March 21, 2023

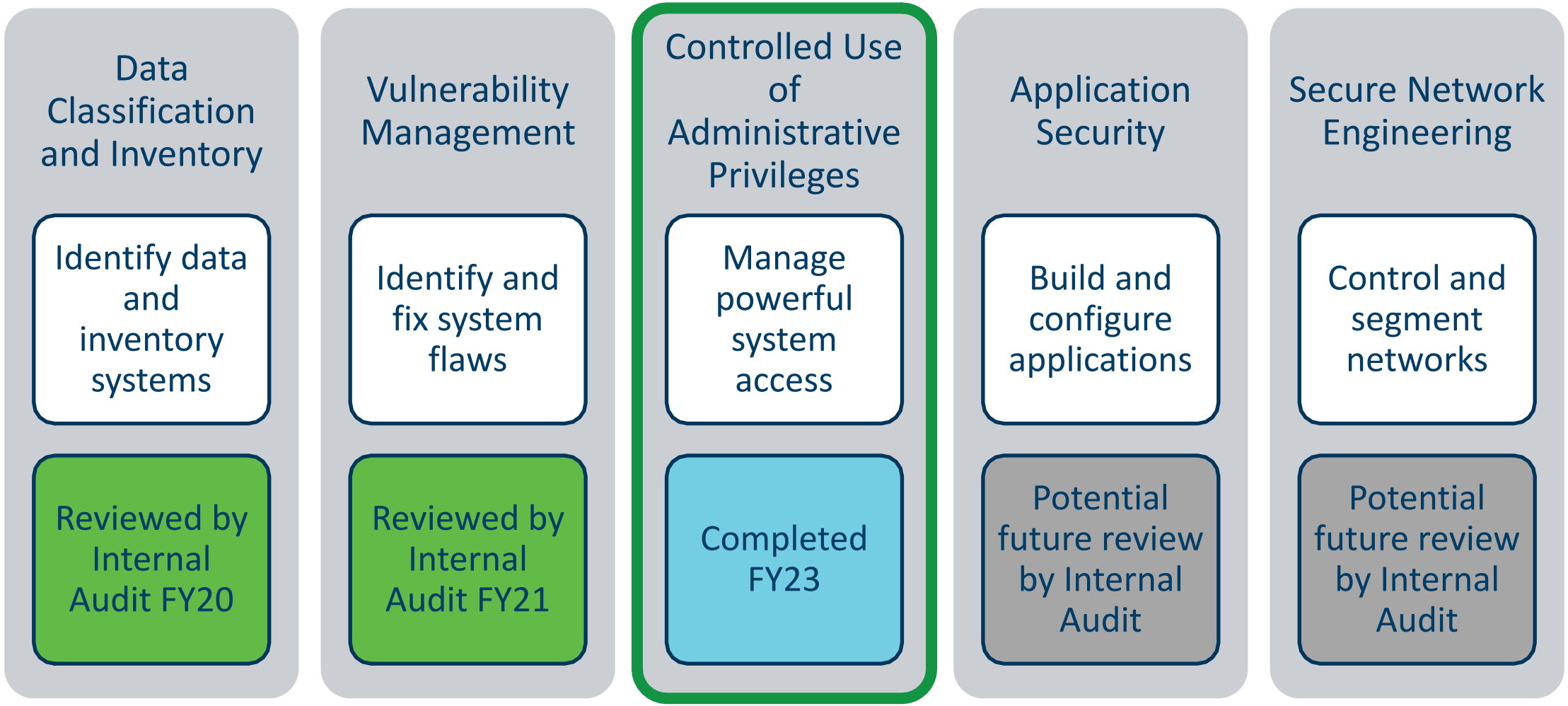
Office of Internal Auditing

Controlled Use of Administrative Privileges Audit

(Assurance Project)

MINNESOTA STATE

Background – Top 5 Cybersecurity Domains



Scope & Risk

What did we do?

Evaluated the implementation of four major control requirements, comprised of 15 safeguards, for the controlled use of administrative privileges

Reviewed all 26 colleges, seven universities, and the system office

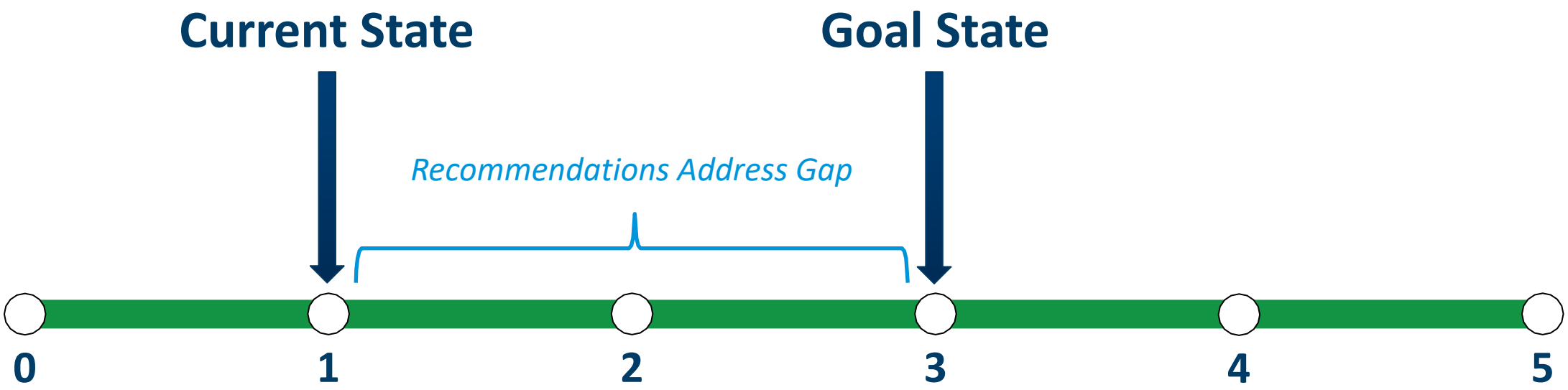
Why do we care?

