STATE OF
NORTH CAROLINA

AUDIT OF APPLICATION CONTROLS

EMPLOYMENT SECURITY COMMISSION

DECEMBER 2008

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

AUDIT OF APPLICATION CONTROLS

EMPLOYMENT SECURITY COMMISSION

DECEMBER 2008

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Mr. Henry Payne, Chairman,
North Carolina Employment Security Commission

Ladies and Gentlemen:

We have completed our information systems (IS) application audit at the Employment Security Commission. The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The primary objective of this audit was to evaluate controls for the Employment Security Commission applications. The scope of our audit was to review the application controls governing specific reports produced by the following systems: Unemployment Insurance (UI) Benefits System, Special Payments System, and Employment Services Client System. Application controls for these systems include data completeness, data accuracy, data validity, data authorization, and data retention. The purpose of application controls is to ensure that as data passes through these system, it is complete, accurate, valid, authorized, and retained.

This report contains an executive summary that highlights the areas where the Employment Security Commission has performed satisfactorily relevant to our audit scope and where improvements should be made.

We wish to express our appreciation to the staff at the Employment Security Commission, for the courtesy, cooperation, and assistance provided to us during this audit.

North Carolina General Statutes require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

Respectfully submitted,

Leslie Merritt

Leslie Merritt, Jr., CPA, CFP
State Auditor

TABLE OF CONTENTS

We conducted an information systems (IS) audit of the Employment Security Commission (ESC), from April 15, 2008, through October 24, 2008. The primary objective of this audit was to evaluate application controls governing specific reports produced by the following systems: Unemployment Insurance (UI) Benefits System, Special Payments System, and the Employment Services Client System. Depending on the report, many different sub-routines were evaluated to determine if controls over the completeness, accuracy, or validity of the transactions exist. The following systems reports were evaluated during this audit:

[UI Benefits System State Reports]
- BP400P1-Amount to be Charged to Reimbursable Accounts
- BP450P1-Amount to be Paid to Reimbursable Accounts
- ESP411DP1-Check Register
- NCUI 550-Transcript and Monetary Determination

[UI Benefits System Federal Reports]
- ETA 191-UI Financial Status of UCFE/UCX Report
- ETA 2112-UI Financial Transaction Summary Report
- ETA 227-Overpayment Detection and Recovery Activities

[Special Payments System Federal Reports]
- TAPR-Trade Act Participant Report
- ETA 563- Quarterly Determinations Allowance Activities and Employability Service under the Trade Act Report
- ATAAAR-Alternative Trade Adjustment Assistance Activities Report

[Employment Services Client System Federal Reports]
- ETA 9002 A-Quarterly Report Services to Participants
- ETA 9002 B-Services to Veterans, Eligible Persons and TSMs
- ETA 9002 C-Performance Outcomes-Exiters
- ETA 9002 D-Performance Outcomes-Veterans, Eligible Persons and TSMs
- Vets 200 A-C-Veterans Employment and Training Service Quarterly Reports

Data Completeness controls are designed to ensure that all transactions are entered into the system once and only once, that all errors are corrected without any being lost, duplicated or added, that all transactions are processed, that databases are updated completely, and that all output reports are complete. Our audit identified significant weaknesses in completeness controls. *Audit Finding 1: Inadequate Completeness Controls in the Process that Produces the BP400P1 and BP450P1 Reports; Audit Finding 2: Inadequate Completeness Controls in the Process that Produces the ESP411DP1, ETA191, ETA2112, and NCUI 550 Reports; Audit Finding 3: Completeness of The ETA 227 Report Cannot Be Ensured; Audit Finding 4: Destructive Updates are Allowed in the ETA 227 Reporting Process and No Audit Trail is Maintained; Audit Finding 5: No Controls Exist To Ensure the Completeness of Data Supporting the Trade Act Participant Report (TAPR); Audit Finding 6: Inadequate Completeness Controls in the Business Process that Produces the ETA 9002 A-D and VETS 200 A-C Reports.*

