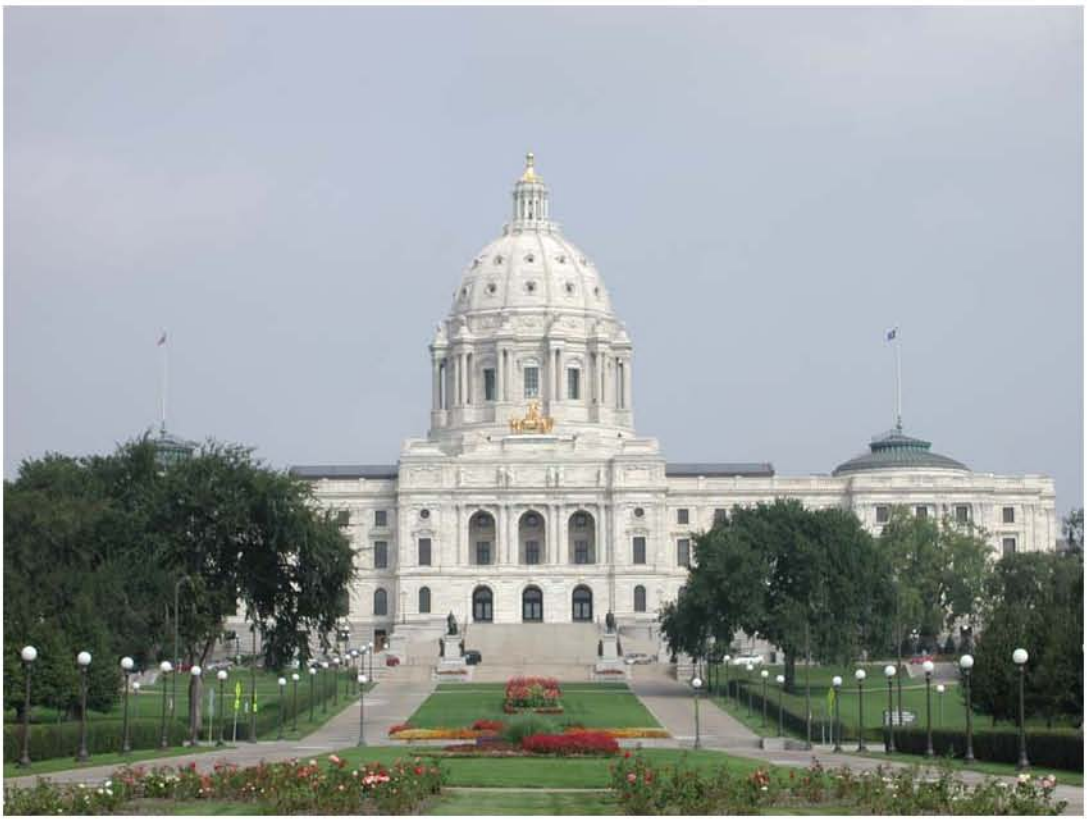
O L A

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Departments of Employee Relations and Finance

SEMA4 Personnel and Payroll Controls



January 23, 2007 **07-01**

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota state government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately forty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of representatives and senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

To obtain a copy of this document in an accessible format (electronic ASCII text, Braille, large print, or audio) please call 651-296-1235. People with hearing or speech disabilities may call us through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

All OLA reports are available at our web site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, or evaluation, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

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

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Ms. Patricia Anderson, Commissioner
Department of Employee Relations

Mr. Tom Hanson, Commissioner
Department of Finance

We have conducted an audit of the State Employee Management System (SEMA4). The scope of our audit focused on application controls that help ensure personnel and payroll transactions are accurately and completely processed and recorded. The Report Summary highlights our overall conclusion. Our specific audit objectives and conclusions are contained in Chapter 2 of this report. The audit report contained six findings related to internal control weaknesses.

