OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Management and Budget

Statewide Integrated Financial Tools (SWIFT) Application Security Controls

Information Technology Audit

November 3, 2011 **Report 11-24**

FINANCIAL AUDIT DIVISION
Centennial Building – Suite 140
658 Cedar Street – Saint Paul, MN 55155
Telephone: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web site: http://www.auditor.leg.state.mn.us
Through Minnesota Relay: 1-800-627-3529 or 7-1-1

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

November 3, 2011

Representative Michael Beard, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

James Schowalter, Commissioner
Department of Management and Budget

This report presents the results of our audit of select security controls for the Statewide Integrated Financial Tools (SWIFT), the state's new accounting system. Development of the system was overseen by the Department of Management and Budget. This report contains four findings presented in the accompanying section of this report titled, *Findings and Recommendations*.

We discussed the results of the audit with the department's staff on October 10, 2011. Management's response to our findings and recommendations is presented in the accompanying section of this report titled, *Agency Response.*

The audit was conducted by Carolyn Engstrom CISA, CISSP (Audit Manager); David Westlund, CPA (Auditor-in-Charge); Chau Nguyen, CPA (Auditor), and Tracia Polden (Auditor).

This report is intended for the information and use of the Legislative Audit Commission and the management of the Department of Management and Budget. This restriction is not intended to limit the distribution of this report, which was released as a public document on November 3, 2011.

We received the full cooperation of the Department of Management and Budget's staff while performing this audit.

James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web Site: www.auditor.leg.state.mn.us • Through Minnesota Relay: 1-800-627-3529 or 7-1-1

Table of Contents

Report Summary

Conclusion

In overseeing the development of the state's new accounting system, Statewide Integrated Financial Tools (SWIFT), the Department of Management and Budget did not design adequate internal controls to safeguard state resources and data by identifying incompatible security access roles and limiting access based on employees' duties.

The department developed a generally adequate approach and identified milestones for updating the department's policies and procedures and its business contingency plan prior to the implementation of SWIFT. However, as of October 10, 2011, the department had not published the SWIFT policy and procedures to supersede the MAPS policy related to security access.

The department did comply with specific legal and financial accounting requirements related to project management and financial reporting for intangible assets.

Findings

- The Department of Management and Budget did not formally assess the level of security controls needed to ensure the integrity and confidentiality of SWIFT data, nor did it subsequently determine the adequacy of the security controls that were designed (Finding 1, page 7)

- The Department of Management and Budget did not provide agency security liaisons with sufficient information to make appropriate SWIFT access decisions; the department also allowed a weak method to authorize access. (Finding 2, page 8)

- The Department of Management and Budget did not sufficiently identify and communicate risks created by incompatible roles. (Finding 3, page 11)

- The Department of Management and Budget did not plan to assess the effectiveness of agencies' mitigating controls for incompatible security access, or they did not plan to implement a process to monitor that agencies' independently assessed the effectiveness of their mitigating controls for incompatible duties. (Finding 4, page 12)

Overview

On July 1, 2011, the Department of Management and Budget replaced the state's primary accounting system with a PeopleSoft Enterprise Resource Planning System designed to integrate administrative functions across state agencies, including human resources, payroll, financial transaction processing and reporting, procurement, and financial statement reporting. The new system is called the Statewide Integrated Financial Tools or SWIFT.

In 2006, an interagency team from the departments of Management and Budget and Administration conducted a feasibility study for an accounting system upgrade. The team performed a technical risk assessment of the existing accounting system, the Minnesota Accounting and Procurement System (MAPS), and concluded that there was a significant risk of system failure due to its outdated technology infrastructure and lack of vendor software updates. The interagency team also reviewed the experiences of many other states as a way to estimate the potential costs and benefits of a new system.

