

New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor

Department of Labor and Workforce Development
Local Office Online Payment System (LOOPS)

August 8, 2011 to March 31, 2013

Stephen M. Eells
State Auditor

LEGISLATIVE SERVICES COMMISSION

SENATE

CHRISTOPHER J. CONNORS
NIA H. GILL
ROBERT M. GORDON
THOMAS H. KEAN, JR.
JOSEPH M. KYRILLOS, JR.
JOSEPH PENNACCHIO
STEPHEN M. SWEENEY
LORETTA WEINBERG

GENERAL ASSEMBLY

JOHN F. AMODEO
JON M. BRAMNICK
ANTHONY M. BUCCO
JOHN J. BURZICHELLI
THOMAS P. GIBLIN
LOUIS D. GREENWALD
ALISON LITTELL MCHOSE
SHEILA Y. OLIVER

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

ALBERT PORRONI
Executive Director
(609) 847-3901

OFFICE OF THE STATE AUDITOR
(609) 847-3470
FAX (609) 633-0834

STEPHEN M. EELLS
State Auditor

GREGORY PICA
Assistant State Auditor

JOHN J. TERMYNA
Assistant State Auditor

The Honorable Chris Christie
Governor of New Jersey

The Honorable Stephen M. Sweeney
President of the Senate

The Honorable Sheila Y. Oliver
Speaker of the General Assembly

Mr. Albert Porroni
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Department of Labor and Workforce Development, Local Office Online Payment System (LOOPS) for the period of August 8, 2011 to March 31, 2013. If you would like a personal briefing, please call me at (609) 847-3470.

Stephen M. Eells
State Auditor
July 18, 2013

Table of Contents

Scope 1

Objective 1

Methodology 1

Conclusions 2

Background 2

Findings and Recommendations

Business Continuity Plan and Disaster Recovery Test 3

LOOPS Security and Access Controls 4

Observation 5

Auditee Response 6

Scope

We have completed an audit of the Department of Labor and Workforce Development's Local Office Online Payment System (LOOPS) for the period August 8, 2011 through March 31, 2013. Our audit evaluated selected general and application controls related to the processing of unemployment claims through this system. The selected controls included change management, system backup and recovery, contingency planning and disaster recovery, system security, and data integrity which included data input, data processing, and data output.

Objective

The objective of the audit was to determine the adequacy of selected general and application controls for change management, system backup and recovery, contingency planning and disaster recovery, system security, and data integrity which included data input, data processing, and data output.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by *Control Objectives for Information and related Technology* (CobiT) issued by the IT Governance Institute, the *Federal Information System Controls Audit Manual* issued by the United States Government Accountability Office, and the International Organization for Standardization.

In preparation for our testing, we studied circular letters promulgated by the Department of the Treasury, and policies and guidelines of the Department of Labor and Workforce Development and the Office of Information Technology. Provisions we considered significant were documented, and compliance with those requirements was verified by interview, observation, and tests of controls. In addition, we obtained and reviewed system administration, security, and user manuals. Functions we considered significant were documented and implementation of those features was verified. We also interviewed agency personnel to obtain an understanding of the internal controls.

A nonstatistical sampling approach was used. Our tests of selected general and application controls were designed to provide conclusions about the adequacy of the controls in place for change management, system backup and recovery, contingency planning and disaster recovery, system security, and data integrity.

Conclusions

Our review disclosed that general and application controls were adequate for change management, system backup and recovery, and data integrity which included data input, data processing, and data output. However, general and application controls for contingency planning and disaster recovery and system security require improvement. We also noted certain facts that, although not subjected to audit procedures, warranted inclusion as an observation.

Background

LOOPS is a 35-year-old legacy mainframe system used as the primary system for unemployment claims receipt and processing. This system is supplemented by a front-end claims receipt, web based self-service application utilized at all three call centers (Union City, Freehold, and Cumberland) with an Interactive Voice Response (IVR) for the Regional Call Center (RCC) that captures responses from customers. The RCC IVR system processes continued claims for benefits, as well as general and claim-specific information questions. In addition to the RCC IVR, there is a separate and distinct IVR system for claims filing for new customers. There are also two publicly accessed applications (Internet Claims and Continued Claims Certification) that interface with both the legacy and web based systems.

Business Continuity Plan and Disaster Recovery Test

The department needs an established business continuity plan and to implement a full disaster recovery test.

