OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Department of Economic Security

Mainfram Scheduled Batch Processing and MIPS Accounting System For the Period Ending February 2000

MAY 18, 2000 00-21

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 fifty 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 and one best practices review.

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.

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 651-296-1727 (voice), or the Minnesota Relay Service at 651-297-5353 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, evaluation, or best practices review, 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

Report Summary

Financial-Related Audit

Department of Economic Security
Mainframe Scheduled Batch Processing and MIPS Accounting System
For the Period Ending February 2000

Key Findings and Recommendations:

- The department scheduled and ran over 300 batch jobs during 1999 that were not subjected to an independent quality control review. Because scheduled batch jobs typically have very powerful security clearances associated with them, we recommended that the department independently review all scheduled batch jobs. (Finding 1, page 6)

- The department provided some information system professionals with more access to the scheduled batch environment than was needed to fulfill their normal job duties. (Finding 2, page 6)

- The department did not perform necessary maintenance on its ACF2 security infrastructure. We recommended that the department periodically cancel or suspend user accounts that are no longer needed and purge unneeded security rules. (Finding 3, page 7)

- The department permitted many users to share powerful network accounts. We recommended that the department create unique network accounts for all people and enforce periodic password changes. (Finding 4, page 9)

Financial-Related Audit Reports address internal control weaknesses and noncompliance issues found during our audits of state departments and agencies. The scope of our work at the Department of Economic Security was limited to a review of access to the department's mainframe scheduled batch processing environment, and access to the department's network-based MIPS accounting system. The department's response to our recommendations is included in the report.

Room 140, 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

Department of Economic Security
Mainframe Scheduled Batch Processing
MIPS Accounting System

Table of Contents

Audit Participation

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

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Christopher Buse, CPA, CISA	Audit Manager
Mark Mathison, CPA, CISA	Auditor-In-Charge
Daniel Kingsley	Auditor

Exit Conference

We discussed the findings and recommendations of the audit with the following representatives of the Department of Economic Security on Tuesday, May 2, 2000:

Earl Wilson	Commissioner
Al St. Martin	Deputy Commissioner
Mick Coleman	Associate Deputy Commissioner
Bonnie Elsey	Acting Assistant Commissioner
Harlan Hanson	Chief Information Officer
John Stavros	Chief Financial Officer
Mark Butula	Director of Internal Security
Jack Weidenbach	Reemployment Insurance Director
Tim Langlie	Accounting Director

OLA

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

Representative Dan McElroy, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Earl Wilson, Commissioner
Department of Economic Security

We have conducted a financial-related audit of selected activities at the Minnesota Department of Economic Security. Our audit scope included a review of access controls to the department's mainframe scheduled batch processing environment and to its Micro Information Products (MIPS) accounting system as of February 2000.

We conducted our audit in accordance with *Government Audit Standards*, as issued by the Comptroller General of the United States. Those standards require that we obtain an understanding of management controls relevant to the audit. The standards also require that we design the audit to provide reasonable assurance that the Department of Economic Security complied with the provisions of laws, regulations, contracts, and grants that are significant to the audit. The department's management is responsible for establishing and maintaining the internal control structure and for compliance with applicable laws, regulations, contracts, and grants.

This report is intended for the information of the Legislative Audit Commission and the management of the Department of Economic Security. This restriction is not intended to limit the distribution of this report, which was released as a public document on May 18, 2000.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: February 29, 2000

Report Signed On: May 10, 2000

Room 140, 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

Chapter 1. Introduction

The Department of Economic Security uses a variety of different computer systems to support its programs. Most of these systems run on an IBM mainframe computer. However, a growing number of systems now run on personal computers and file servers that are connected to a department-wide network.

The primary objective of this audit was to review controls over scheduled batch processing on the mainframe computer. However, we also reviewed controls over an accounting system called Micro Information Products (MIPS). The department uses MIPS to account for financial activities and prepare financial statements for the Reemployment Insurance Program. The MIPS accounting system does not run on the mainframe computer. Instead, it runs on personal computers that are connected to the department-wide network.