The analysis demonstrated that the state had a significant opportunity to improve the effectiveness of government operations by modifying its business processes and replacing MAPS with an integrated system. In January 2009, the state released a Request for Proposal to put the new system into operation. Following a competitive bidding process, the state contracted with MAXIMUS,[1] a consulting firm specializing in large system implementations.

The replacement project began in August 2009. The implementation team was composed of financial, procurement, technical, project management, and change management experts. Nearly 320 state employees and consultants worked on SWIFT project teams or served as subject matter experts. State agencies also assigned approximately 170 staff members as project sponsors, project managers, and readiness coordinators; many more employees participated as part of agency implementation teams. As of June 30, 2011, the department has expended approximately $43 million on the implementation of SWIFT.

[1] MAXIMUS, Inc.'s U.S.-based Oracle Peoplesoft ERP business was acquired by CherryRoad Technologies Inc. on September 30, 2010.

Objective, Scope, and Methodology

The objective of our audit was to answer the following questions:

- Did the Department of Management and Budget design adequate controls to safeguard state resources and data by identifying incompatible security access roles and limiting access based on employees' duties?

- Did the Department of Management and Budget develop an approach and identify milestones for updating the department's policies and procedures and its business contingency plan prior to the implementation of SWIFT?

- Did the Department of Management and Budget comply with specific legal and financial accounting requirements related to project management and financial reporting for intangible assets?

To answer these questions, we interviewed staff of the Department of Management and Budget and CherryRoad, the consultant. We assessed policies, procedures, and other relevant documentation, including security access training documentation, security role and permission documentation, security workflows, and the department's incompatibility matrix.

We used the guidance contained in Internal Control-Integrated Framework, published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission,[2] as our criteria to evaluate the manual controls. For further guidance on the COSO model, we used the Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government*. In addition, to assessing information technology security controls, we used *National Institute of Standards and Technology Special Publication 800-53*, *Recommended Security Controls for Federal Information Systems and Organizations*.[3] Finally, we used, as evaluation criteria, Minnesota Statutes and Rules and state policies and procedures established by the Department of Management and Budget and the Department of Administration.

[2] The Treadway Commission and its Committee of Sponsoring Organizations were established in 1985 by the major national associations of accountants. One of their primary tasks was to identify the components of internal controls that organizations should have in place to prevent inappropriate financial activity. The resulting *Internal Control-Integrated Framework* is the accepted accounting and auditing standard for internal control design and assessment.

[3] The National Institute of Standards and Technology *Special Publication 800-53*, *Recommended Security Controls for Federal Information Systems and Organizations* is considered to be the information security industry standard. The state's Office of Enterprise Technology uses this publication as a foundation for many of its standards and policies.

Conclusion

In overseeing the development of the state's new accounting system, Statewide Integrated Financial Tools (SWIFT), the Department of Management and Budget did not design adequate internal controls to safeguard state resources and data by identifying incompatible security access roles and limiting access based on employees' duties.

The department developed a generally adequate approach and identified milestones for updating the department's policies and procedures and its business contingency plan prior to the implementation of SWIFT. However, as of October 10, 2011, the department had not published the SWIFT policy and procedures to supersede the MAPS policy for security access.

The department did comply with specific legal and financial accounting requirements related to project management and financial reporting for intangible assets.

The following *Findings and Recommendations* section explains the deficiencies.

Findings and Recommendations

Finding 1

The Department of Management and Budget did not formally assess the level of security controls needed to ensure the integrity and confidentiality of SWIFT data, nor did it subsequently determine the adequacy of the security controls that were designed.