We would like to thank staff from the departments of Employee Relations and Finance for their cooperation during this audit.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Cecile M. Ferkul

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

End of Fieldwork: October 3, 2006

Report Signed On: January 22, 2007

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 • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

Cecile Ferkul, CPA, CISA	Deputy Legislative Auditor
Eric Wion, CPA, CISA, CISSP	Audit Manager
Mark Mathison, CPA, CISA	Auditor-In-Charge
John Kelcher	Auditor
Carl Otto, CPA, CISA	Auditor
Ching-Huei Lee, CPA	Auditor
Xin Wang	Auditor

Exit Conference

We discussed the findings and recommendations with the following representatives of the departments of Employee Relations, Finance, and the Office of Enterprise Technology at the exit conference held January 5, 2007:

Department of Employee Relations

Wendy Dwyer	Assistant Commissioner
Paul Larson	Deputy Commissioner
Steve Jorgenson	Chief Information Officer
Laurie Hansen	Human Resources Division Manager

Department of Finance

Tom Hanson	Commissioner
Lori Mo	Assistant Commissioner, Accounting and Information Services
Jean Henning	Chief Information Officer
Mary Muellner	Payroll Director
John Vanderwerf	SEMA4 Technical Director

Office of Enterprise Technologies

Chris Buse	Chief Information Security Officer
Mark Mathison	Information Technology Compliance Manager

Departments of Employee Relations and Finance
SEMA4 Personnel and Payroll Controls

Report Summary

Conclusion:

The departments of Employee Relations and Finance had controls to ensure that employee pay and accrual rates are correct. The departments also had controls to ensure that the payroll is accurately processed and recorded in the state's accounting system. However, as highlighted in the next section, we identified some internal control deficiencies.

Key Findings:

- The departments of Employee Relations and Finance have not developed a comprehensive plan and process to manage personnel and payroll-related risks. (Finding 1, page 6)

- The Department of Employee Relations' criteria for delegating personnel duties were not well defined. (Finding 3, page 8)

- The departments of Employee Relations and Finance have not adequately limited the ability of employees to perform incompatible payroll and personnel transactions in SEMA4. (Finding 4, page 9)

The audit report contained six findings relating to internal control weaknesses.

Audit Scope:

We assessed SEMA4 application controls as of October 2006.

Background:

During fiscal year 2006, the state processed personnel and payroll transactions for over 50,000 employees, resulting in total payroll and business expenses that exceeded $3 billion.

The state administers its personnel and payroll responsibilities through individual state agencies and two central oversight agencies: the departments of Employee Relations and Finance. The Department of Employee Relations provides support for personnel functions, and the Department of Finance oversees payroll processing. Both departments maintain the central personnel and payroll system, called the State Employee Management System (SEMA4).

This page intentionally left blank.

Chapter 1. Introduction

The state administers its personnel and payroll responsibilities through each state agency and the two central oversight agencies: the departments of Employee Relations and Finance. These oversight agencies maintain the central personnel and payroll system, called the State Employee Management System (SEMA4). In general, Employee Relations provides support for personnel functions, and Finance oversees payroll processing. However, due to the interrelationship between personnel and payroll activities, the departments closely coordinate their efforts. During fiscal year 2006, SEMA4 processed transactions for over 50,000 employees, resulting in total payroll and business expenses that exceeded $3 billion.

SEMA4 has edits to help ensure personnel and payroll transactions comply with legal provisions and terms in bargaining agreements. The system also has extensive on-line policies and procedures to help state agencies record and process transactions. However, individual state agency staff are ultimately responsible for understanding and complying with compensation plan terms and other pertinent legal provisions. The departments of Employee Relations and Finance monitor select personnel and payroll activities to help ensure compliance.

This audit assessed the adequacy of key application controls that help ensure personnel and payroll transactions are accurately and completely processed and recorded. Application controls filter out invalid data before it can be processed and ensure that remaining transactions are completely and accurately processed. Application controls include both manual procedures, such as reconciliations and computerized edits.

Audit Approach

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. These standards require that we obtain an understanding of internal controls relevant to the audit objectives. These standards also require that we plan our work to provide reasonable assurance that the departments complied with financial-related legal provisions that are significant to the audit. In determining compliance with legal provisions, we considered requirements of laws, regulations, and bargaining agreements.

We used the guidance contained in the *Control Objectives for Information and Related Technology (COBIT)*, as our criteria to evaluate controls.[1] We also used payroll and personnel policies and procedures to obtain evaluation criteria. Finally, we used information published by the vendors of the computer system to evaluate select controls.

[1] COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gaps among control requirements, technical issues, and business risks. COBIT is published by the IT Governance Institute, a research think tank that exists to be the leading reference on IT-enabled business systems governance.

This page intentionally left blank.