Administrative privileges are the most powerful system user accounts, which allow almost unlimited control of data and systems.

Compromised administrative accounts are commonly used by criminal attackers to infiltrate, steal data, and deploy ransomware.

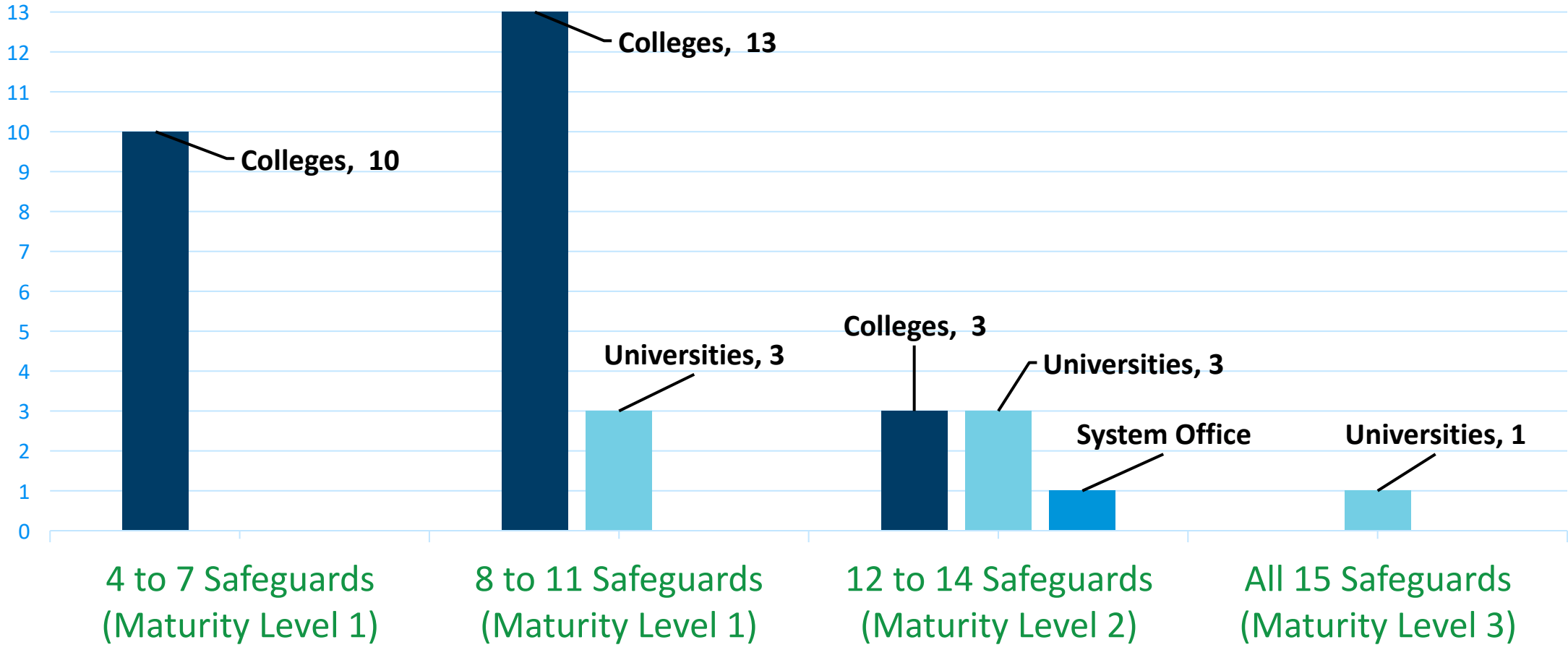
Conclusion

Overall System Wide Maturity



Conclusion

Count of Institutions by Safeguards Implemented



Strengths

All institutions have appropriately assigned job positions authorized to have administrative privileges to servers, network devices, and databases.

Most institutions do not have shared or generic administrative accounts, however, if there are generic (i.e., service) accounts, they are appropriately restricted to authorized personnel.

The great majority of institutions have audit trails enabled on servers, network devices, and databases to log administrative user activity.

Recommendations

Institutions should prioritize the completion of all requirements, then the system office information security team should monitor the performance of all institutions.

System office information security team should update all related guidance documents to clarify administrative account requirements, and work with institutions to define and document responsibilities.

System office information security team should assist institutions with the creation of remediation training plans, as needed. Minnesota State should also consider the implementation of shared security alerting tools (e.g., Splunk).

Management Response Next Steps

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

Jacquelyn Bailey
Vice Chancellor & CIO

Craig Munson
Chief Information Security Officer