Minnesota State Colleges and Universities

Enterprise Systems Controls Assessment
of Top 5 Security Domains

Summary Results

October 31, 2022

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

Introduction to Top 5 Control Framework

Minnesota State Colleges and Universities (Minnesota State) has developed a control framework that is unique to Minnesota State and references elements of internationally recognized frameworks including: New Zealand Information Security framework, Center for Internet Security (CIS) Critical Security Controls and the NIST Cybersecurity framework.

This control framework was adopted as a methodology to assist with the assessment of information security risk within the System Office and the 37 colleges and universities. The framework allows Minnesota State to measure key components of the organization's security posture.

Introduction to Top 5 Control Framework (Continued)

Five security domains have been identified as being critical for reducing IT operational risk within the system office and the colleges and universities that make up the Minnesota State system. Each domain has a range of activities that range from minimal effort being made in the area, to high effort expended on activities in the domain.

The goal of this security plan is to define a baseline for each domain and the measurable activities that can be performed during the next fiscal year to show progress in each area. It is critical to understand that the activities in each domain are additive and continuous. Movement along the scale by definition means additional and continuous workload in order to remain vigilant in reducing risk. The ultimate goal is to take each activity and make it part of basic operations.

Control Maturity (Measurement)

Within each of the Top 5 Security Domains, criteria was established by Minnesota State to measure the maturity of controls against the framework including level of effort as described below:

Effort	Description
Minimal (Starting)	Describes the minimal controls that must be implemented to demonstrate commitment by management
Moderate (Improving)	Describes additional controls that must be implemented to illustrate improvement from the baseline controls required under the Minimal Effort category
High (Advancing)	Describes controls that are in addition to those under the Minimal and Moderate Effort categories

Scope

CliftonLarsonAllen LLP (CLA) was engaged to assess controls in meeting the following key components of the framework:

- Data Classification and Inventory
- Vulnerability Management
- Controlled Use of Administrative Privileges
- Application Security
- Secure Network Engineering

Approach

CLA used the following approach to reach a conclusion for each component:

- Reviewed existing policy statements and procedures applicable to the assessment.
- Met with appropriate Minnesota State personnel applicable to the assessment to obtain a baseline understanding of the controls implemented.
- Requested documentation as evidence of control(s) being implemented as applicable to the assessment.
- Reviewed the documentation provided to determine if the evidence illustrated compliance with the key components of the Top 5 Security Domains.
- Prepared a report summarizing CLA conclusions in preparation for presentation to the Board of Trustees.

Results of Assessment – Data Classification

Minimal Effort (Starting)	Moderate Effort (Improving)	High Effort (Advancing)
Data Classification and Inventory		
Identify/assign “Data Owners” – Note: The data owner typically is not the IT department Create an inventory of systems under IT’s control or management (Note: ISRS is part of the system office’s inventory)	Identify systems and applications where ‘Highly Restricted’ data resides	Identify systems and applications where ‘Restricted’ and ‘Low’ data resides
Conclusion		
Meets Criteria	**Meets Criteria**	**Meets Criteria**
Management Response		
Not Required	**Not Required**	**Not Required**

Results of Assessment – Vulnerability Management

Minimal Effort (Starting)	Moderate Effort (Improving)	High Effort (Advancing)
Vulnerability Management		
Assign devices to appropriate device scanning groups based on the asset's value. Value is determined by the confidentiality and integrity requirements of the data stored, processed or transferred by the device	Implement credentialed scanning on all managed devices	Develop patching and remediation plan and process using a risk-based approach. Plan includes a prioritized top-down patching approach that addresses higher risk resources first (e.g. Internet facing systems, CAP server and PCI networks) and critical patches (e.g. zero-day exploits) as highest priority. Monitor progress using reports and metrics
Conclusion		
Meets Criteria for Data Center	**Meets Criteria for Data Center**	**Meets Criteria for Data Center**
Meets Criteria for Workstations	**Partially Meets Criteria for Workstations** 80% of workstations were scanned which is not within the 5% tolerance.	**Partially Meets Criteria for Workstations** 67% of the workstations scanned scored less than 1000
Management Response		
Not Required	Management agrees with the finding. Due to the increase in teleworking remotely, scanning a device has required the remote user to manually initiate a connection to Minnesota State's network. Two (2) projects are currently in progress to alleviate the manual process, ensuring devices are automatically attached and scanned.	Management agrees with the finding. Due to the increase in teleworking remotely, scanning a device has required the remote user to manually initiate a connection to Minnesota State's network. Two (2) projects are currently in progress to alleviate the manual process, ensuring devices are automatically attached, scanned and patched.

Results of Assessment – Administrative Privileges

Minimal Effort (Starting)	Moderate Effort (Improving)	High Effort (Advancing)
Controlled Use of Administrative Privileges		
Identify job responsibilities that require administrative access to specific systems (including desktop/laptop PCs) Assign access as appropriate	Conduct periodic review of access using established review schedule	Administrative access is granted based on Minnesota State methods that align with “industry accepted practices”
Conclusion		
Meets Criteria	**Meets Criteria**	**Meets Criteria**
Management Response		
Not Required	**Not Required**	**Not Required**

Results of Assessment – Application Security

Minimal Effort (Starting)	Moderate Effort (Improving)	High Effort (Advancing)
Application Security		
Application security training for internal development staff Create comprehensive inventory of applications with appropriate data classification assigned	Establish software development life-cycle that includes security touch-points for internally developed applications Establish process to assess 3rd party applications for appropriate security controls and practices	Implement scanning and/or peer review of code for internally developed applications, identifying and remediating vulnerabilities Implement process to assess 3rdparty applications for appropriate security controls and practices Plan for and retire applications that are no longer supportable
Conclusion		
Partially Meets Criteria Minnesota State has not formalized a secure coding practices training program for developers.	**Meets Criteria**	**Meets Criteria**
Management Response		
Management agrees with the finding. Management has implemented formal processes that require scanning of all developed software, and vulnerabilities remediated to an acceptable risk level prior to implementing into production. Most developers have completed baseline training. Management will identify gaps in training and ensure training is completed.	**Not Required**	**Not Required**

Results of Assessment – Secure Network Engineering

Minimal Effort (Starting)	Moderate Effort (Improving)	High Effort (Advancing)
Secure Network Engineering		
Develop a comprehensive network diagram for all campus network, server and end-point infrastructure	After classifying data as Highly Restricted, Restricted or Low, and the criticality of the data to the business or academic functions, identify where the data is stored and/or transmitted Identify the perimeters between the various network segments based on data classification level and business/academic functional needs	Implement network security access controls/policies between different data classification levels commensurate with the data's classification and the business or academic needs. Validate controls/policies exist between segments of different trust levels. Implement appropriate secure remote access methods (e.g. multi-factor, VPN, etc.) to data based on data classification level and criticality to business or academic needs
Conclusion		
Meets Criteria	**Partially Meets Criteria** Minnesota State had not identified the physical locations where Highly Restricted, Restricted and Low classified data resides	**Meets Criteria**
Management Response		
Not Required	Management agrees with the finding and accepts the risk. Minnesota State has implemented strong controls that limit access to sensitive data based on 'need-to-know' and a person's job responsibilities. The controls mitigate unauthorized access and the need to physically identify where classified data resides.	**Not Required**