Minnesota State Colleges and Universities

Information Technology Segment of
Financial Statement Audit for Fiscal Year Ending June 30, 2022

Description of Application System(s) & Information Technology Control(s) Design in Support of Financial Statement Audit

October 31, 2022

In planning and performing our audit of the financial statements of Minnesota State Colleges and Universities as of and for the year ended June 30, 2022, in accordance with auditing standards generally accepted in the United States of America, we considered Minnesota State Colleges and Universities' internal controls over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of Minnesota State Colleges and Universities internal controls. Although this document was generated in support of the financial statement audit of Minnesota State Colleges and Universities, we do not express an opinion on the effectiveness of Minnesota State Colleges and Universities' internal controls.

This report is **Proprietary & Confidential** and intended solely for the information and use of Minnesota State Colleges and Universities management and is not intended to be and should not be used by anyone other than these specified parties.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

Scope 1
Approach 1
Summary Analysis 3

Executive Summary

Scope

In support of the 2022 financial audit process conducted by CliftonLarsonAllen, LLP, (CLA) the scope of the *Information Technology and Application System(s) Analysis* was focused on the internal controls related to application system(s) and supporting technical infrastructure that could impact the integrity of the financial statement reporting process specific to Minnesota State Colleges and Universities (Minnesota State). Specific application systems included in the analysis for this fiscal year were as follows:

Application	Business Purpose	Database	Operating System	Hosted	Managed
ISRS	GL-AP-Accruals	Oracle	Linux	Internally	Internally
ISRS	HR (SCUPPS)	Oracle	Linux	Internally	Internally
eTime	Time Reporting	Oracle	Linux	Internally	Internally
eProcurement (Marketplace)	Purchasing	Hosted App	Hosted App	Externally	Internally

Segregation of duties conflicts within ISRS applications identified above were tested for the following:

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

Approach

To achieve the analysis objectives, CliftonLarsonAllen focused on controls within the following domain(s):

Section	Control Domain
1	Organization Administration
2	Application System(s) Administration
3	Information Systems Operations
4	Data Administration
5	Technical Infrastructure Administration
6	Contingency Planning

Representatives of Minnesota State were requested to provide information specific to application system(s) and underlying technical infrastructure that were relevant to the financial reporting process to assist CLA in analyzing the adequacy of control design for each of the domains identified above to determine reliability of data.

This information was also used by CLA as a basis for discussions during planning and follow up interviews to confirm adequacy (suitability) of control design and compliance with control design to determine effectiveness.

The results of the analysis were intended to identify design and implementation deficiencies that prevent the control(s) from being effective and are reported as follows:

Results	Definition
Exists	Control exists as a result of inquiry and/or observation
Partially Exists	Control partially exists as a result of inquiry and/or observation
Does Not Exist	Control does not exist as a result of inquiry and/or observation
Effective	Control is effective based on audit evidence
Partially Effective	Control is partially effective based on audit evidence
Not Effective	Control is not effective based on audit evidence
Not Applicable	Control is not applicable to the environment

To assist management in responding to control design and/or implementation deficiencies, the following guideline is provided as a reference in determining risk due to inadequate controls:

Risk	Definition
Extreme	Immediate potential to negatively impact reliability/integrity of financial data, availability/security of systems or protection of confidential data (*i.e. no control*)
High	Potential to negatively impact reliability/integrity of financial data, availability/security of systems or protection of confidential data *(i.e. weak control due to improper design or high risk of failure)*
Medium	Intermittent potential to negatively impact reliability/integrity of financial data, availability/security of systems or protection of confidential data (*i.e. control exists but not enforced consistently or needs to be expanded*)
Low	Controls are in place and operating effectively – however inherent risk exists

In addition, each **Comment(s)** was assigned a priority that defines a suggested review period and period of time that a mitigating control should be identified and potentially implemented.

Priority	Review Period	Identify Mitigating Controls
Immediate	Within 10 Days	Within 30 Days
High	Within 30 Days	Within 60 - 90 Days
Medium	Within 90 Days	Within 120 – 180 Days
Low	Within 180 Days	Comments are based on "*best practice*" and can be addressed as time permits to determine if additional controls should be implemented.