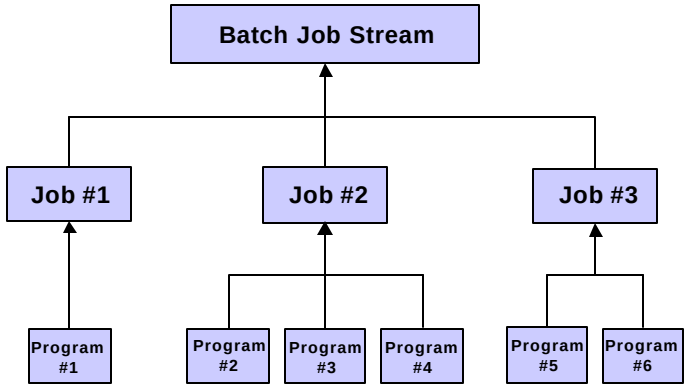
Mainframe Scheduled Batch Processing

Scheduled batch processing is a special type of computing environment that requires little or no user interaction. Interactive processing, on the other hand, is an environment where a computer responds to commands as soon as a person enters them. Most scheduled batch processing occurs at night, thus preserving valuable computing resources during the day for interactive users.

The primary unit of work in a scheduled batch environment is referred to as a "job." A scheduled batch job can consist of a single computer program or a collection of computer programs. Some jobs run on specific dates or at certain times, while others only execute after the successful completion of a predecessor job. A collection of interrelated and dependent batch jobs is commonly referred to as a "job stream." Figure 1-1 is an example of a job stream for a computerized business system. This computer system's job stream contains three separate jobs, each of which contain one or more computer programs.

Most computerized business systems that run on the mainframe rely on a large, overnight batch stream. The computer programs in these batch streams perform many mission-critical business functions, such as processing reemployment insurance benefit payments for unemployed people.

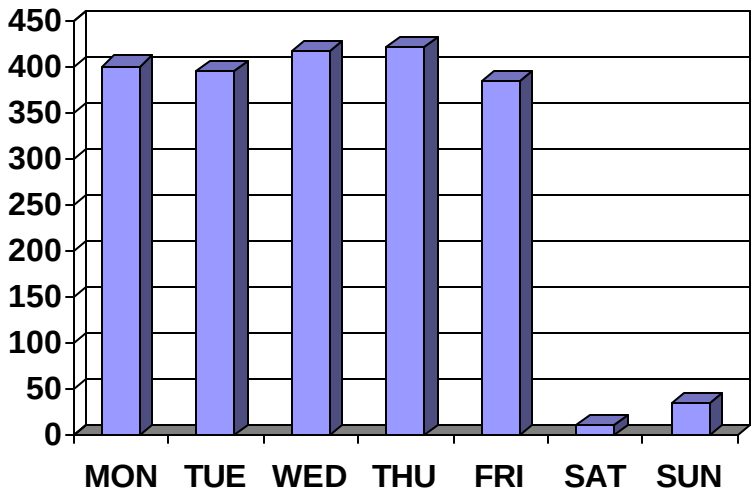
Figure 1-1
Components of a Batch Stream for a Computerized Business System



Source: Auditor prepared.

The department uses a software package called CONTROL-M to manage scheduled batch processing. During 1999, the department used CONTROL-M to process over 107,000 batch jobs. As illustrated in Figure 1-2, the department ran approximately 400 batch jobs on a typical business day.

