November 15/16, 2022

Office of Internal Auditing

Top 5 Cybersecurity Domains

(Progress Summary)

MINNESOTA STATE

Background – Top 5 Cybersecurity Domains

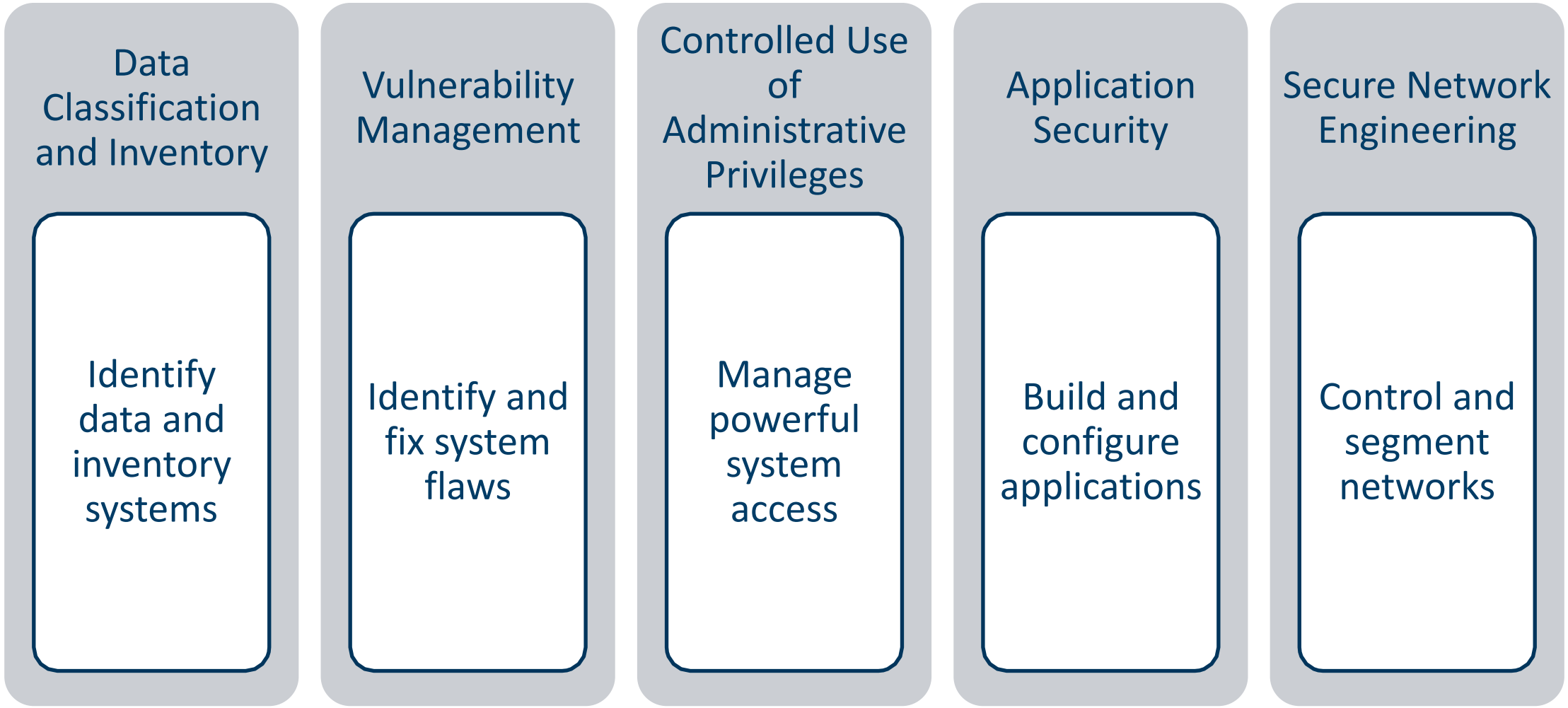
Goal to protect systems and data based on each entity's unique cybersecurity risks

Custom developed by Minn State as the initial cybersecurity framework for all 33 colleges and universities and system office to adopt