Summary Analysis

The results of the current year review process are summarized below. The content within the table identifies controls relevant to financial statement reporting that did not exist or could be strengthened:

Background Investigations			
Control Expectation(s)	Background investigations including criminal history are performed on all candidates that will have access to confidential information as a condition of employment.		
Control Analysis	Only candidates that will fill executive positions (*i.e. Presidents*) and IT positions have background checks completed as a condition of employment.	**Reference** **Results** **Risk**	3.04 Partially Exists Medium
Comment(s)	To the extent possible, Minnesota State should consider background checks on any employee that will have access to confidential information. As an example, requirements for background checks could be performed based on data classifications (*i.e. Highly Restricted, Restricted*) adopted by Minnesota State and the candidate's anticipated access to data in the specific classification(s).	**Priority**	Medium
2020 Management Response	Management agrees with this comment. Minnesota State's Human Resources division will explore conducting background checks for individuals that have access to significant amounts of Highly Restricted data.		
2021 Management Response	Management has developed guidelines for background checks. Currently it is up to each Vice Chancellor to determine which staff will require background checks. Due to budget restrictions in 2021 it was determined to keep the background checks the same. Management will review the requirements again in 2022.		
DRAFT 2022 Management Response	Management accepts this risk. Employees new to Minnesota State complete training regarding the proper management of public vs. non-public data as defined by Chapter 13 Minnesota Data Practices. Current employees attend training annually. Breaches of data privacy are considered just cause for employee discipline up to and including discharge. Background check findings are unlikely to provide assurance that breaches of data privacy will not occur. 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. Minnesota State believes its ongoing awareness protocols for the proper handling of private data is an effective method for ensuring the proper handling of private data by all employees. Minnesota State performs background checks on finalists for executive positions and those required by law or to receive federal funding.		

Application Administration – ISRS			
Control Expectation(s)	Technical permissions within application systems and assignment of roles should be reviewed for appropriateness to determine if a user has excessive privileges or privileges that do not adequately separate authority.		
Control Analysis	Combinations of security roles within ISRS have been identified to be incompatible. Results of user account testing for the institutions in scope for the current fiscal year identified individuals that have technical privileges within ISRS to perform transactions that are considered conflicting. Counts of individuals, by institution are identified in the table below. Details have been shared with management.	**Reference**	6.18
		Results	Pending Completion of Financial Statement Audit
		Risk	Medium

College(s) / Universities	Individuals w/ HIGH Risk Conflicts	Individuals w/ MEDIUM Risk Conflicts	Individuals w/ BOTH Risk Conflicts
Dakota County Technical College	1	5	1
Fond du Lac Tribal & Community College	2	2	1
Hibbing Community College	2	1	0
Inver Hills Community College	0	3	1
Itasca Community College	3	2	0
Lake Superior College	1	2	0
Mesabi Range College	1	1	1
Minnesota State College - Southeast Technical	1	0	1
Minnesota State University Moorhead	1	0	0
Northland Community & Technical College	1	0	1
Pine Technical College	2	2	1
Rainy River Community College	2	1	0
St. Cloud State University	0	2	1
Saint Paul College	0	1	1
Vermilion Community College	3	1	0
System Office	4	2	0

Comment(s)	Management should analyze users with conflicting technical permissions within ISRS to determine if privileges are based on business need and / or compensating controls are in place to reduce or eliminate risk. Specifically, management should establish procedures to approve conflicting technical permissions that are necessary to perform business responsibilities and monitor activity performed by these users to ensure all transactions are authorized. CLA financial audit staff will identify in the financial audit management letter any conflicting roles where management has not identified a compensating control.	**Priority**	Medium

Application Administration – ISRS			
2020 Management Response	Management agrees with this comment and feels the Security Management application currently provides adequate notification to the security role approver of an incompatibility before the role is approved. Additionally, when a role with an incompatibility is approved, the Security Management application provides a text box where the security role approver should record the mitigating control that will be in place. Colleges and universities with incompatibilities noted in the scope of this audit have reviewed the assigned roles and confirmed the business need or removed the role in cases where the business need no longer exists.		
2021 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.		
DRAFT 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.		

Monitoring Users with Known Segregation of Duties (SOD) Conflicts			
Control Expectation(s)	Activity performed by users with conflicting permissions is logged and reviewed by management on a scheduled basis.		
Control Analysis	As a result of discussions with management of “in scope” colleges and universities, it was noted that SOD conflicts were a result of business need, either for backup of personnel or cross training. However, activity performed by users with known conflicts is not reviewed on a scheduled basis.	**Reference**	6.15
		Results	**Pending Completion of Financial Statement Audit**
		Risk	Medium
Comment(s)	Management should review activity performed by users with SOD conflicts on a scheduled basis to confirm only authorized transactions were performed.	**Priority**	Medium
2020 Management Response	Management agrees with this comment and colleges and universities noted in the scope of this audit will review current practices and look into adding a review of their incompatible duties, compensating controls, and the documentation of those controls.		
2021 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.		
DRAFT 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.		