Chapter 2. Application Controls

Chapter Conclusions

The departments of Employee Relations and Finance had controls to ensure that employee pay and leave accrual rates are correct. The departments also had controls to ensure that the payroll is accurately processed and recorded in the state's accounting system. However, the departments could improve internal controls in some areas. For example, as explained in Finding 1, the departments have not developed a comprehensive plan and process to manage personnel and payroll-related risks. Findings 2 through 3 discuss additional personnel or payroll control deficiencies. Finally, Findings 4 through 6 describe some security-related weaknesses.

Application controls are controls over the input, processing, and output of data. Application controls are important because they help ensure that only complete, accurate, and valid data is processed. These controls include computerized edits and manual procedures, such as the review of computer generated exception reports. The personnel and payroll system was built and distributed by a well-known and reputable vendor. The product comes standard with many embedded computerized edits, controls, and reports. When first implemented, the departments of Employee Relations and Finance added edits, controls, and reports to customize the product to the unique needs of the state. To save money and make future upgrades of the product more efficient, management of the departments decided to significantly reduce the number of customized edits in 2003. Accordingly, since many of the customized controls no longer exist, manual detective controls have taken on much more significance.

The Department of Employee Relations has many controls to ensure that people are paid the appropriate pay rates. Of greatest significance, internal tables in SEMA4 define the negotiated salary ranges for most positions in state government. When agencies use the system to assign an employee to a job, SEMA4 ensures that the pay rate is within the pay range in these control tables. The department also monitors select transactions.

The Department of Finance has controls to verify the accuracy of the bi-weekly payroll processing. Payroll officers in each state agency enter their employees' hours worked and leave taken at the end of each pay period. SEMA4 uses this data to calculate the gross pay, deductions, and net pay for the state workforce. The system also posts accounting transactions to the state's accounting system. Numerous internal tables in SEMA4 help control these processes. The department also produces many reports that allow agency staff to detect processing errors before the state actually pays employees. Finally, the department performs important reconciliations to ensure that payroll is accurately recorded in the accounting system, and amounts disbursed to employees are accurate.

Departments of Employee Relations and Finance
SEMA4 Personnel and Payroll Controls

Our review of application controls focused on the adequacy of personnel and payroll processing controls. Specifically, we designed our work to answer the following questions:

- Did the departments of Employee Relations and Finance have adequate controls to ensure that employee pay and leave accrual rates are accurate and comply with bargaining agreements?

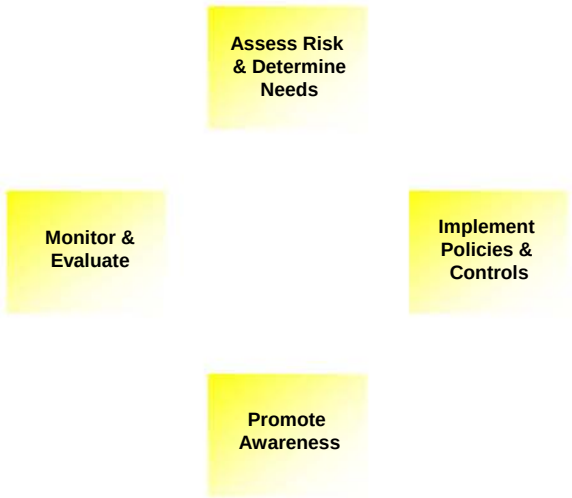
- Did the departments of Employee Relations and Finance have adequate controls to ensure that the biweekly payroll is completely and accurately processed and recorded in the state's accounting system?

Current Findings and Recommendations

1. The departments of Employee Relations and Finance have not developed a comprehensive plan and process to manage personnel and payroll-related risks.

The departments have not developed a formal methodology to conduct risk assessments. Risk assessments are a means of providing decision makers with information needed to understand factors that can negatively influence operations allowing them to make informed judgments concerning the extent of actions needed to reduce risk. A risk assessment is one element of a broader set of risk management activities, collectively referred to as the "risk management cycle." Other elements include implementing appropriate policies and related controls, promoting awareness, and monitoring and evaluating the effectiveness of those policies and controls. While all elements are important, risk assessments provide the foundation for all other elements of the cycle. Since risks change over time, it is important for organizations to periodically reassess risks and reconsider the appropriateness and effectiveness of the existing policies and controls. Figure 2.1 illustrates this continuous risk management cycle. The departments will need to perform this process of assessing risks and selecting controls for each important business process.