The Department of Management and Budget did not formally assess the level of security controls needed to ensure the integrity and confidentiality of SWIFT data. The department could have followed a process like the one outlined by the National Institute of Standards and Technology (NIST)[4] referred to as "security categorization." In that process, organizations separately assess the need for controls to ensure data's integrity, confidentiality, and availability based on the likelihood and impact of risk. The level of risk is categorized as high, moderate, or low. If the risk is categorized as "high," there is a need for robust controls and a greater need for assurance that controls are operating effectively. As result of the department not adequately assessing the level of security controls needed for SWIFT, the department had the following deficiencies:

- **Integrity** – Findings 3 and 4 report deficiencies in the way the department established employee system access, which is directly related to the integrity of the data within the system. Compromises to data integrity are prevented by limiting the ability to add, modify, or delete data and records to appropriate personnel, as well as segregating recording, custody, authorization, and reconciliation duties among individuals. Those privileges and restrictions are implemented in a system through its security access structure. If business operation requirements prevent the systematic segregation of privileges, controls should be developed and implemented to detect if such an intentional or accidental compromise occurred. These deficiencies may have been avoided if the department had incorporated security categorization procedures and implemented appropriate controls to ensure the integrity of the data within SWIFT. By adequately managing security access to enforce data integrity, the department can reduce the risk of inappropriate access, resulting in unauthorized modification or deletion of data and erroneous or fraudulent transactions.

[4] NIST is provided as an example. Other common risk management frameworks such as *OCTAVE and* International *Standards Organization (ISO) Standard 27005* and control frameworks *Control Objectives for Information Technology* and *NIST 800-53* all refer to confidentiality, integrity, and availability as a basis for assessing risks to systems and data.

- **Confidentiality**[5] – Although the department's staff stated that they identified and protected fields within SWIFT that would contain not public data,[6] they did not document the analysis and could not demonstrate how they used the analysis to address statutory requirements for data protection within the system.[7]

Security categorization is based on a simple and well-established concept - use security priorities for information systems to apply appropriate measures to adequately protect those systems. The security controls applied to a particular information system are proportionate with the potential adverse impact on operations, assets, individuals, and other organizations if there were a loss of integrity, confidentiality or availability.[8] By not explicitly categorizing the security requirements for SWIFT, the department increased the risk of implementing inadequate security controls within the application, which could result in unauthorized modification or disclosure of not public data.

Recommendation

- *The Department of Management and Budget should conduct a security categorization of SWIFT, document the results, and show how the analysis supports the SWIFT security program.*

Finding 2

The Department of Management and Budget did not provide agency security liaisons with sufficient information to make appropriate SWIFT access decisions; the department also allowed a weak method to authorize access.

The department delegated to the agencies the responsibility to determine the specific security roles for their employees and required each agency to designate a security liaison. The department had the following weaknesses in the way it implemented the process for agency employees to access SWIFT:

- The department did not clearly define the responsibilities of "requestor" and "approver" to ensure that agencies created an appropriate approval structure for system access. Generally, the "requestor" should be able to

[5] The term "confidentiality" is not meant to be interpreted in the narrow context of *Minnesota Statutes* 2010, Chapter 13. It is intended to mean the broad process of restricting the ability to view data that should be limited to a need to know basis in accordance with the data classification.
[6] Data fields in SWIFT could include a variety of not public data, such as social security numbers, names of benefit recipients, vendor and benefit recipient banking information, and employees' home addresses.
[7] *Minnesota Statutes* 2010, Chapter 13, Government Data Practices, generally defines most government data as public, but also categorizes not public data as confidential, private, nonpublic, or protected nonpublic. The statute requires the state to establish "appropriate security safeguards" to protect not public data from unauthorized access.
[8] National Institute of Standards and Technology *Special Publication 800-53*, *Recommended Security Controls for Federal Information Systems and Organizations* - 3.2 Categorization.

verify that the requested access met and is limited to the specific job responsibilities of the user, and the "approver" should be the data owner who can verify that access requests met certain criteria.[9]

- As of October 10, 2011, the department had developed, but not published, the 1101-07 Security and Access Operating Policy, 1101-07-01 Agency Security Administrators Procedures and 1107-07-02 Compensating Controls Procedures to supersede MMB MAPS Operations and Programming Policy and Procedures 1101-01, 1101-02, and 1101-07. The purpose of the policy and procedures is to establish the responsibilities agencies must execute as a part of establishing security access for their employees in SWIFT.