Provides protection guidance in five domains, rather than strict, prescriptive requirements, following a maturity model

Allows each entity to implement protections that fit their unique environment

Background – Top 5 Cybersecurity Domains



Background – Internal Audit's Approach to Assessing Top 5 Cybersecurity Domains

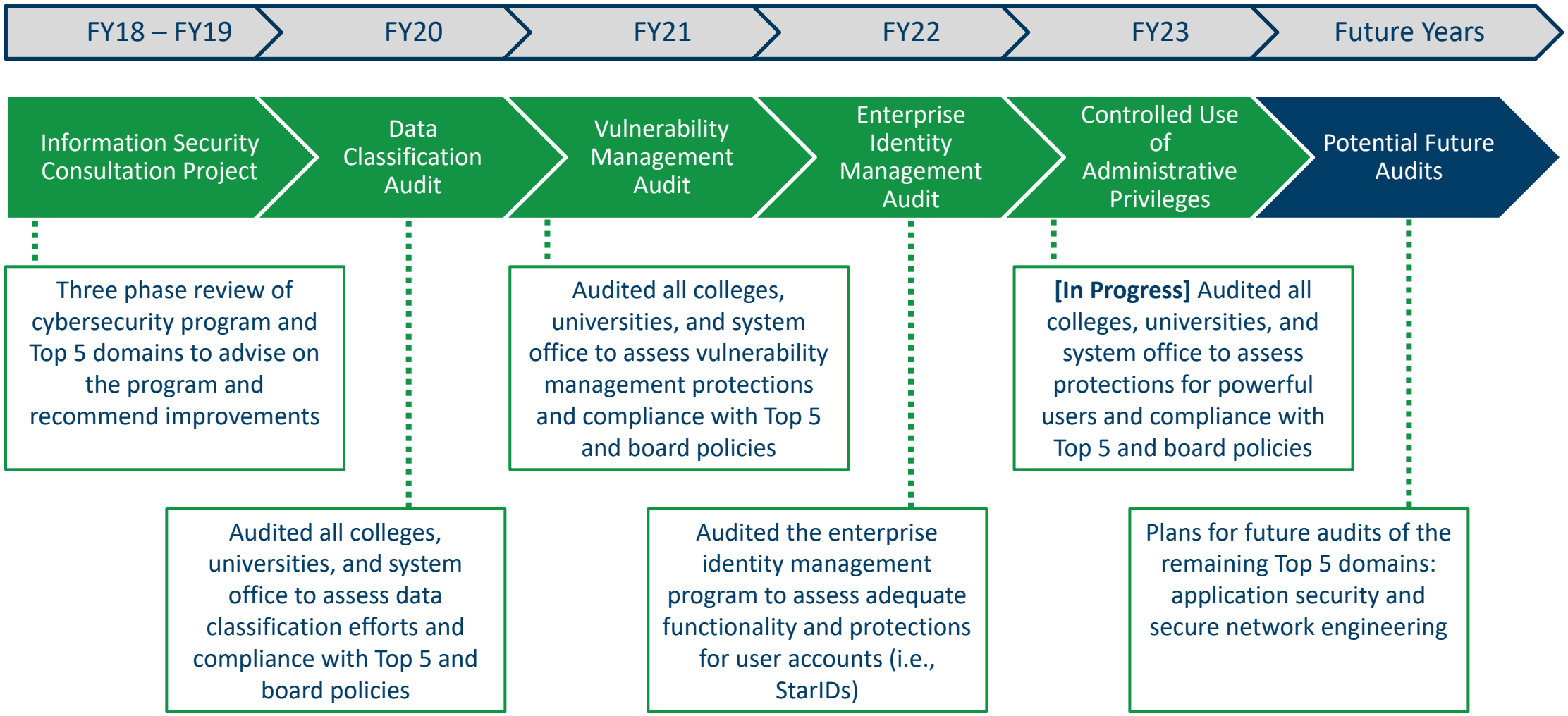
Approach was first assessing the overall program, then audit each domain