Data Accuracy controls are designed to ensure that the details of transactions are entered and processed correctly, and that printed output is not distributed to the user until it is checked for reasonableness. Our audit identified significant weaknesses in accuracy controls. *Audit Finding 7: Edit Checks Are Not Sufficient To Prevent Inaccurate Information for the ETA 227, ETA 563, ETA 9002 A-D and Vets 200 A-C Reports.*

Data Validity controls are designed to ensure that the data entered into the application is valid. A division of roles and responsibilities should exist, which should exclude the possibility for a single individual to subvert a critical process. Our audit identified a significant weakness in the validity controls. *Audit Finding 8: Improper Segregation of Duties Exist in The Reporting Process For The ATAAAR, ETA 563, ETA 9002 A-D, and VETS 200 A-C Reports.*

Data Authorization controls are designed to ensure that access to data is appropriate and authorized and that access is granted on a need to know, need to use basis. The access control environment should consist of access control software and information security policies and procedures that are implemented appropriately to protect the application data. Our audit identified a significant weakness in the data authorization. *Audit Finding 9: Programmers Have Direct Access To Production Data That Produces The Following Reports: ATAAAR, ETA 563, TAPR, ETA 9002 A-D, and VETS 200 A-C Reports.*

Data Retention controls are designed to ensure that data is retained according to federal and state guidelines. Our audit identified a significant weakness in data retention. *Audit Finding 10: Retention of Supporting Documentation For ETA 563, TAPR, ATAAAR, ETA 9002 Parts A-D and VETS 200 Parts A-C Reports.*

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the North Carolina General Statutes Chapter 147-64.6, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. This IS audit was designed to ascertain the effectiveness of application controls at the Employment Security Commission.

SCOPE

Application controls govern whether the design of the critical application control supports management's financial statement assertions, federal compliance, and that the controls are functioning effectively. The scope of our IS application controls audit was to review application controls which directly affect the state and federal reports produced by Employment Security Commission application systems. Other IS access control topics were reviewed as considered necessary.

METHODOLOGY

We audited policies and procedures, interviewed key administrators and other personnel, examined system configurations, tested on-line system controls, reviewed appropriate technical literature, and reviewed computer-generated reports in our audit of application controls. We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States and *Information Systems Audit Standards* issued by the Information Systems Audit and Control Association.

[This Page Left Blank Intentionally]

The North Carolina Employment Security Commission was created as the Unemployment Compensation Commission by the General Assembly in a special session on December 16, 1936. The name was changed by law to Employment Security Commission effective April 1, 1947. Originally established as a three-member body, it was changed to a seven-member commission effective July 1, 1941. The Commission's mission is to promote and sustain the economic well being of North Carolinians in the world marketplace by providing high quality and accessible workforce-related services. The Employment Security Commission is led by the chairman, two deputy chairmen, two deputy commissioners and three directors.

The Unemployment Insurance (UI) Benefits System administers the UI benefit payments to eligible individuals who are out of work due to no fault of their own. These benefits are to provide temporary, partial compensation for lost wages. The Special Payments System is an intranet based processing system for TAA/TRA claims and benefits. These benefits provide assistance to workers adversely affected by foreign trade to enable them to return to work as quickly as possible. Employment Service Client System (ESCS) maintains client registration data for work search and job orders from employers and matches jobs to job seekers based on qualification requirements and client capabilities.

[This Page Left Blank Intentionally]

The following audit results reflect the areas where the Employment Security Commission has performed satisfactorily and where recommendations have been made for improvement.

APPLICATION CONTROLS

Application reviews consist of determining whether the design of the critical application control supports management's financial statement assertions, federal compliance, and that the controls are functioning effectively. These reviews are performed when the auditor intends to rely on an application system control to reduce the amount of substantive testing of details required before rendering an opinion on the financial statements.

DATA COMPLETENESS

Data completeness controls are designed to ensure that all transactions are entered into the system once and only once, that all errors are corrected without any being lost, duplicated or added, that all transactions are processed, that databases are updated completely, and that all output reports are complete. Our audit identified significant weaknesses in completeness controls.