Figure 1-2
Average Number of Scheduled Batch Jobs Run Each Day
Calendar Year 1999

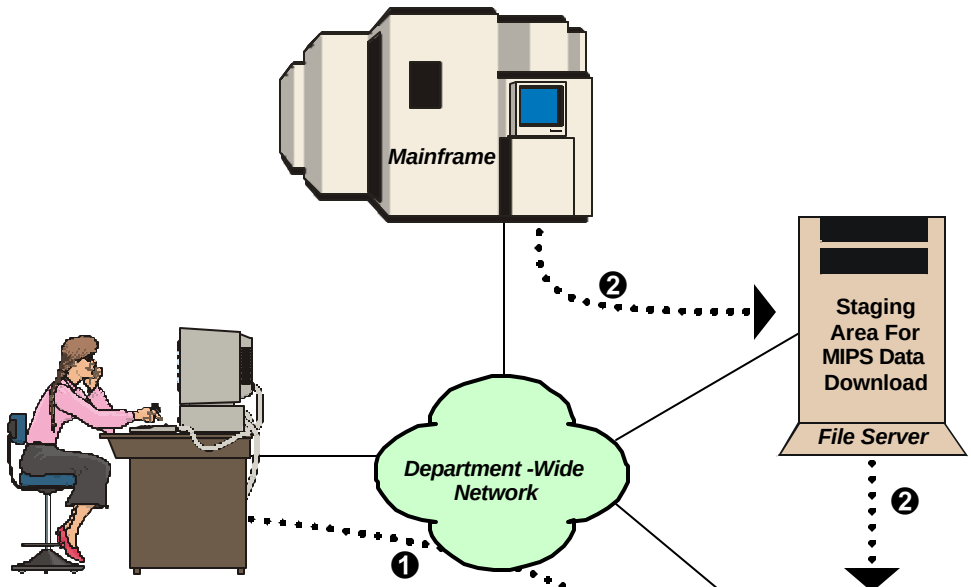


Source: Auditor prepared from CONTROL-M data.

MIPS Accounting System

The MIPS database resides on a file server that is connected to the department-wide network. Employees access and update this data through personal computers that are also connected to the network. Employees use MIPS screens to enter most accounting transactions. However, the department also downloads some reemployment insurance data into MIPS from the mainframe computer. Each night, a scheduled batch job gathers and downloads this data to a designated file server. Employees then use a special utility program to copy the data from this staging area to the file server that houses the MIPS database. Figure 1-3 illustrates the methods used to input reemployment insurance data in MIPS:

Figure 1-3
MIPS Reemployment Insurance Data Input Methods



❶ **On-line:** Employees use MIPS screens to enter transactions.
❷ **Download:** Scheduled batch job gathers and downloads data to staging area. Employees import data into MIPS database with special utility program.

Source: Auditor prepared.

Chapter 2 discusses the scope of our work and conclusions reached from our review of mainframe scheduled batch processing. In Chapter 3, we discuss the scope of our work and conclusions reached from our review of the MIPS accounting system.

Chapter 2. Mainframe Scheduled Batch Processing Controls

Chapter Conclusions

The Department of Economic Security created a secure environment to perform scheduled batch processing. However, some jobs scheduled and run in this environment were not subjected to a stringent quality control review. Also, some information system professionals had inappropriate security clearances. Finally, the department has not performed necessary maintenance on its ACF2 security infrastructure.

The Department of Economic Security uses a software package called CONTROL-M to manage scheduled batch processing. Employees in the Data Control Unit program CONTROL-M to run some batch jobs at predefined dates or times, while others only run after the successful completion of a predecessor job. CONTROL-M also provides the department with a variety of useful scheduling and job tracking reports.

The department uses a software package called ACF2 to limit access to its mainframe computer and data, including the CONTROL-M environment. ACF2 protects against the unauthorized destruction, disclosure, or modification of data. ACF2 will not permit a person to access data unless a security officer or the data owner explicitly authorizes that access. ACF2 security “rules" define these explicit authorizations.

Audit Objective and Methodology

This portion of our audit analyzed controls over the scheduled batch environment. Specifically, we designed our work to answer the following question:

- Did the department limit access to its scheduled batch environment to only those people who need that access to fulfill their job duties?

