Minnesota State
Colleges and Universities

Information Technology (IT) Segment of Financial Audit
Summary Results

October 31, 2022

2022 Scope – Colleges and Universities

Dakota County Technical College	Fond du Lac Tribal & Community College	Hibbing Community College*	Inver Hills Community College
Itasca Community College*	Lake Superior College	Mesabi Range College*	Minnesota State College – Southeast
Minnesota State University Moorhead	Northland Community & Technical College	Pine Technical & Community College	Rainy River Community College*
St. Cloud State University	Saint Paul College	Vermilion Community College*	System Office

* Indicates the institutions recently combined as Minnesota North

2022 Scope – Control Domain(s) & Application(s)

Control Domain(s)

- Organization Administration

- Application System(s) Administration

- Information Systems Operations

- Data Administration

- Technical Infrastructure Administration

- Contingency Planning

- Physical Environment

Application(s)

- ISRS
  - General Ledger
  - Accounts Payable
  - Human Resources (HR) / SCUPPS

- eTime
  - Time Reporting

- MarketPlace
  - Purchasing

Results of Controls Analysis

Control(s)	Results	Risk	Priority	Comment(s)
Background Investigations	Partially Exists	Medium	Medium	Background investigations are only completed on candidates that will fill executive and IT positions
2022 Management Response	*Management accepts this risk. New and current employees attend annual training regarding private data. Further, the expansion of background checks potentially increases our risk of potential disparate treatment or disparate impact claims that is inherent in conducting criminal background checks.*			

Results of Controls Analysis

Control(s)	Results	Risk	Priority	Comment(s)
Segregation of Duties	Pending Completion of Financial Statement Audit	Medium	Medium	Some users within "in scope" colleges and universities have known conflicting roles within applications
2022 Management Response	*Management will work with any colleges and universities where the financial statement auditors determine appropriate compensating or mitigating controls are not in place.*			

Results of Controls Analysis

Control(s)	Results	Risk	Priority	Comment(s)
Monitoring Users with Known Segregation of Duties (SOD) Conflicts	Pending Completion of Financial Statement Audit	Medium	Medium	The CLA Financial Audit team will determine if mitigating/monitoring controls are in place for "in scope" college and universities for users with known conflicting roles within applications
2022 Management Response	*Management will work with any colleges and universities where the financial statement auditors determine appropriate compensating or mitigating controls are not in place.*			
Stale Users	Partially Effective	Medium	Medium	Very limited number of user accounts remain active for separated employees
2022 Management Response	*Management agrees with this comment and feels that the Minnesota State Colleges and Universities have continued to make great strides in reducing stale security roles in recent years. The few colleges and universities named in the scope of this audit have or will remove the identified stale users.*			

Results of Controls Analysis

Control(s)	Results	Risk	Priority	Comment(s)
Data Transfers – Outgoing	Partially Exists	Medium	Medium	Outgoing "adhoc" file transfers do not require approval prior to transfer of data
2022 Management Response	*Management partially agrees with this comment. Minnesota State will continue evaluating and/or implementing a Data Loss Prevention tool. However, due to resources and personnel constraints, implementing a comprehensive process where data owners approve transfers of confidential data in all instances may not be feasible. As a mitigating control, the Public Jobs; Private Data online training module instructs employees to only share data with authorized individuals on a need-to-know basis. Minnesota State has also developed guidance on where users should store sensitive, protected or personally identifiable information and secure methods for transmitting information in technology systems.*			

Results of Controls Analysis

Control(s)	Results	Risk	Priority	Comment(s)
Network and Web Application Testing	Partially Exists	Medium	Medium	External and Internal network penetration tests were not performed during FY2022 as part of the alternating year plan. Web-facing applications are scanned for vulnerabilities but were not penetration tested during FY2022
2022 Management Response	*Management agrees with this comment. Testing was delayed due to budget constraints. Management will evaluate the viability of conducting penetration testing in FY2023.*			

Create Opportunities

Results of Controls Analysis

Control(s)	Results	Risk	Priority	Comment(s)
Server Administrator Passwords	Partially Exists	Medium	Medium	Server administrator passwords are not technically enforced for length
2022 Management Response	*Management accepts the risk. In the event that MFA fails, as a mitigating control, accounts are locked out after 10 attempts.*			
Business Continuity and Disaster Recovery Plan Testing	Does Not Exist	Medium	Medium	The BCP and DRP were not formally tested during FY2022.
2022 Management Response	*Management agrees with this comment. A project to mature DRP and BCP processes and documentation was completed in fiscal year 2022. A tabletop exercise is scheduled November 2022 to identify gaps and make any required changes to the processes and documentation.*			

Results of Controls Analysis

Control(s)	Results	Risk	Priority	Comment(s)
Physical Security	Partially Exists	Medium	Medium	Physical access activity logs from each colocation data center are not reviewed by management.
2022 Management Response	*Management agrees with this comment. Management will review current processes for identifying individuals that have separated from the organization and have them removed from the list of those authorized in a timely manner.*			

Application System(s) & Information Technology Analysis Report

Detailed information related to the results of the control analysis performed by the Information Security Services Group (ISSG) within CliftonLarsonAllen LLP is contained within the Application System(s) & Information Technology Analysis Report that was provided as a separate document.