Figure 2.1
Risk Management Cycle



Source: Auditor prepared based on the U.S. Government Accountability Office's *Executive Guide, Information Security Management, Learning From Leading Organizations.*

Although a formal risk assessment methodology has not been adopted, risks have not been ignored. For example, the Department of Employee Relations has a small team that reviews bi-weekly reports to monitor state agency personnel transactions. However, the department had not documented the expectations of the review, including who should perform the review, what they should monitor,

when they should perform the review, and what action they should take if they identify exceptions. A formal risk assessment process would have specified this type of information. The bi-weekly reports often included all transactions for all agencies and did not highlight exceptions or riskier transactions that may require more review. In addition, staff did not document actions taken because of the monitoring efforts. Accordingly, the department does not have the information it needs to determine whether the reviews are effective.

Similarly, it was difficult to determine what controls the departments of Employee Relations and Finance expected to be in place at other state agencies. The departments have not provided agencies adequate guidance and reports that focus on riskier transactions and desired controls. For example, a policy requires agencies to verify all personnel and payroll transactions have been correctly processed. A corresponding procedure requires agency personnel to review a report called the "Payroll Register" each pay period to verify transactions are correct. However, the procedure does not stipulate what specifically should be reviewed, why, and by whom. The Payroll Register report contains all payroll transactions for an agency and includes such things as employee names, position, pay rates, hours, and amounts paid. It does not highlight transactions that may merit review to ensure proper authorization and accuracy. For example, the report does not highlight new employees, pay rate increases, or other transactions that may require review by someone independent of the process to ensure they were authorized and appropriate.

Since personnel and payroll responsibilities are shared between the departments of Employee Relation, Finance, and other state agencies it is important to have a formal process to manage risks and clearly define who should do what, when, and why to mitigate those risks.

Recommendation

- *The departments should develop a comprehensive plan and process to manage personnel and payroll-related risks.*

2. The departments of Employee Relations and Finance have not implemented adequate controls to prevent unauthorized transactions.

The departments have not implemented controls in SEMA4 to prevent unauthorized transactions. Transactions entered by personnel and payroll officers require authorization from others with the authority to make personnel and payroll decisions. However, the way the departments use SEMA4, it does not require evidence of that approval before it processes the transactions. Since transaction authorization is a fundamental personnel and payroll control, it is better to prevent erroneous or fraudulent transactions from happening rather than relying on detecting them after they occur.

SEMA4 has the capability (called Workflow) to automate, streamline, and control the flow of information to better manage business processes. Online approvals through Workflow would provide more effective controls to ensure that agencies obtained the appropriate authorization for transactions and would eliminate the need for less effective detective controls. For example, if a

transaction required approval, SEMA4 would automatically route the transaction to the designated person and would not process it until it was approved. Similarly, if a Department of Employee Relations' representative and an agency head must first approve the transaction, processing of the transaction would not occur without obtaining both approvals.

Recommendation

- *The departments should explore using online approvals to ensure that personnel and payroll transactions are authorized.*

3. The Department of Employee Relations' criteria for delegating personnel duties were not well defined.

The commissioner of Employee Relations is the chief personnel and labor relations manager for the executive branch. To fulfill these duties, *Minnesota Statutes* give the commissioner of Employee Relations the authority to delegate certain responsibilities to individual state agencies. The department generally based its decision to delegate duties to agencies on several factors. The primary factor was whether an agency had an adequate system of internal controls over personnel processes and had personnel staff skilled and knowledgeable about policies and procedures. However, the department had not developed objective and specific criteria to evaluate these factors either when initially delegating authority or periodically thereafter.

The Department of Employee Relations primarily based its evaluation of someone's knowledge and skills on their personal experiences in working with the agency employee. The department should establish objective criteria to gauge an agency employee's level of knowledge and skills pertinent to applicable bargaining agreements, laws, and SEMA4. For example, the successful completion of a series of SEMA4 training classes, as well as classes that cover applicable bargaining agreement and personnel laws, could be one such criterion. Requiring additional periodic training to maintain the delegation may also be appropriate to ensure that the agency remains competent to perform the delegated duties.

Recommendations

- *The department should develop objective criteria to evaluate delegation decisions.*

- *The department should develop a process to reassess delegation decisions on a periodic basis.*

4. The departments have not adequately limited the ability of employees to perform incompatible payroll and personnel transactions in SEMA4.

Over 120 state employees have the ability to perform incompatible payroll and personnel transactions in SEMA4. SEMA4 has distinct payroll and personnel security profiles that provide the ability to separate incompatible duties and help prevent erroneous or fraudulent transactions.

