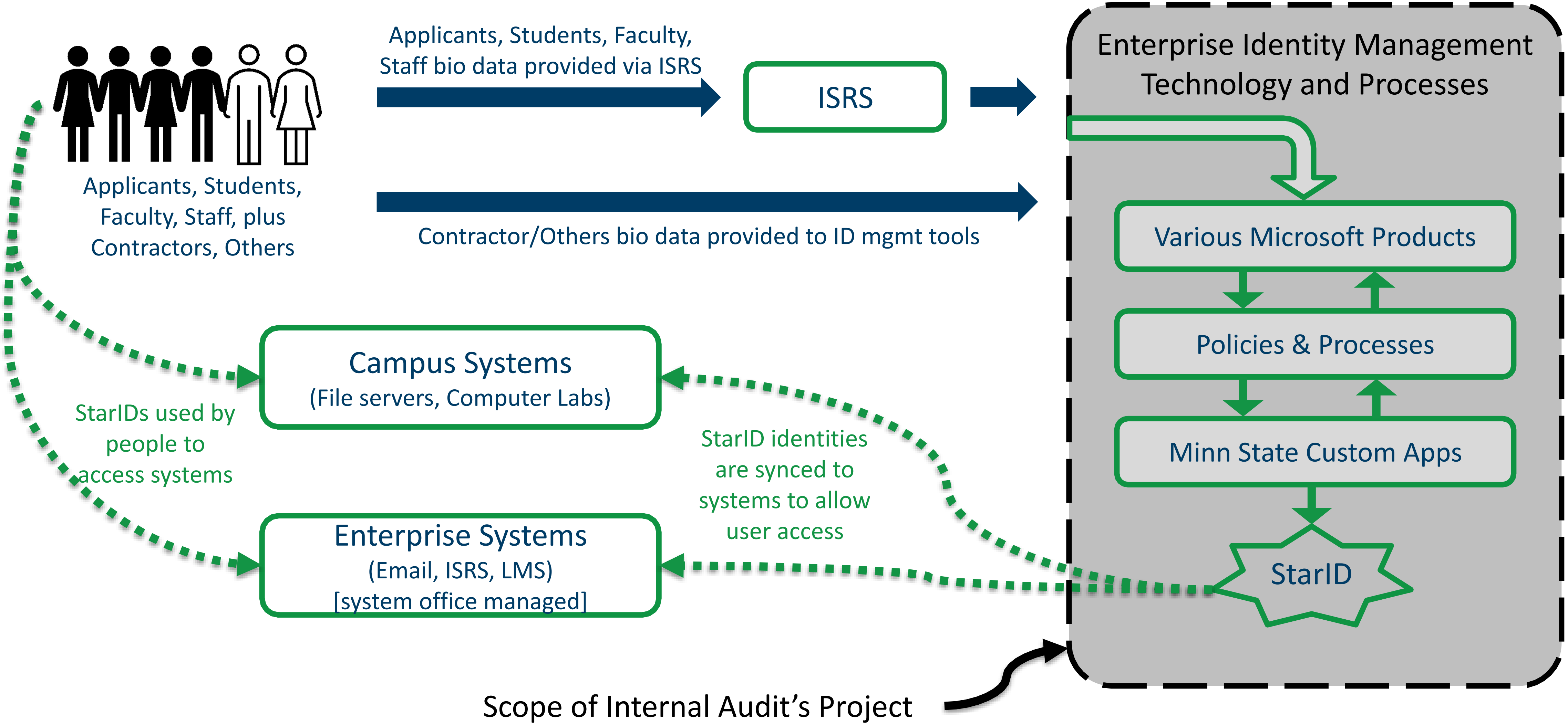
Background – Top 5 Cybersecurity Domains

Enterprise Identity Management is a foundational element of cybersecurity and of both security domains



Data Classification and Inventory	Vulnerability Management	Controlled Use of Administrative Privileges	Application Security	Secure Network Engineering
Identify data and inventory systems	Identify and fix system flaws	Manage powerful system access	Build and configure applications	Control and segment networks
Reviewed by Internal Audit FY20	Reviewed by Internal Audit FY21	Under review by Internal Audit FY23	Potential future review by Internal Audit	Potential future review by Internal Audit

Enterprise Identity Management Components


Applicants, Students, Faculty, Staff bio data provided via ISRS
ISRS
Enterprise Identity Management Technology and Processes
Applicants, Students, Faculty, Staff, plus Contractors, Others
Contractor/Others bio data provided to ID mgmt tools
Various Microsoft Products
Policies & Processes
Minn State Custom Apps
StarID
Campus Systems
(File servers, Computer Labs)
StarIDs used by people to access systems
StarID identities are synced to systems to allow user access
Enterprise Systems
(Email, ISRS, LMS)
[system office managed]
Scope of Internal Audit's Project

Project Objectives, Scope, Methodology

Objectives	Scope	Methodology
• Assess the system's enterprise identity management program • Evaluate whether applicable risks are identified and controlled appropriately by the system office • Assess system office compliance with relevant policies and guidance	• Specific technology components, including a combination of commercial off-the-shelf products and custom developed in-house applications • Certain processes that support the identity management program	• Tested that administrative privileged access was adequately controlled • Tested that technology components are securely configured and properly maintained • Assessed the identity management program, including policies/procedures, roles, system monitoring

Strengths

Automated rules are used to periodically review identities thereby enabling and/or disabling StarIDs as necessary (e.g., reviewing student StarIDs at the end of a semester).