AUDIT FINDING 1: INADEQUATE COMPLETENESS CONTROLS IN THE PROCESS THAT PRODUCES THE BP400P1 AND BP450P1 REPORTS

We found inadequate completeness controls in the business process that produces the BP400P1 and BP450P1 reports. This business process collects inputs from multiple locations, and this information is stored into one file. The programs associated with these reports scan files to accumulate the totals represented on the reports. If a transaction that should have been included within the report is somehow corrupt, or missed, no controls exist to notify the programmer that all transactions relating to these reports were not included. We found no transaction sequence numbers being used to help identify missing transactions. A control of this nature would help to ensure that transactions are accounted for and no gaps within the population exist. Furthermore, we found inputs are not reconciled against the resulting report for this process, thus completeness of this report cannot be ensured. Finally, the person responsible for ultimately reviewing this report does not receive the associated error reports, resulting in information that cannot be truly reconciled to the underlying data. As a result, transactions that should be included in the report totals could be missing from the population.

There should be controls in place to check for authenticity of origin and integrity of content before passing transaction data between internal/external applications.

Recommendation: ESC should implement a completeness control, such as transaction sequence totals on the source population and carry this information into extracted populations so a reconciliation can be performed to determine if a transaction is not included in the population. Error reports should also be delivered to the persons responsible for reconciling the BP400P1 and BP450P1 reports with the underlying data. This would enhance this person's ability to detect errors that have occurred, thus affecting the totals reported on this report.

Auditee's Response: As agreed in the meeting between ESC and audit staff, ESC will take the following actions to meet audit requirements:

In addition to saving all check register reports, ESC will retain the detail records that support the generation of the BP 400P1 and BP 450P1 in a separate file. This file will contain the following data elements: payment date, transaction number, void indicators, amounts and associated reimbursable employer account numbers.

AUDIT FINDING 2: INADEQUATE COMPLETENESS CONTROLS IN THE PROCESS THAT PRODUCES THE ESP411DP1, ETA191, ETA2112, AND NCUI 550 REPORTS

We found inadequate completeness controls in the business process that produces the ESP411DP1, ETA191, ETA2112, and NCUI 550 reports. Although the mainframe has some completeness controls such as input and output control totals, ESC programmers are not using these controls to ensure completeness of extractions. Also, audit trails are not used to reconcile the JCL error reports and transaction reports. As a result, transactions that should be included in the report could be lost from the population, and no controls are in place to detect the lost transactions.

There should be controls in place to ensure that adequate update controls such as run-to-run control totals and master file update controls are in place, and to check for authenticity of origin and integrity of content before passing transaction data between internal/external applications. Significant emphasis should be placed on maintaining the authenticity and integrity of transactions during transmission or transport.

Recommendation: ESC should implement various completeness controls within this business process, such as hash totals, audit trails, and reconciliations to ensure that all data is included within the resulting reports.

Auditee's Response: As agreed in the meeting between ESC and audit staff, ESC will take the following actions to meet audit requirements:

1. ESC will retain the detail records that support the generation of the ESP411DP1 in a separate file.
2. ESC will create and retain a file of all Monetary Determination and Wage Transcripts generated and the wage data by employer used in the associated calculations that recorded on the NCUI 550.

3. ESC has extended the retention period for the ETA 191 quarterly report and the associated detail file which is used to generate the ETA 191 to a total 16 quarters.
4. ESC will review existing completeness controls for the ETA 2112 and strengthen these controls where practical and introduce additional supervisory oversight as a compensating control where appropriate.

AUDIT FINDING 3: COMPLETENESS OF THE ETA 227 REPORT CANNOT BE ENSURED

ESC extracts information from a master file to create the ETA 227 Report. The federal agency uses this report to monitor the integrity of the benefit payment process in the UI Benefits system. Failure of ESC to meet performance requirements can result in a reduction of grant monies to the state agency, and incorrect reporting can skew the NC and Federal Overpayments Ratio Performance Report.