Some small agencies have limited staff and may not be able to avoid incompatible access for their employees. The departments of Employee Relations and Finance should explore options for these agencies. For example, Employee Relations and Finance could centrally provide payroll or personnel services, or small agencies could pool their resources to share such services.

Nearly half of the 120 employees with incompatible access worked for the departments of Human Services, Natural Resources, and Transportation. Although these agencies may have developed mitigating controls, they have sufficient staff to separate incompatible duties. Because this is such a fundamental control, the departments of Employee Relations and Finance should not allow large agencies to have incompatible access to SEMA4 and should require them to make changes to their processes that would allow them to adequately separate duties.

Finally, the departments of Employee Relations and Finance have not defined the required mitigating controls for those agencies that cannot separate duties. Typically such controls should require an independent person to review transactions entered by the individual with incompatible access and obtain sufficient evidence to ensure the transactions were authorized and appropriate.

Recommendations

- *The departments of Employee Relations and Finance should explore options and work with state agencies to minimize employees' incompatible access.*

- *The departments of Employee Relations and Finance should define the mitigating controls needed by agencies when incompatible access exists.*

5. The departments of Employee Relations and Finance stored account names and passwords in plain text in computer programs that was accessible by a large number of people.

Eight computer programs contained account names and passwords in plain text. The programs use these accounts and passwords to logon to internal computers and perform miscellaneous tasks. Because the programs store the information in plain text, rather than encrypted, anyone with access to the programs could read the contents. The accounts and passwords could potentially be used inappropriately and cause a service disruption. Over 20,000 accounts, belonging to people and programs, had the ability to read the contents of each of these programs. Only a few individuals or programs need to read the contents of programs.

Recommendations

- *The departments should remove or encrypt account names and passwords stored in programs.*

- *The departments should limit the ability to read the contents of programs to a few individuals who need the access to fulfill their job duties.*

6. Firewall rules did not restrict attempts to access SEMA4 personnel and payroll data to only those computers and individuals that needed such access.

The firewall rules did not adequately restrict attempts to access the SEMA4 database without going through the SEMA4 application. Only a few information technology staff working at the departments of Employee Relation and Finance need such access. The firewall did not restrict access to only those individuals. Instead, virtually any computer on the state's network could attempt to access the database. A firewall is an added layer of security used to prevent access attempts from unauthorized people and computers.

The Office of Enterprise Technology manages the firewalls that help protect state computer systems and data, including personnel and payroll data, from unauthorized access attempts. Each agency must work with the Office of Enterprise Technology to ensure firewalls are configured to protect their computer systems and data.

Recommendation

- *The departments of Employee Relations and Finance should work with the Office of Enterprise Technology to ensure firewalls adequately protect payroll and personnel data.*

Status of Prior Audit Issues
As of March 2006

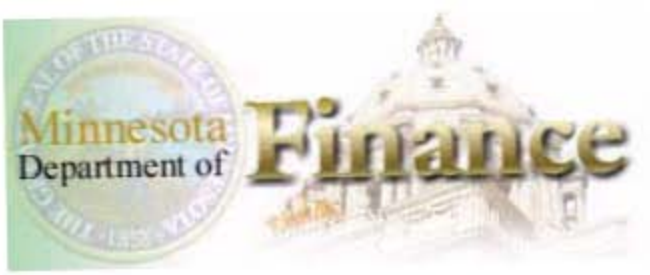
Most Recent Audit

Legislative Audit Report 04-36, issued August 31, 2004, assessed the adequacy of key application and general controls of the State Employee Management System (SEMA4). The report included five written findings related to computer security weaknesses. We did not follow up on these findings as part of our current audit because our scope examined application controls and not security controls.

State of Minnesota Audit Follow-Up Process

The Department of Finance, on behalf of the Governor, maintains a quarterly process for following up on issues cited in financial audit reports issued by the Legislative Auditor. The process consists of an exchange of written correspondence that documents the status of audit findings. The follow-up process continues until Finance is satisfied that the issues have been resolved. It covers entities headed by gubernatorial appointees, including most state agencies, boards, commissions, and Minnesota state colleges and universities. It is not applied to audits of the University of Minnesota, any quasi-state organizations, such as the metropolitan agencies, or the State Agricultural Society, the state constitutional officers, or the judicial branch.

This page intentionally left blank.