Control Objectives for Information and related Technology (CobiT) states an Information Technology (IT) continuity plan should be developed and designed to reduce the impact of a major disruption in key business functions and processes. The plan should be based on an understanding of the risks of potential business impacts and address requirements for resilience, alternative processing, and recovery capability of all critical IT services. It should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach. The continuity plan needs to be periodically and thoroughly tested which is essential in determining whether it will function as intended in an emergency situation. Testing the IT continuity plan on a regular basis provides assurance that IT systems can be effectively recovered, deficiencies identified, and the plan remains relevant. The testing should involve recovery of single applications, inclusion of integrated scenarios, end-to-end tests, and integrated vendor tests.

The department has drafted a business continuity plan, titled "Unemployment Insurance Division of Information Technology (D.I.T.) Contingency Plan," which includes LOOPS; however, it has not been finalized and approved. Testing has been limited to tabletop exercises and no comprehensive disaster recovery test has been performed on LOOPS, nor is one part of the department's current plans. The Office of Information Technology (OIT) administers the LOOPS application and has two contingency plans, the Continuity of Operations Plan and the Disaster Recovery Plan, that only address the IBM mainframe on which LOOPS resides. The OIT plans do not specifically address a recovery of LOOPS. Without a finalized contingency plan that has been properly tested through a complete disaster recovery test, management may not have properly identified deficiencies with either their Unemployment Insurance D.I.T. Contingency Plan or OIT's plans. Any service outages as a result of an insufficient and untested plan could greatly impact the ability of individuals to file for and collect unemployment insurance.

Recommendation

The department should finalize and adopt the Unemployment Insurance D.I.T. Contingency Plan. It should also perform a full disaster recovery test of LOOPS as soon as possible. This test should be done to identify and correct any deficiencies of the Unemployment Insurance D.I.T. Contingency Plan and to test the effectiveness of OIT's Continuity of Operations Plan and the Disaster Recovery Plan with respect to LOOPS.

LOOPS Security and Access Controls

The department should review LOOPS access rights periodically to ensure they are appropriate.

Control Objectives for Information and related Technology states that management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to reduce the risk of errors, fraud, misuse, or unauthorized alteration. Although the department's Division of Information Technology (DIT) has formal procedures for establishing, issuing, suspending, and closing user accounts, they do not effectively monitor user access to the LOOPS application. The department utilizes a set of programs that enables security on mainframes commonly referred to as Access Control Facility (ACF2). The Information Security Representative (ISR) at the department uses ACF2 to create a new user ID and grants requested LOOPS access based upon the employee's job function.

Our audit disclosed 9,993 LOOPS ACF2 logon IDs at the time of our testing. Our analysis of these IDs revealed 7,771 IDs (78%) belonging to 6,847 unique users who had some type of access to LOOPS. Of these, 5,815 had inquiry only access, while the remaining 1,956 had an ability to move a claim through the LOOPS application with 834 of them capable of processing a claim with payment. The 2,222 logon IDs that do not have LOOPS access should be canceled; 926 have already been identified as suspended and 1,296 had been created without the capability to access the LOOPS application.

Of the logon IDs with current access, there are users who should be evaluated to determine if they still need the logon ID. We found 121 logon IDs have never accessed LOOPS and 712 logon IDs have not accessed LOOPS since 2010.

Additionally, there are 85 users that have super user access granting them the ability to perform all functions within the application. Our last audit of LOOPS identified seven users with this capability. Although the number of users with this capability increased significantly due to the need to process a large volume of claims and to deal with a large backlog as a result of the high unemployment rate in the state, these users' access privileges should be evaluated to determine if this unlimited access is still justified. We also found that 117 users have multiple logon IDs with 42 of those users having their LOOPS access privileges escalated with the issuance of the additional ID.

Lastly, we found users had left state service but still had access to the LOOPS application. Testing of the department's 23 employees retired in July of 2011 disclosed that 18 had not been suspended or deleted from accessing LOOPS by the end of 2011. These comprised 21 out of 26 logon IDs since some employees had multiple logon IDs associated with them. Two of these IDs had accessed LOOPS after the related users retirement date although there is no evidence that improper actions were taken. The department's DIT states that they have a logical access procedure in place to suspend or delete users' logon IDs when employees transfer, retire, or leave state service. However, this procedure is not working as intended. The DIT receives a

separated employee report from the Human Resource department, but the ISRs do not suspend or delete the users' logon ID and their associated access in a timely manner. In order to analyze and monitor users' access, ACF2 Executive Information Summary (ACFEIS) reports are used. These reports identify users by a logon ID and Personnel Management Information System (PMIS) name and can be employed to match against state databases to determine if a user is a current employee, or has been transferred, retired, or died. DIT does not use the same naming convention for LOOPS users as what is found on PMIS. This does not allow the department's ISRs to perform accurate, periodic matches to determine the employment status of LOOPS users.