To answer this question, we interviewed the information system professionals who manage the scheduled batch environment. We also interviewed the department's ACF2 security officers. Finally, we analyzed detailed CONTROL-M and ACF2 data.

Conclusions

The department limited access to its scheduled batch environment. However, as discussed in Finding 1, some scheduled batch jobs were not subjected to an independent quality control review. Finding 2 discusses our concerns about some information system professionals with inappropriate clearance to the scheduled batch environment. Finally, in Finding 3, we discuss ACF2 maintenance issues that came to our attention.

1. Some scheduled batch jobs were not subjected to an independent quality control review.

During 1999, the department scheduled and ran over 300 batch jobs without first subjecting them to an independent quality control review. Referred to by the department as "ad hoc" or "fix" jobs, these jobs contain programs that will typically be used only once to accomplish a specific objective. These jobs accounted for less than one percent of the scheduled batch activity during 1999. Currently, a programmer who develops one of these jobs must submit a Fix/ADHOC Job Run Request form to the Data Control Unit. Data Control then uses this information to schedule and run the job. Throughout this process, no independent person reviews the propriety of the job contents.

It is important to independently review scheduled batch jobs because they are inherently risky. Scheduled batch jobs typically have very powerful security clearances and do not require passwords. The introduction of an unauthorized or improperly coded scheduled batch job could lead to a disastrous loss or the widespread destruction of critical business data.

Recommendation

- *The department should independently review all scheduled batch jobs.*

2. Some information system professionals have inappropriate clearance to the scheduled batch environment.

Some information system professionals with access to the scheduled batch environment do not need this clearance to fulfill their regular job duties. We found groups of computer operations, help desk, and telecommunications employees who had complete and unfettered access to critical components of the scheduled batch environment. We also found two former employees with complete access. One of these former employees never used his account to access the mainframe and the other last used her account in November 1998.

We recognize that there are occasions when employees outside the Data Control Unit may need access to the scheduled batch environment. However, granting large groups of

people complete and continuous access to sensitive batch job data exposes the department to unnecessary business risks.

Recommendations

- *The department should limit access to the scheduled batch environment to only those people who need that access to fulfill their normal job duties.*

- *The department should develop special scheduled batch environment access procedures for those employees outside the Data Control Unit.*

3. The department did not perform necessary maintenance on its ACF2 security infrastructure.

We found many obsolete ACF2 security rules and user accounts during our review of scheduled batch processing. Maintaining the ACF2 security databases is an important security administration responsibility. When left uncontrolled, inactive accounts and unneeded security rules can provide intruders with access to critical business data.

We identified these same weaknesses in our audit report released in March 1998. In response to this issue, the department purchased software to streamline ACF2 maintenance. However, security officers have not used this software since 1998.

Recommendations

- *The department should periodically cancel or suspend user accounts that are no longer needed.*

- *The department should periodically purge unneeded security rules from the ACF2 security database.*

Chapter 3. MIPS Data Integrity

Chapter Conclusions

The Department of Economic Security designed and implemented controls to protect the integrity of MIPS data. However, we found several network security weaknesses that diminished the effectiveness of those data integrity controls.

The department purchased an accounting system called Micro Information Products (MIPS) to account for the financial activities of the Reemployment Insurance Program. The MIPS software runs on personal computers that are connected to the department-wide network. All MIPS data resides on a file server that is also connected to the network.

The MIPS accounting system has built-in security features. The department uses these security features to limit access to specific MIPS screens. The department uses both the accounting system's built-in security features as well as network operating system security features to limit access to the MIPS database. Collectively, these two security layers limit the number of people who can view, modify, or delete data without using the intended MIPS screens.

Audit Objectives and Methodology

This portion of our audit focused on the department's MIPS data integrity controls. Specifically, we designed our work to answer the following questions:

- Did the department limit access to MIPS screens to only those employees who need that access to fulfill their job duties?