January 16, 2007

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street
140 Centennial Office Building
St. Paul, MN 55155-4708

Dear Mr. Nobles:

Thank you for the opportunity for our staff to discuss your audit finding with the individuals in your office responsible for the State Employee Management System (SEMA4) audit. We are committed to providing accurate financial and human resource information to state agencies, the legislature, and the public. We will continue to work toward improvements in our processes.

Finding 1: The departments of Employee Relations and Finance have not developed a comprehensive plan and process to manage personnel and payroll-related risks.

Recommendation: The departments should develop a comprehensive plan and process to manage personnel and payroll-related risks.

Response: We concur with the recommendation**.** Currently, the departments of Employee Relations and Finance do not have a formal risk assessment process in place. However, as this audit report states, the departments have not ignored business risks and have dealt with the risks in a number of ways. Employee Relations and Finance maintain and distribute policies and procedures, online help, and periodic memos to assist agency human resources and payroll staff. This documentation informs agency staff about existing processes and controls, provides reference material, and highlights current issues. Each department also has standard reports for agencies to review, as well as other reports, which agency staff may run on an as needed basis. In addition, both Employee Relations and Finance run centralized reports to identify transactions, which are causing system errors, or have been identified as potential problems.

The Office of the Legislative Auditor (OLA) has given examples for each department, where the auditors believe a formal risk assessment methodology would provide additional benefits. In each example cited, the departments have defined the processes in the form of statewide policies and procedures, internal procedures, or position descriptions. Detective controls exist as part of these processes. The audit findings suggest more could be done to promote awareness of potential risks to agency human resources and payroll staff by providing additional preventative controls in the form of system edits, or by providing reports or other tools to highlight specific transactions, where further review may be required.

Over the next twelve months, the departments of Employee Relations and Finance will work together to assemble a comprehensive plan to manage personnel and payroll-related risks. The plan will also include new or revised policies, procedures and reports that state agencies will use to raise their awareness of human resource and payroll related risks and outlines agency's roles in the process. The plan will define the process to monitor and periodically re-evaluate risks, as well as the needs associated with those risks. In addition, the plan document will include the frequency of the evaluation process.

The first step in the process of developing a comprehensive plan will be to assemble all of our existing documentation into one comprehensive reference document. Once this has been done, then we will assess the state of the existing documentation. The assessment will start at the beginning of the risk management cycle to ensure all relevant risks have been identified and documented. The plan will include a process for cost benefit analysis to determine when risks are acceptable, or need to be mitigated.

Next, the mitigating controls for the identified risks will be reviewed and additional documentation will be created as needed. Existing mitigating controls must be communicated to department staff, as well as agency human resources and payroll staff. Whenever feasible, the departments shall strive to implement additional preventative controls, or provide additional tools to agency staff, which may be used to highlight riskier transactions. The implementation of additional mitigating controls will be dependent upon cost benefit analysis and resource availability.

Finally, the plan will document areas where potential business risks have been identified; but due to the results of cost benefit analysis or resource availability, these risks have been deemed acceptable.

Person responsible: Laurie Hansen, Department of Employee Relations
Mary Muellner, Department of Finance
Implementation date: January, 2008

Finding 2: The departments of Employee Relations and Finance have not implemented adequate controls to prevent unauthorized transactions.

Recommendation: The departments should explore using online approvals to ensure that personnel and payroll transactions are authorized.

Response: We concur with the recommendation. There are existing policies, procedures, reports, and security controls currently in place designed to ensure that personnel and payroll transactions are properly authorized. But for many transactions, we rely on agency procedures for proper authorization, and documentation of those approvals is maintained in the individual agencies rather than in the central SEMA4 system. The availability of workflow functionality in our current version of the software provides for system resident controls where we did not previously have that option. With any system upgrade, one of our tasks is to assess the additional functionality offered by the software vendor and make decisions regarding what to implement within resource constraints. At the time of the most recent version upgrade (2003) we concluded that effort needed to implement the workflow option exceeded our resource availability. Since then, we have implemented the workflow function on a very limited basis in the areas of on-line time reporting and business expense approvals, and employee address change requests. In these areas we have found it to be a useful and efficient option. Expanded use of this functionality

needs to be evaluated for each process individually and a cost benefit analysis completed. While we don't anticipate that broader use of this feature would be technically difficult, substantial business analysis is needed to fully utilize the functionality and in some cases would require collection of data elements not currently maintained.

In the coming months we will be assessing the costs, benefits, and timing of another version upgrade; we will include expanded use of workflow in that analysis.