Technology components are securely configured following vendor guidance and industry leading practices.

Code changes for custom developed in-house applications are scanned and reviewed for security issues and prior to implementation.

Interface between ISRS, which serves as the system of record for identities, and the other technology components is monitored to ensure that complete and accurate data flows between the components.

Conclusion

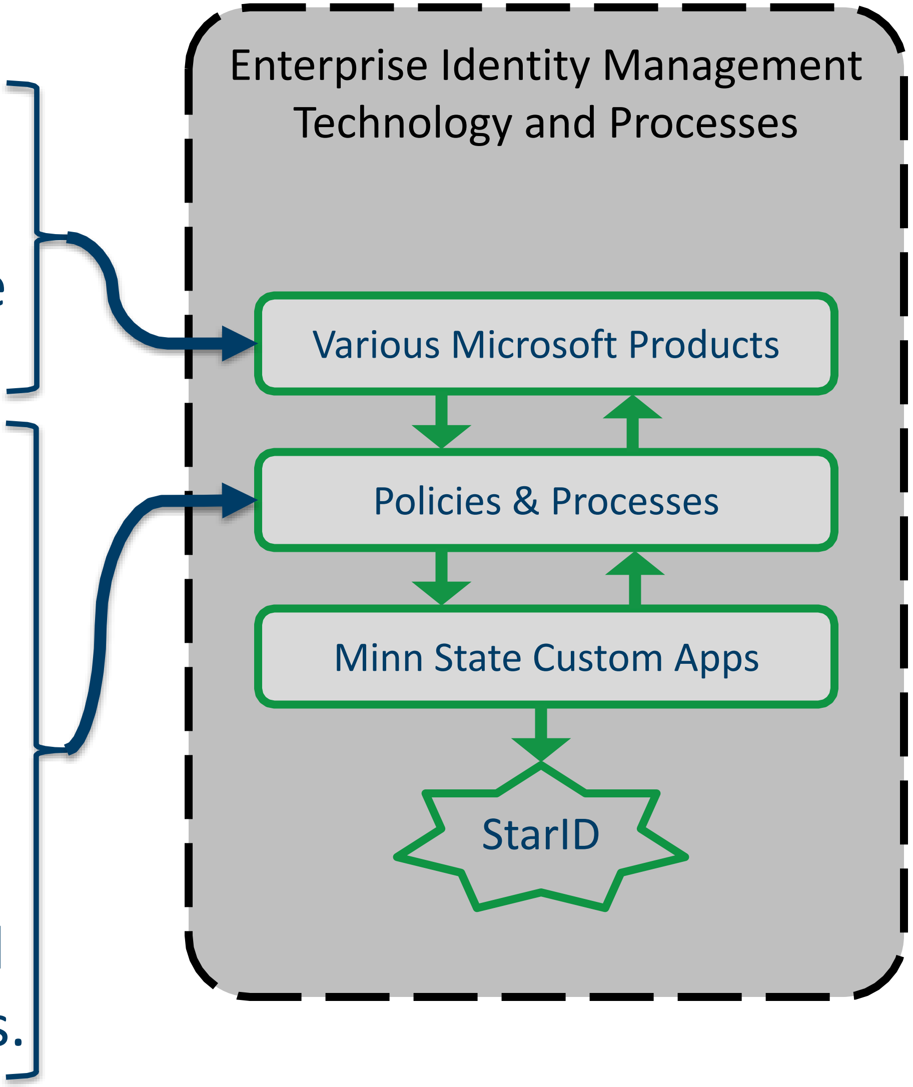
Identity management technology components and processes are adequately controlled to meet Minnesota State's current needs for functionality and security.

Minnesota State must replace a key technology component that will no longer be supported by the vendor, Microsoft Identity Manager (MIM).

To improve the maturity of the identity management program, Minnesota State should improve practices related to monitoring, standards, and verification.

Recommendations

1. Microsoft Identity Manager must be replaced prior to the end of vendor support; replacing this critical technology component will not be simple nor inexpensive.
2. System office should adopt a formal periodic review process for administrative users.
3. System office should establish and document formal guidance for colleges and universities to verify new student applicants StarIDs.
4. System office should complete the formal review of applicable policies, procedures, and operating instructions and make any revisions.


Enterprise Identity Management Technology and Processes
Various Microsoft Products
Policies & Processes
Minn State Custom Apps
StarID

Management Response – Next Steps

The CISO and CIO will work with the system and campus IT communities to implement recommendations presented in this assessment.

Jacquelyn Malcom
Vice Chancellor & CIO

Craig Munson
Chief Information Security Officer

Management Response - Findings

Retire current system in 2026

Replacement system to provide more functionality. Enhance security capabilities and options. Easier Integrations with additional systems including NextGen.

Incorporate an annual review of Administrator access - Manual vs. Automate review process

Automate at termination, looking at ways to automate when transfer. Small support staff.

Student applicant verification (AKA Bogus Applicants)

Balance the student experience and ease when applying for college/university admission with protection of system resources. Implemented several technical controls.

Board Policies, System Procedures and Operating Instructions updates

Reviewing and updating in progress.

Management Response

Transformational

One identity for use at any Minnesota State college or university.

Large, Complex system

1,000,000 logins per day, to 100s of applications. 500k active accounts.

Identity is integral to security

“Who are you?”, determines access to information assets and services. Identity data critical during security incidents & investigations.

Identity system is foundational to NextGen

With enhanced onboarding & offboarding processes. Opportunity to provide greater visibility into identity lifecycle.