- The department did not require security liaisons to complete a comprehensive training program prior to performing their assigned duties.[10] A comprehensive training program should include applicable policies, the importance of the separation of incompatible duties or roles, separation of rights granted by security roles, available tools, and security access reports. On August 15, 2011, a month and a half after SWIFT's July 1, 2011, implementation date, the department directed security liaisons to an online training module that only addressed basic administrative functions, such as how to complete certain forms, reset passwords, reroute transactions, and remove roles. In addition, the department did not verify that security liaisons had completed any training and understood their roles and responsibilities prior to granting them the authority to approve access requests.

- The security role descriptions published by the department on June 15, 2011, did not sufficiently describe the functionality provided by the 119 security roles available to all agencies. Security role descriptions are a primary tool for security liaisons, and for those who approve security access, to help them make good decisions about appropriate security roles for employees within their agencies. Because employees assigned as security liaisons may not be approving security access on a regular basis, it is important that reference documentation to explain the roles is sufficient for them to understand the functions provided by security roles and the incompatibilities created by role combinations.

- The department did not accurately describe the agency security roles, limiting the ability for agency security liaisons to make appropriate employee access decisions. For the security role descriptions we tested, 12 of 27 had discrepancies between the role description and the actual access

[9] National Institute of Standards and Technology *Special Publication 800-53*, AC-2: Account Management and AC-3: Access Enforcement.

[10] National Institute of Standards and Technology *Special Publication 800-53*, AT-3 Security Training.

provided by the role. For example, the department's description of the security role "voucher entry" only stated that it provided the user with the ability to create a payment voucher; however, the role also allowed the user to override controls intended to ensure that payments are authorized and accurate. Because of the inaccurate description, security liaisons could inadvertently provide employees with access they did not intend.

- SWIFT Security Access Request Forms allow security liaisons to copy, or "mirror," one employee's access to another. This practice is not consistent with the principle of "least privilege," which expects that the access of each employee is limited to the needs of specific job duties.[11] Basing one employee's access on the access of another employee assumes that the copied access was appropriately designed initially, and the new employee's duties exactly match those of the copied employee. If these assumptions are not true, there is a risk that employees may inadvertently be granted excessive access. While mirroring access is quick and easy, it bypasses explicit documentation of the employee's authorized security roles. Although agencies could detect the excessive access through their annual reviews and recertifications of SWIFT security access, the excessive access would exist for an unacceptably long period.

The integrity of the financial data in SWIFT, or any application, depends initially on the careful design of security roles. Regardless of how well designed security roles are, security access can be rendered ineffective if the individuals requesting and approving security access do not understand what each role can do, the implications of assigning certain roles, the potential impacts of setting up one employee's access by copying another employee's access, the importance of periodic access review, and the risks of incompatible duties. Without adequate training, documentation of roles, or business rules, it would be difficult for the security liaisons to adequately execute their approval responsibilities.

Recommendations

- *The Department of Management and Budget should define the responsibilities for agency staff requesting and approving security access.*

- *The Department of Management and Budget should develop a comprehensive training program for agency security liaisons and ensure that the liaisons completed the training before granting the authority to approve requests.*

[11] National Institute of Standards and Technology *Special Publication 800-53*, AC-6 Least Privilege.

- *The Department of Management and Budget should review and revise security role descriptions to ensure they provide sufficient information about the role and accurately reflect the actual access provided by the roles so that properly trained approvers and security liaisons could make appropriate security access decisions.*

- *The Department of Management and Budget should require security liaisons to authorize specific security roles for each employee instead of copying another employee's access; alternatively, the department could require agencies to review and recertify security access more often than annually.*

Finding 3

The Department of Management and Budget did not sufficiently identify and communicate risks created by incompatible roles.