- Did the department limit the number of people who can update or delete MIPS data without using the intended MIPS screens?

To answer these questions, we interviewed the employee who manages the security features within MIPS. We also interviewed the employee who is responsible for administering network security. Finally, we examined both MIPS and network security data.

Conclusion

The department limited access to MIPS screens to only those employees who need access to fulfill their job duties. The department also limited the number of people who can update or delete MIPS data without using the intended screens. However, we found some network security weaknesses that could diminish the effectiveness of the MIPS data integrity controls. Finding 4 discusses these weaknesses in more detail.

4. The department did not adequately control some powerful network accounts.

During our audit, we found one powerful network account that was being shared by 13 people. This account had complete and unfettered access to most data on the department-wide network. This powerful network account, as well as eight other powerful network accounts, also did not require periodic password changes.

Creating unique accounts and passwords for all people is an important control because it ensures individual accountability. When people share accounts, it becomes nearly impossible to trace specific actions to individuals. Sharing accounts with powerful security clearances is particularly risky. In fact, it exposes the entire department to significant and unnecessary risks.

Enforcing periodic password changes is also an important control. Computers use passwords to authenticate the identity of specific people. Unfortunately, computerized tools now permit unscrupulous people to guess passwords. Enforcing periodic password changes minimizes this risk.

Recommendation

- *The department should create unique accounts for all people and enforce periodic password changes.*

State of Minnesota
Department of Economic Security
390 North Robert Street
Saint Paul, Minnesota 55101

Office of the Commissioner

May 8, 2000

Mr. James R. Nobles
Legislative Auditor
First Floor, Centennial Office Building
658 Cedar Street
St. Paul, Minnesota 55155

Dear Mr. Nobles:

The following information is offered in response to your draft audit report for the period ended February 29, 2000.

Conclusion:

1. **Some scheduled batch jobs were not subjected to an independent quality control review.**

Response:
We agree. The Department of Economic Security will revise it's policy regarding the running of "fix" and "ad hoc" jobs to require the approval of the programming supervisors responsible for the specific job or program effected. A paper copy of the "fix" or "ad hoc" job request will be retained in the Data Control unit. Following the entry on the security log a data security administrator will review the paper request to ensure that all required approvals were obtained prior to the jobs being run.

Responsible Individual: Mark Butala

Conclusion:

2. **Some information system professionals have inappropriate clearance to the scheduled batch environment.**

Response:
We agree. Only individuals who have a business reason should have access to the scheduled batch environment. Scheduled batch job access was recently deleted for the two former employees. Data security staff will meet with the supervisors of employees who currently have access. Together, the batch environment software supervisor, the security administrator and business unit supervisors will determine which individuals have a legitimate business need, all others will have their access deleted.

Responsible Individual: Mark Butala

Conclusion:

3. The department did not perform necessary maintenance on its ACF2 security infrastructure.

Response:
We agree. Beginning in February 2000 a computer job was implemented and will continue to be run monthly. The job will cancel all user logons that have not been accessed within a 90-day period. Also, the same job will cancel any logon that has not been accessed since being established or since the last time a data security administrator changed the password.
Since April 2000 the data security administrators have used ETF/A software for maintaining its ACF2 databases. Currently dataset rules and resource rules through the fourth quarter of 1999 have been purged. Security staff will continue to keep these databases current.

Responsible Individual: Mark Butala.

Conclusion:

4. The department did not adequately control some powerful network accounts.

Response:
We agree. The Department of Economic Security will review all Novell Network accounts to insure that all user passwords will expire on a routine basis. We will also review the use of shared accounts and determine the appropriateness of their use. Particular attention will be paid to accounts with powerful rights and privileges and wherever possible individual, unique accounts will be created or additional layers of access controls will be implemented.

Responsible Individual: Mark Butala

Sincerely,

/s/ Earl R. Wilson

Earl R. Wilson
Commissioner