Methods include surveys, automated tools, interviews, walkthroughs

Scope includes all colleges and universities and system office when feasible, and pilot institutions for detailed testing when possible

Audit objectives focus on ensuring adequate implementation of the top 5 domains and compliance with Board Policies, Procedures, Guidelines, and Operating Instructions

Background – History of Internal Audit Projects



Summary – Strengths

Top 5 program is designed to address many of the critical cybersecurity risks faced by colleges and universities

Secure Network Engineering is the most mature domain due to system office implementing technologies that provide many protections to the entire system

Scanning to proactively find vulnerable software includes over 100,000 IT systems is automated using a centrally managed tool available to all colleges and universities and the system office

User identities (e.g., StarIDs usernames) are centrally supported to allow students, faculty, and staff to easily access enterprise and campus systems regardless of location

Summary – Recommendation Themes

Implement a specific, defined program for conducting routine cybersecurity assessments of colleges, universities, and system office

Update the Top 5 document, operating instructions, and system procedures to include specific requirements and explicit roles and responsibilities to support colleges and universities with protection implementation

Prioritize the completion of IT system inventory and classification, then formalize vulnerability detection and remediation activities for all colleges and universities

Create collaborative workspaces to share best practices for Top 5 and serve as a consolidated toolkit of existing and new trainings, tools, and templates from across the system

Develop a plan for transitioning from the custom developed Top 5 to an industry accepted cybersecurity framework (e.g., NIST Cybersecurity Framework)

Summary – Status of Recommendations FY18-22

Cybersecurity Area	Total Recommendations				
	Made by Internal Audit	Made by CLA	Resolved by management	Risk accepted by mgmt.	Unresolved
Data Classification	3	1	1	2	1
Vulnerability Management	3	2	0	0	5
Enterprise Identity Management	4	N/A	0	0	4
Controlled Use of Admin Priv	TBD*	4	2	2	0
Application Security	TBD*	6	4	2	0
Secure Network Engineering	TBD*	1	0	1	0
CLA Financial Statement Audit IT Findings (FY18-21)	N/A	20	9	6	5
TOTALS	**10**	**34**	**16**	**13**	**15**

* = Audits are in progress or planned for future, as such no recommendations have been made yet by Internal Audit.

Next Steps

Dr. Jacquelyn Bailey
Vice Chancellor & CIO

Craig Munson
Chief Information Security Officer

Our Scale and Threat Environment

1,000,000 StarID logins/day (at peak), 660,000 average/day

Over 500 database Transactions/second (at peak) in ISRS (Student Record System)

Roughly 1.4 Billion attempts to connect to our firewalls per day
Over half of those connection attempts are hostile and are denied

Enterprise Systems Log Storage = 1 Terabyte/day
About 3 miles of Webster dictionaries stacked up every day

Year in recap

Security Incidents

6 Major - Large disruptions or significant loss of data

Multifactor Authentication for employees has brought this down

792 Minor - (phishing/compromised student accounts, etc.)

Cybersecurity Control Implementations - Recent

Multifactor Authentication – Enhanced Identity Validation (Password and 2nd factor)

Improved Logging Infrastructure, "Splunk" – Building infrastructure for NextGen (and ransomware resistance)

Annual Campus Security Assessment- Evaluate general security practices & alignment with Top 5 framework

3rd Party Vendor Risk Assessments enhancements

Looking Ahead - Transition Top 5 to NIST 800-171

Federal Department of Education direction, specifically for student aid

Broader range of control areas

Still maintain flexibility in implementing controls

Work Effort - Alignment, then compliance

Currently conducting NIST gap analysis
Much of NIST controls already implemented in Top 5

Looking Ahead – Ransomware Resilience

Align with NIST 800-171

Enhance Threat Intelligence using Logging & Monitoring/Splunk

Integrate enhanced Identity controls

Increase collaboration with Campus leadership and security staff

Looking Ahead – NextGen & Security

NextGen will change security posture, significant benefits

Enhance agility and scale

Better opportunity for role-based security, least privilege design

Better “auditability” of the system and transactions