The department did not sufficiently identify or communicate incompatibilities of SWIFT security roles to agency security liaisons because it based its role analysis on preliminary information, rather than actual role permissions, did not consider incompatibilities between role types, and did not clearly communicate its expectations for agencies to limit assigning incompatible roles to employees.

SWIFT security liaisons authorized access to SWIFT by assigning an employee one or more security roles. Each role had one or more security permissions, which are the basic building blocks of access to SWIFT. It is the permissions assigned to the security access roles that determined the access actually granted by the role and allowed the user to view and modify different screens within SWIFT.

The department classified each security role into three distinct types: The **agency** role is for regular transaction processing, the **central** role is for department staff providing agency assistance, and the **SWIFT** role is for employees performing system maintenance duties. The department also categorized the security roles according to four main functions - approval, recording, reconciliation, and custodian. Combinations of role types or functions result in access incompatibilities.

In March 2011, the department's Internal Control and Accountability Unit analyzed agency type security roles based on design documentation and business process workflow diagrams. The purpose of the analysis was to identify and communicate to agency security liaisons the combinations of security agency roles that would result in employees having incompatible access. The department suggested, but did not require, that agencies avoid assigning employees security role combinations identified as incompatible by its analysis. This proactive analysis showed the department's recognition of the risk of incompatible access and its desire to limit the state's exposure to that risk. However, the department's

staff told us they did not plan to revise the analysis after user testing was performed in March and April 2011 and the department accepted the final permissions and roles from the consultant on May 25, 2011, or to expand the analysis to include central and SWIFT type roles.

Based on data provided to us as of May 25, 2011, our analysis of the 124 roles and the 256 permissions assigned to those roles identified 40 security roles and 10 security permissions that appeared to be inherently incompatible (an incompatibility existed without the assignment of another permission or role). At the time of the audit, the department could not provide documentation to show that the roles were not incompatible or resulted in a low potential risk. In addition, 84 agency permissions within the 40 agency roles were also assigned to 15 SWIFT or central type roles; an additional 11 SWIFT permissions were assigned to 4 agency roles. Because of the unique operational needs of each role type, the department did not intend for one role type to include permissions of another role type.

Agencies assigned about 2,000 employees with combinations of security roles that the department's analysis had identified as being incompatible based on the May 25, 2010 data. In addition, agencies assigned about 1,800 additional employees with security roles that had potential incompatibilities identified in our testing of the roles at the permission level, bringing the total of employees with SWIFT incompatibilities to about 3,800. Limiting system access incompatibilities is a fundamental internal control to prevent fraud.[12] Incompatible access would allow one employee the ability to complete a transaction without involving other employees to ensure the accuracy and validity of the transaction. By not providing complete information about incompatibilities and clear direction to agencies to avoid authorizing incompatible roles to employees, an unacceptable number of employees had incompatible SWIFT access when it began operations.

Recommendation

- *The department should expand its analysis of SWIFT security access roles to identify and communicate incompatibilities that exist at the permission level within and between roles and role types.*

Finding 4

The Department of Management and Budget did not plan to assess the effectiveness of agencies' mitigating controls for incompatible security access; they also did not plan to implement a process to monitor that agencies' independently assessed the effectiveness of their mitigating controls for incompatible duties.

The department did not help agencies avoid authorizing incompatible security roles or ensure that the agencies designed effective internal controls to mitigate

[12] Government Accountability Office – *Internal Control Management and Evaluation Tool*.

the risks created by the incompatibilities. As discussed in Finding 3, about 3,800 employees had security roles that created real or potential incompatibilities, based on the May 25, 2011 data. Incompatibilities without effective mitigating controls could allow error or fraud to occur without detection. Larger agencies should be better able to separate incompatible security roles among its employees; smaller agencies may not be able to separate incompatible security roles and will need to have effective mitigating controls. Although the department's Internal Control and Accountability Unit suggested in a bulletin that agencies develop and document mitigating controls over incompatible access, it did not plan to review the existence and effectiveness of those controls.[13] Instead, the unit asserted that its role was to provide guidance, including developing policies, and agencies had the responsibility to ensure compliance. Based on the historical inability of agencies to appropriately limit incompatibilities or design effective mitigating controls, it is unlikely that agencies will successfully reduce the risks created to an acceptably low level.[14]