We found that the ETA 227 Report utilizes some manually entered dates. We also found that edit checks over these manual dates are not working properly. We confirmed this by testing the population of dates that fell outside of the century as well as the reporting period. As a result, some reports may not contain all data due to the incorrect dates.

Because the extraction from the master file depends on dates, completeness for the ETA 227 Report heavily depends on the accuracy of the date. System-generated dates normally ensure that dates are entered accurately, and that transactions are not inadvertently excluded. Manual dates, without proper edit checks, can be entered incorrectly and cause transactions to be lost.

Recommendation: ESC should use system-generated dates for all programs where applicable, and if a manually entered date is used, edit checks should ensure that transaction dates do not fall outside of the reporting quarter.

Auditee's Response: As agreed in the meeting between ESC and audit staff, ESC will take the following action to meet audit requirements:

ESC will determine the valid date range for manually entered dates and will implement edits to assure that these dates fall within the determined range.

AUDIT FINDING 4: DESTRUCTIVE UPDATES ARE ALLOWED IN THE ETA 227 REPORTING PROCESS AND NO AUDIT TRAIL IS MAINTAINED

Invalid overpayments are deleted from the database automatically by the ETA 227 program. Also, no audit trail is maintained for the ETA 227 Report transaction data. Procedures should be in place to ensure original source documents are retained or are reproducible by the organization for an adequate amount of time to facilitate retrieval or reconstruction of data, as well as to satisfy legal requirements.

An audit trail should be maintained for all critical transaction events that occur in a production database.

Recommendation: All transactions should be retained for at least 3 years. To offset an entry, an adjusting entry should be added to cancel the overpayment. Programmers should not be allowed to alter the production data in any manner. In the event the data has to be altered, proper audit trails should exist, and recording of all actions taken should be performed. Also, an audit trail should be generated to capture all transactions, especially adjustment transactions.

Auditee's Response: As agreed in the meeting between ESC and audit staff, ESC will take the following actions to meet audit requirements:

ESC will retain ETA 227 transactions for a minimum of 3 years. ESC will write invalid overpayments to a separate file for audit purposes prior to the deletion of such records from the overpayment master file. ESC will review and correct the existing audit trail program. ESC agrees that programmers should not have the authority to alter the data included in the ETA 227 report. Such access or authority is not available to ESC IS staff.

AUDIT FINDING 5: NO CONTROLS EXIST TO ENSURE THE COMPLETENESS OF DATA SUPPORTING THE TRADE ACT PARTICIPANT REPORT (TAPR)

The ESC Information Systems (IS) and Labor Management Information (LMI) divisions are responsible for producing the underlying data that is electronically submitted to the Department of Labor for the TAPR statistics. As this information is passed between the employees, no controls were found to ensure the completeness of this data. A reconciliation would help to identify errors in completeness of the report. As a result, transactions could be lost or become corrupt, and both employees would not be aware that this error had occurred. Furthermore, the TAPR statistics may be incomplete.

Management should check for authenticity of origin and integrity of content before passing transaction data between internal/external applications. Thus, significant emphasis should be placed on maintaining the authenticity and integrity of transactions during transmission or transport. Management should verify that all data expected for processing are received and processed completely, accurately and in a timely manner, and that all output is delivered in accordance with business requirements.

Recommendation: ESC management should implement completeness controls such as run-to-run control totals, record count comparisons, and master file update controls. Run-to-run totals, record counts, and byte comparison should be shared between the two divisions to ensure completeness.