Person responsible: Jean Henning, Department of Finance
Steve Jorgenson, Department of Employee Relations

Implementation date: October 2007

Finding 3: The Department of Employee Relations' criteria for delegating personnel duties were not well defined.

Recommendations: The department should develop objective criteria to evaluate delegation decisions.

The department should develop a process to reassess delegation decisions on a periodic basis.

Response: We concur with the recommendation. We acknowledge the Legislative Auditor's concern that the Department of Employee Relations does not currently have objective and specific criteria to determine when to delegate certain responsibilities to individual state agencies. We have used more subjective criteria to determine whether agencies had an adequate system of internal controls and had personnel staff skilled and knowledgeable about policies and procedures. The Legislative Auditor suggests using knowledge of applicable bargaining agreements, laws, and SEMA4 as identified by completion of appropriate training. While these are essential factors, there are also more intangible factors, i.e., understanding the state's classification and compensation systems and using good judgment to determining their proper application, which is gained by quality experience in addition to training. While this has not created any problems for us in the past, recognizing the Legislative Auditor's concerns, we will better delineate objective criteria for how agencies can apply for delegation and what is needed to qualify for delegation by March 15, 2007.

In addition, the Legislative Auditor was concerned that the Department of Employee Relations does not have an ongoing process to reassess delegation decisions on a periodic basis. While we have reviewed and removed agencies' delegated authority on an as-needed basis, we recognize the Legislative Auditor's concerns and will develop a more systematic process for reviewing our delegation decisions in the future. This process will be developed by June 1, 2007.

Person responsible: Chad Thuet, Department of Employee Relations
Laurie Hansen, Department Employee Relations

Implementation date: March 15, 2007 regarding delegation criteria; June 1, 2007 regarding on-going assessment process.

Finding 4: The departments have not adequately limited the ability of employees to perform incompatible payroll and personnel transactions in SEMA4.

Recommendation: The departments of Employee Relations and Finance should explore options and work with state agencies to minimize employees' incompatible access.

The departments of Employee Relations and Finance should define the mitigating controls needed by agencies when incompatible access exits.

Response: We concur with the recommendation. While we have been working in close cooperation with the OLA on incompatible access for a number of years, we recognize the need to continue to separate payroll and human resource functions. SEMA4 has distinct payroll and personnel security profiles that provide agencies with the ability to separate incompatible duties. The departments will review the separation of human resources and payroll functions and the information and analysis will be incorporated into the earlier finding related to the risk assessment.

The departments will explore options for both small and large agencies and develop models agencies can use to separate payroll and personnel functions. In addition, the departments will create or update policies, procedures and reports that agencies will use to guide them in the separation of these functions.

The departments will also research how the various small agencies are currently handling their payroll/personnel services. We will determine if there are opportunities for small agencies to partner with another small agency to share payroll/personnel services or determine if a small agency could partner with a large "sister" agency to provide these functions. We will also review the feasibility of Employee Relations and Finance's ability to centrally provide payroll or personnel services to small agencies.

Finally, the departments will work to define the required mitigating controls for those agencies who cannot separate duties.

Person responsible: Laurie Hansen, Department of Employee Relations
Implementation date: September 2007

Finding 5: The departments of Employee Relations and Finance stored account names and passwords in plain text in computer programs that was accessible by a large number of people.

Recommendation: The departments should remove or encrypt account names and passwords stored in programs.

The departments should limit the ability to read the contents of programs to a few individuals who need the access to fulfill their job duties.

Response: We concur with the recommendation and have removed the user names and passwords from all programs.

Person responsible: John Vanderwerf, Department of Finance

Implementation date: Completed

Finding 6: Firewall rules did not restrict attempts to access SEMA4 personnel and payroll data to only those computers and individuals that needed such access.

Recommendation: The department of Employee Relations and Finance should work with the Office Enterprise Technology to ensure firewalls adequately protect payroll and personnel data.

Response: We concur with the recommendation and have discussed the issue with the Office of Enterprise Technology (OET). OET also concurs with the finding and will take steps to ensure that access to the SEMA4 database is restricted to only those individuals who need such access to fulfill their job duties.

Person responsible: Mark Mathison, Office of Enterprise Technology.

Implementation date: January 19, 2007.

Sincerely,

Tom J. Hanson, Commissioner
Department of Finance

Patricia Anderson, Commissioner
Department of Employee Relations