State statutes require the Department of Management and Budget to provide internal control support to agencies.[15] By not planning to evaluate the design and effectiveness of the agencies' mitigating controls nor planning to monitor that agencies' had independently assessed the effectiveness of their mitigating controls, the department cannot be assured that the state had adequately reduced the risks created by incompatible system access, including the risk of fraud and error not being detected, and the controls that were designed to prevent errors and fraud were operating as intended to provide accurate financial information used to compile the state's financial statements.

Recommendation

- *The department should develop a process to evaluate the effectiveness and operation of mitigating controls over system incompatibilities implemented by other state agencies. Alternatively, the department should develop a process to monitor that agencies have conducted an evaluation of the effectiveness and operation of the agency's mitigating controls over system incompatibilities.*

[13] Department of Management and Budget, Internal Control and Accountability Unit's March 2011 Internal Controls Bulletin, "*Security Role Assignments Impact Internal Controls.*"

[14] The existence of incompatible access without effective mitigating controls is a common finding in our audits of state agencies. See the following Office of the Legislative Auditor's Financial Audit Division reports as examples: 10-01, *Report on Internal Control Over Statewide Financial Reporting*, issued February 11, 2010, (Finding 2); 11-02, *Report on Internal Control Over Statewide Financial Reporting*, issued January 13, 2011, (Finding 2).

[15] *Minnesota Statutes* 2010*,* 16A.057, subdivisions 3 and 4.

MINNESOTA Management & Budget

November 1, 2011

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
140 Centennial Office Building
658 Cedar Street
St. Paul, Minnesota 55155

RE: SWIFT Information Technology Audit

Dear Mr. Nobles:

Thank you for the opportunity to discuss your findings on the SWIFT Information Technology audit. We are committed to strong financial controls and we value suggestions to make our existing processes even stronger. Strong security capabilities were an important part of our system requirements when selecting the SWIFT system software and we have worked hard to implement a comprehensive security solution. Since your audit work was done in the April-June 2011 timeframe, while the implementation work was still underway, considerable changes have been made in a number of areas, both before and since the July 1, 2011 go live.

Recommendation – Finding 1

The Department of Management and Budget should conduct a security categorization of SWIFT, document the results, and show how the analysis supports the SWIFT security program.

Response:

Although we have not conducted a formal security categorization, as proposed by NIST 800-60, we believe that we have adequately addressed the integrity, confidentiality, and availability concerns of SWIFT. We understand that each SWIFT module has unique impact levels, depending on the purpose and use of the module, and have considered those impacts when designing SWIFT security. We also understand that some of the SWIFT modules contain specific information elements, such as vendor, client, or banking information that also affect impact levels. We believe that SWIFT security, as it has been designed, sufficiently manages the impact levels we consider to be high. We also acknowledge that at some future time, more formally documenting our risk and security decisions using a tool such as NIST 800-60 may be considered.

Person responsible: Lori Mo
Estimated completion date: June 2012

400 Centennial Building • 658 Cedar Street • St. Paul, Minnesota 55155
Voice: (651) 201-8000 • Fax: (651) 296-8685 • TTY: 1-800-627-3529
An Equal Opportunity Employer

Recommendation – Finding 2

The Department of Management and Budget should define the responsibilities for agency staff requesting and approving security access.

The Department of Management and Budget should develop a comprehensive training program for agency security liaisons and ensure that the liaisons complete the training before granting the authority to approve requests.

The Department of Management and Budget should review and revise security role descriptions to ensure they both accurately reflect the actual access provided by the roles and provide sufficient information about the role so that properly trained approvers and security liaisons could make appropriate security access decisions.