Auditee's Response: As agreed in the meeting between ESC and audit staff, ESC will take the following actions to meet audit requirements:

When transmitting the TAPR data to the ESC LMI staff, IS staff will send an e-mail to the designated LMI TAPR staff that will contain the following elements:

1. Record count
2. File size
3. Report quarter to which the data applies
4. Request for verification by LMI of control totals
5. A reminder to retain both the e-mail and all files for audit purposes

AUDIT FINDING 6: INADEQUATE COMPLETENESS CONTROLS IN THE BUSINESS PROCESS THAT PRODUCES THE ETA 9002 A-D AND VETS 200 A-C REPORTS

ESC has inadequate controls in place to ensure the completeness of data reported on the ETA 9002 A-D and VETS 200 A-C Reports. Although record counts are inherent in the mainframe, use of these records counts to ensure completeness of the file transfer from the mainframe to secondary system could not be verified. As a result, transactions that should be included in the reporting period could be missing from the population, thus skewing the federal benchmarks that are relied upon in these reports.

Recommendation: ESC should implement a completeness control, such as, documenting the comparison of record counts between the mainframe and the secondary system for files transferred.

Auditee's Response: As agreed in the meeting between ESC and audit staff, ESC will take the following actions to meet audit requirements:

As a compensating control, documents will be retained that demonstrate consistency between the mainframe record count and the record count of the processed data.

DATA ACCURACY

Data accuracy controls ensure that the details of transactions are entered and processed correctly, and that printed output is not distributed to the user until it is checked for reasonableness. Our audit identified significant weaknesses in data accuracy controls.

AUDIT FINDING 7: EDIT CHECKS ARE NOT SUFFICIENT TO PREVENT INACCURATE INFORMATION FOR THE ETA 227, ETA 563, ETA 9002 A-D AND VETS 200 A-C REPORTS

Accuracy of the ETA 227, ETA 9002 A-D and VETS 200 A-C reports could not be asserted. Recovery activities are manually entered for the ETA 227 report, and birth dates of program participants are manually entered for the ETA 9002 A-D and VETS 200 A-C transaction; keying errors are inherent in this process. These critical dates could be entered incorrectly, thus greatly impacting the accuracy of the ETA 227, ETA 9002 A-D and VETS 200 A-C reports. We also found that ETA 227, ETA 9002 A-D and VETS 200 A-C transaction data had dates that were outside of this century. Strong input edit checks, i.e. accuracy controls, should govern this process, and more supervisory oversight should be employed.

Management should ensure that transaction data entered for processing are subject to a variety of controls to check for accuracy, completeness and validity. Procedures should also assure that input data are validated and edited as close to the point of origination as possible.

Recommendation: ESC management should add edit checks to ensure that all dates entered are accurate and valid. Edit checks should be placed in the code to ensure that no date greater than the current date or less than the current reporting period should be entered into the system. Also, edit checks to ensure that a participant's date of birth is reasonable should exist. This would ensure that manually entered dates will not fall outside of the correct reporting period, and that grouping by participants age are accurate.

Auditee's Response: As agreed in the meeting between ESC and audit staff, ESC will take the following actions to meet audit requirements:

For inputs to the ETA 227, ESC will determine the valid date range for manually entered dates and will implement edits to assure that these dates fall within the determined range.

DATA VALIDITY

Data validity ensures that the data entered into the application is valid. A division of roles and responsibilities should exist, which should exclude the possibility for a single individual to subvert a critical process. Our audit identified a significant weakness in the data validity controls.

AUDIT FINDING 8: IMPROPER SEGREGATION OF DUTIES EXIST IN THE REPORTING PROCESS FOR THE ATAAAR, ETA 563, ETA 9002 A-D, AND VETS A-C REPORTS

Inadequate segregation of duties exists in the reporting process to the federal government. The programmer who maintains the programs is also responsible for generating the reports. This weakness is heightened because this same programmer in many cases must manipulate the underlying data, thus creating an opportunity for transactions to become lost, removed or corrupt, and little to no supervision exists within this process. The reports affected by this inadequately designed process are the ATAAAR, ETA 563, ETA 9002 A-D, and Vets 200 A-C reports.