Failure to have adequate access controls can diminish the reliability of computerized data and increase the risk of destruction, inappropriate disclosure of data, or the fraudulent issuance of an unemployment benefit. Separated employees that still possess access to LOOPS could make unauthorized changes to an unemployment claim. In addition, logon IDs with access to critical LOOPS conversations, such as conversations P100 and P200 which issues unemployment benefit payments, could process a fraudulent payment.

Recommendation

The department's DIT should initiate a comprehensive review of LOOPS access statewide. The assessment should include evaluating access needs corresponding with the users' job functions, reviewing existing profiles in LOOPS to determine validity, and creating and adjusting roles in LOOPS as necessary. In addition, to enhance matching procedures, DIT should require the same naming convention for each user in LOOPS as are found in PMIS.

»»-««

Observation

In January 2005, the Department of the Treasury, Purchase Bureau, requested final bid submissions for the design, development, and implementation of the New Jersey State Unemployment Compensation Claimant and Employer Service System (NJ SUCCESS). NJ SUCCESS was to be a comprehensive, integrated, web based solution that included document management, imaging, workflow, telephony, and infrastructure to modernize the delivery of Unemployment Insurance (UI) benefit services. With a proposed fixed price of $40 million and after expenditures of $50 million to the contracted vendor, NJ SUCCESS provided only the web based portion of processing UI claims and failed to be the complete replacement for LOOPS as it was intended to be.

Since the first system design, development, and implementation endeavor did not accomplish all of its objectives, in August 2012 the department published a Request for Information (RFI) to address a new UI operations modernization system. The RFI's purpose was to gather information on industry approaches and solutions to develop, operate, and support a modernized UI benefits system. A Request for Proposal will be issued for this project in the near future.

State of New Jersey

DEPARTMENT OF LABOR AND WORKFORCE DEVELOPMENT
PO BOX 110
TRENTON, NEW JERSEY 08625-0110

CHRIS CHRISTIE
Governor

KIM GUADAGNO
Lieutenant Governor

HAROLD J. WIRTHS
Commissioner

July 12, 2013

Mr. Stephen M. Eells, State Auditor
New Jersey State Legislature
Office of the State Auditor
125 South Warren Street, P.O. Box 067
Trenton, NJ 08625-0067

Dear Mr. Eells:

We are writing to you in response to the draft audit report of the State of New Jersey Department of Labor and Workforce Development (LWD), Local Office Online Payment System (LOOPS). The report covered the period of August 8, 2011 to March 31, 2013 and contained two findings in regard to LOOPS. The following is our response to the findings raised in the draft report:

FINDING#1: The department needs an established business continuity plan and to implement a full disaster recovery test.

LWD RESPONSE: Unemployment Insurance (UI) program area, Office of Information Technology and the LWD Division of Information Technology (DIT) will be meeting in the near future to discuss a business driven LOOPS disaster recovery plan for UI. The key to this initiative is to document and get clarity on the business requirements, scope of the project, testing strategy, roles of each agency in this initiative. Since LOOPS is maintained by OIT, it's their primary responsibility to successfully implement this project with DIT/UI Program assistance.

FINDING #2: The department should review LOOPS access rights periodically to ensure they are appropriate.

LWD RESPONSE: The Office of Internal Audit (OIA) has been working with DIT to review suspended accounts. DIT is coordinating with OIT to remove any account which has not accessed LOOPS since December 31, 2011. Then, on a quarterly basis, any account which has not accessed LOOPS within the previous 12 months will be removed. OIA will follow-up with the UI program area to review access levels for appropriateness.

If you have any questions or need additional information please contact Jerry Calamia, Director of OIA at (609) 292-1885.

Sincerely,

Harold J. Wirths
Commissioner

c: Aaron Fichtner
Frederick Zavaglia
Sriram Vilayanur
Ronald Marino
Jerry Calamia

New Jersey Is An Equal Opportunity Employer