The Department of Management and Budget should require security liaisons to authorize specific security roles for each employee instead of copying another employee's access; alternatively, the department could require agencies to review and recertify security access more often than annually.

Response:

Minnesota Management and Budget, in conjunction with its primary vendor and state agencies, worked to define and set up security through a comprehensive process beginning in the spring of 2010. In addition to the security administrators in place at state agencies, SWIFT had a dedicated project security team working to empower agencies with the information and resources they needed to set up security through June 2011; since May, a permanent security team of four at MMB have been managing security processes, policies and building the capacity of agency security administrators to protect the integrity of the state's new financial systems. The SWIFT team provided agency security liaisons with a series of documents, web based seminars, and live workshops to communicate the extensive security information related to the new system including roles, risks, permissions and potential conflicts prior to go-live.

Prior to go live, we addressed the high risk issues related to roles and permissions. The online materials provided in August related only to delegated authority of some limited administrative functions. In our decision to allow security administrators to "mirror" one employee's access to another, we considered both the risks of excessive access with the alternate risk of errors when mirror access is appropriate. As you suggest, we will evaluate the benefits of more frequent recertification for high risk access roles.

Minnesota Management and Budget recognizes that the effectiveness of the state's new accounting and procurement system hinges on a sound security process. Moving forward we will update security documentation as changes are made and will develop training for ongoing agency security administrators.

Person responsible: Carol Stein
Estimated completion date: February 2012

Recommendation – Finding 3

The department should expand its analysis of SWIFT security access roles to identify and communicate incompatibilities that exist at the permission level within and between roles and role types.

Response:

Knowing the importance of security and access to the new SWIFT system, MMB's Internal Control and Accountability Unit performed a review of preliminary agency security roles, based on information sent to agencies on October 2010. At the time of that review, we knew that security roles would continue to evolve. However it was our intent to provide agencies with an early indication of which roles might theoretically provide conflicts. The security role conflict matrix, along with guidance on compensating controls, was provided to agencies prior to their final review and approval of security roles in May 2011.

Substantial work to address any conflicting permissions was performed by agencies and central staff during the June timeframe, prior to the system going live July 1, 2011, and the process has continued to be improved since July. In some instances, our review has determined that the roles in question includes less significant permissions, such as the ability to set up projects within the system or update an organization's address. We have determined some combinations are acceptable, when paired with the related workflow, which requires approval for every transaction.

Now that the system has been implemented, it is the department's intent to reevaluate the security roles and provide updated guidance to agencies. We also intend to have security administrator's review and certify to all current employee security roles within their departments, both those granted through the SWIFT implementation process (MTK) or granted subsequent to go-live. This process will allow agencies to verify all SWIFT security roles given to their employees to date. We also plan to repeat the recertification at least annually.

Person responsible: Carol Stein and Barb Shlaefer
Estimated completion date: January 2012

Recommendation – Finding 4

The department should develop a process to evaluate the effectiveness and operation of mitigating controls over system incompatibilities implemented by other state agencies.
Alternatively, the department should develop a process to monitor that agencies have conducted an evaluation of the effectiveness and operation of the agency's mitigating controls over system incompatibilities.

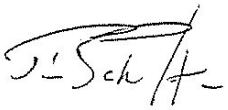
Response:
The department has issued a Security and Access Policy, designed to assist agencies in maintaining adequate internal control systems. We have also issued a companion procedure, specifically relating to

compensating controls. Although we believe that agencies are primarily responsible for their own internal control systems, pursuant to Minn. Stat. Section 16A.057, we are available to assist individual agencies with designing and implementing compensating controls that provide sufficient review and oversight of incompatible activities.

Person responsible: Jeanine Kuwik
Estimated completion date: Complete

Thank you for your recommendations. We value your audit work and the improvements it generates further improve our financial management practices.

Sincerely,



Jim Schowalter
Commissioner