We also found for some reports the same programmer is responsible for verifying the accuracy of the report and is responsible for submitting the report to the federal agency. Subsequently, no controls exist to determine whether any changes have been made to the data, or who made them. The programmer is able to make adjustments to the created program without the review and approval of another employee. The design of this process violates ESC's policy that programmers should not have direct access to production data. ESC management should ensure segregation of duties is maintained and work performed is routinely verified for processing data.

Management should implement a division of roles and responsibilities that reduce the possibility for a single individual to compromise a critical process.

Recommendation: Proper segregation of duties should be implemented to ensure data is not changed. Emphasis should be placed on appropriate supervisory oversight by a knowledgeable employee who is familiar with the ATAAAR, ETA 563, ETA 9002 A-D, and Veterans A-C reports.

Auditee's Response: As agreed in the meeting between ESC and audit staff, ESC will take the following actions to meet audit requirements:

ESC agrees to implement division of roles and responsibilities where practical and to introduce additional supervisory oversight as a compensating control where appropriate.

DATA AUTHORIZATION

Controls are designed to ensure that access to data is appropriate and authorized and that access is granted on a need to know, need to use basis. The access control environment should consist of access control software and information security policies and procedures that are implemented appropriately to protect the application data. Our audit identified a significant weakness in data authorization.

AUDIT FINDING 9: PROGRAMMERS HAVE DIRECT ACCESS TO PRODUCTION DATA THAT PRODUCES THE FOLLOWING REPORTS: ATAAAR, ETA 563, TAPR, ETA 9002 A-D, AND VETS 200 A-C REPORTS

We found that programmers had direct access to manipulate underlying data that supported the aforementioned reports. In some cases, we found programmers manually inserting a series of statements into the databases used to prepare the reports submitted to federal government.

Management should ensure that personnel are performing only authorized duties relevant to their respective jobs and positions.

Recommendation: ESC management should limit programmer access to production data, and reassign the actual report creation and verification to another employee who is knowledgeable about these reports.

Auditee's Response: As agreed in the meeting between ESC and audit staff, ESC will take the following actions to meet audit requirements:

ESC agrees to implement division of roles and responsibilities where practical and to introduce additional supervisory oversight as a compensating control where appropriate.

DATA RETENTION

Data retention controls are designed to ensure that data is retained according to federal and state guidelines. Our audit identified a significant weakness in the data retention.

AUDIT FINDING 10: RETENTION OF SUPPORTING DOCUMENTATION FOR ETA 563, TAPR, ATAAAR, ETA 9002 A-D AND VETS 200 A-C REPORTS

Management does not retain the extract files used to generate ETA 563, TAPR, ATAAAR, ETA 9002 A-D AND VETS 200 A-C reports. Since the data used to create the reports is dynamic, the reports, as well as the extract files used to create the reports, represent a snapshot in time that cannot be replicated unless management retains the extract files. Since management saves this supporting documentation into an extract file in order to generate the report, it should continue to retain the extract file for audit purposes, as instructed by federal guidelines.

During our audit, we attempted to replicate the quarter ending December 31, 2007, by extracting transactions for this period and running this information through scripts set-up as required by ETA 563, TAPR, ATAAAR, the ETA 9002 and VETS 200 instructions.

The results proved that we could not exactly agree to what was reported to the federal government, and the only explanation provided was that timing differences may have caused a disparity between our reports.

Failure to retain the extract files associated with the reports significantly reduces the auditability of the underlying data, which, in turn, impairs the integrity of the reports.

Recommendation: Management should retain the extract files used to generate reports. This will enhance both the integrity and auditability of these reports.

Auditee's Response: As agreed in the meeting between ESC and audit staff, ESC will take the following actions to meet audit requirements:

Create and retain requested extracts of the data for auditing purposes in accordance with federal guidelines.

[This Page Left Blank Intentionally]

ORDERING INFORMATION

Audit reports issued by the Office of the State Auditor can be obtained from the web site at www.ncauditor.net. Also, parties may register on the web site to receive automatic email notification whenever reports of interest are issued. Otherwise, copies of audit reports may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Telephone: 919/807-7500

Facsimile: 919/807-7647