User Account Administration – Stale User(s)			
Control Expectation(s)	User accounts for employees that separate should be disabled / deleted on or before the last date of employment. In addition, department managers should perform a periodic user account review to ensure user accounts were disabled / deleted as expected and report any evidence of misuse to management.		
Control Analysis	Based on analysis of current user accounts compared to a list(s) of current or terminated employees, it was noted that some user accounts were still active for employees that separated from Minnesota State. This included employees who left Minnesota	**Reference**	6.16 / 6.20
		Results	**Partially Effective**
		Risk	Medium

User Account Administration – Stale User(s)

State that had user accounts that were still active at the time of field work. User access was primarily “view only” permissions. Counts of user accounts, by institution are identified in the table below. Details have been shared with management.

Risk Medium

College(s) / Universities	Stale Users by Application		
	HR SCUPPS	General Ledger	Market Place
Dakota County Technical College	0	2	1
Fond du Lac Tribal & Community College	0	0	0
Hibbing Community College	0	0	0
Inver Hills Community College	0	4	0
Itasca Community College	0	0	0
Lake Superior College	0	0	0
Mesabi Range College	0	1	0
Minnesota State College - Southeast Technical	0	2	0
Minnesota State University Moorhead	0	2	0
Northland Community & Technical College	0	2	1
Pine Technical College	0	0	2
Rainy River Community College	0	0	0
St. Cloud State University	2	3	0
Saint Paul College	0	2	0
Vermilion Community College	0	0	0
System Office	0	0	1

Comment(s)

Management should review procedures for disabling / deleting user accounts within application systems that transfer or separate from colleges and universities. User accounts that remain active for separated employees represent risk to Minnesota State, especially any accounts with elevated privileges.

Priority Medium

2020 Management Response

Management agrees with this comment and feels that the Minnesota State Colleges and Universities have made great strides in reducing stale security roles in recent years through communication and functionality added to the Security Management process. Supervisors can now remove security roles through the Employee Dashboard. Active security is also reviewed and recertified annually during November and December and stale security roles that are not removed by the supervisor will be found during that process. The four universities and colleges named in the scope of this audit will remove the stale users that have been identified.

2021 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 through communication and functionality added to the Security Management process. Supervisors can now remove security roles through the Employee Dashboard. Active security is also reviewed and recertified annually during November and December and stale security roles that are not removed by the supervisor will be found during that process.

The few colleges and universities named in the scope of this audit have or will remove the stale users that have been identified. Some of the names identified as of 6/30/21 actually current users so no action necessary on those. Overall, the small number of state users is very impressive and staff had left within a few months’ time.

User Account Administration – Stale User(s)	
DRAFT 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. The table also indicates quite a few colleges and universities did not have any users identified during the audit review.

Logical Access – User Account Administration			
Control Expectation(s)	Determine that logical access to network resources and application systems is appropriately managed for the organization including administration of user accounts and passwords.		
Control Analysis	Operating Instruction 5.23.1.1 identifies minimum password length of 8 characters. In December 2021, the Center for Internet Security (CIS) updated the recommended minimum password length to 14.	**Reference**	8.05
		Results	**Partially Exists**
		Risk	Medium
Comment(s)	Management should consider strengthening passwords by increasing password length from 8 to 14 with technical enforcement.	**Priority**	Medium
DRAFT 2022 Management Response	Management accepts the risk. Minnesota State requires multi-factor authentication for all system administrators that access enterprise technology systems, and for all students, faculty and staff that utilize the Microsoft Office 365 applications. These systems store or handle much of Minnesota State's sensitive and personally identifiable information. Minnesota State has also implemented lockouts for enterprise systems after 10 unsuccessful login attempts. Management feels the requirement of multi-factor authentication, and the implementation of lockouts, are adequate compensating controls in lieu of a 14-character password.		

Data Transfer(s) – Outgoing			
Control Expectation(s)	Data custodians and/or data owners must approve confidential data being transferred to an external entity prior to transmission of data.		
Control Analysis	Approval to transmit data outside of the organization on a scheduled basis as part of an automated job is obtained as part of the job approval process. Adhoc file transfers do not require approval prior to transfer of data.	**Reference**	12.03
		Results	**Partially Exists**
		Risk	Medium
Comment(s)	To the extent reasonable, approval should be obtained before transmitting any confidential data outside of the organization. In addition, Minnesota State should continue the evaluation / implementation of a Data Loss Prevention (DLP) tool.	**Priority**	Medium
2020 Management Response	Minnesota State 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.		
2021 Management Response	Minnesota State 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.		

Data Transfer(s) – Outgoing	
Control Expectation(s)	Data custodians and/or data owners must approve confidential data being transferred to an external entity prior to transmission of data.
DRAFT 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.

Network and Web Application Penetration Testing			
Control Expectation(s)	Network and web application penetration testing is performed annually by an external security services firm.		
Control Analysis	External and Internal network penetration tests were not performed during FY2022 as part of the alternating year plan. The internal network penetration test is still being evaluated for feasibility based on financial budget. Web applications are scanned for vulnerabilities but were not penetration tested during FY2022.	**Reference**	15.10 / 15.11 / 15.12
		Results	Partially Exists
		Risk	Medium
Comment(s)	CLA recommends Internal, External and Web Application penetration testing be performed annually to identify and remediate new vulnerabilities which may be present due to configuration or application changes, or new vulnerabilities being discovered and added to vulnerability scanning databases.	**Priority**	Medium
2021 Management Response	Management agrees with this recommendation. Testing was delayed due to budget constraints and the impact of COVID-19 and Minnesota State staff not being onsite. Management will evaluate the viability of conducting penetration testing in FY2022.		
DRAFT 2022 Management Response	Management agrees agree with this recommendation. Testing was delayed due to budget constraints. Management will evaluate the viability of conducting penetration testing in FY2023.		

Server Administrator Passwords			
Control Expectation(s)	Server administrator access requires a unique user ID and password that is stronger than non-privileged users. This includes changing passwords on a more frequent basis than non-privileged users.		
Control Analysis	Stronger passwords are used in practice by administrators, but not technically enforced. However, users that have been assigned server administrator privileges must authenticate with Multi-Factor Authentication (MFA) prior to accessing servers in the data center.	**Reference**	16.02 16.03
		Results	Partially Exists
		Risk	Medium
Comment(s)	Even though MFA is required to access servers in the data center, Minnesota State should implement technical enforcement of longer passwords. This is intended to mitigate the risk of compromised credentials that could result in unauthorized access if MFA is bypassed.	**Priority**	Medium
2020 Management Response	Management accepts the risk. In the event that MFA fails, as a mitigating control, accounts are locked out after 10 attempts.		

Server Administrator Passwords	
Control Expectation(s)	Server administrator access requires a unique user ID and password that is stronger than non-privileged users. This includes changing passwords on a more frequent basis than non-privileged users.
2021 Management Response	Management accepts the risk. In the event that MFA fails, as a mitigating control, accounts are locked out after 10 attempts.
DRAFT 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 Plan (BCP) & Disaster Recovery Plan (DRP)			
Control Expectation(s)	The DRP is tested on a periodic basis for reliability by the organization to determine that technical infrastructure and application systems could be recovered within an acceptable time period by the business including consideration of relocating to an alternate location if the current facility is rendered unusable.		
Control Analysis	The BCP & DRP were not formally tested during FY2022. In addition, since there was no testing of either the BCP or DRP the existing Plans were not updated.	**Reference**	20.04 & 20.05 21.03 & 21.04
		Results	Does Not Exist
		Risk	Medium
Comment(s)	Minnesota State should test the BCP & DRP annually to ensure infrastructure and application systems could be recovered within a time period acceptable to the business.	**Priority**	Medium
2021 Management Response	Management agrees with this finding. A project has been started to mature DRP and BCP processes and documentation.		
DRAFT 2022 Management Response	Management agrees with this finding. 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.		

Physical Security			
Control Expectation(s)	Physical access activity is periodically reviewed by management. In addition, colocation data centers are notified of employee separation(s) with individuals authorized to access the colocation data centers periodically validated by management.		
Control Analysis	Physical access activity logs are available from each colocation data center but are not reviewed by management. Processes are in place to notify the colocation data center(s) when an authorized employee separates and validate authorized employees annually.	**Reference** **Results** **Risk**	22.05 / 22.06 / 22.07 Partially Exists Medium
Comment(s)	Management should review the current processes to notify the colocation data centers when an employee that is authorized to access the data centers separates. The periodic validation should occur timely to identify any individuals that did not get their authorization removed as part of a role change or separation. Physical access activity should be reviewed periodically to ensure no unauthorized resources accessed the EDC4 or EDC6 data centers.	**Priority**	Medium
2021 Management Response	Management agrees with this finding. 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.		
DRAFT 2022 Management Response	Management agrees with this finding. 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.		