THIRD PARTY REVIEW

Department of Central Management Services
Bureau of Communication and
Computer Services

July 2010

TABLE OF CONTENTS

REPORT DIGEST

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATION AND COMPUTER SERVICES

THIRD PARTY REVIEW
For the Year Ended:
June 30, 2010

Release Date:
July 2010

State of Illinois
Office of the Auditor General
WILLIAM G. HOLLAND
AUDITOR GENERAL

To obtain a copy of the Report contact:
Office of the Auditor General
Iles Park Plaza
740 E. Ash Street
Springfield, IL 62703
(217) 782-6046 or TTY (888) 261-2887

This Report Digest and Full Report are
also available on
the worldwide web at

http://www.auditor.illinois.gov

INTRODUCTION

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/405-10; 20 ILCS 405/405-20; 20 ILCS 405/405-250; 20 ILCS 405/405-255; 20 ILCS 405/405-260; 20 ILCS 405/405-270 and 20 ILCS 405/405-410). To fulfill its responsibilities, the Department operates the Central Computer Facility (CCF), the Communications Center, and branch facilities. Through its facilities, the Department provides data processing services to approximately 100 user agencies.

The Department is mandated to manage or delegate the management of the procurement, retention, installation, maintenance, and operation of all electronic data processing equipment used by State agencies to achieve maximum economy consistent with development of adequate and timely information in a form suitable for management analysis, in a manner that provides for adequate security protection and back-up facilities for that equipment.

The Department functions as a service organization providing computing and telecommunication resources for State agencies' use. The Department and the agencies that use the Department's computer resources share the responsibility for maintaining the integrity and security of computerized data and functions.

We reviewed data processing general controls at the Department primarily during the period from January 4, 2010 to May 31, 2010. We performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific control objectives and procedures we considered necessary to evaluate the controls.

We also reviewed application controls for systems maintained by the Department for State agencies' use. The systems reviewed were the Accounting Information, Central Payroll, Central Inventory, and Central Time and Attendance Systems.

AUDITORS' OPINION

The procedures were generally sufficient to provide reasonable, but not absolute, assurance that relevant general and application control objectives were achieved.

WILLIAM G. HOLLAND, Auditor General

ILLINOIS DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATION AND COMPUTER SERVICES

STATISTICS	2010
Mainframes	4 Units Configured as 11 Production Systems and 6 Test Systems 1 Unit Configured as 5 Systems for Business Continuity
Services/Workload	Impact Printing – 7.2 Million Lines per Month Laser Printing – 14.5 Million Pages per Month
State Agency Users	100
Bureau Employees	2007 -- 748 2008 -- 708 2009 -- 679 2010 -- 641
Historical Growth Trend**	2007 -- 3,962 -- MIPS 2008 -- 4,018 -- MIPS 2009 -- 4,035 -- MIPS 2010 -- 3,908 -- MIPS -- Million Instructions Per Second ** In the month of April for each year listed

Information provided by the Department – Unaudited

DEPARTMENT DIRECTOR AND DEPUTY DIRECTOR/BUREAU MANAGER
During Audit Period and Current: Director: James Sledge During Audit Period: Deputy Director/Bureau Manager: Doug Kasamis (7/1/2009 to 9/30/2009) Currently: Acting Deputy Director/Bureau Manager: Rich Fetter (10/1/2009 to present)

Springfield Office:

Iles Park Plaza
740 East Ash - 62703-3154
Phone: 217/782-6046
Fax: 217/785-8222 TTY (888) 261-2887

Chicago Office:

State of Illinois Building - Suite S900
160 North Lasalle – 60601-3103
Phone: 312/814-4000
Fax: 312/814-4006

Office Of The Auditor General
William G. Holland

AUDITOR'S REPORT

The Honorable William G. Holland
Auditor General - State of Illinois

We have examined the accompanying description of controls related to the systems and procedures used to control data processing operations at the Bureau of Communication and Computer Services of the Department of Central Management Services (Department). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the Department's controls that may be relevant to a user agency's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user agencies applied the controls contemplated in the design of the Department's controls; and (3) such controls had been placed in operation as of May 31, 2010. Our examination started in July 2009 and primarily performed between January 4, 2010 and May 31, 2010, was limited to controls at the Department. The control objectives were specified by management of the Department. Our examination was performed in accordance with the Illinois State Auditing Act, applicable generally accepted auditing standards, and "Government Auditing Standards" issued by the Comptroller General of the United States. We included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

The accompanying description identifies several controls that were deemed inaccurate, based on test work performed. The identified controls are outlined in Appendix C.

In our opinion, except for the matters referred to in the preceding paragraph, the accompanying description of the aforementioned systems and procedures presents fairly, in all material respects, the relevant aspects of the Department's controls that had been placed in operation as of May 31, 2010.

Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user agencies applied the controls contemplated in the design of the Department's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in the body of the report, to obtain evidence about their effectiveness in meeting the related control objectives, listed in the body of this report, during the period from January 4, 2010 through May 31, 2010. The specific controls and the nature, timing, extent, and results of the tests are listed in the body of the report. This information has been provided to the Department's user agencies and to their auditors to be taken into consideration, along with information about the internal control at user agencies, when making assessments of control risk for user agencies. In our opinion, the controls that were tested, as described in the body of the report, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in the body of the report were achieved during the period from January 4, 2010 through May 31, 2010.

The relative effectiveness and significance of specific controls at the Department, and their effect on assessments of control risk at user agencies, are dependent on their interaction with the controls and other factors present at individual user agencies. We have performed no procedures to evaluate the effectiveness of controls at individual user agencies.

The description of controls at the Department is as of June 30, 2010, and information about tests of the operating effectiveness of specified controls covers the period from January 4, 2010 through May 31, 2010. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specified controls at the Department is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended for the information and use of the Auditor General, the General Assembly, the Legislative Audit Commission, the Governor, Department management, affected State agencies, and auditors of the State agencies. However, this report is a matter of public record and its distribution is not limited.

Willi J. Say

William J. Sampias, CISA
Director, Information Systems Audits

Mary K. Lovej

Mary Kathryn Lovejoy, CPA, CISA
Information Systems Audit Manager

May 31, 2010

REPORT SUMMARY

INTRODUCTION

The Department of Central Management Services' (Department) Bureau of Communication and Computer Services (Bureau) carries out statutory responsibilities relating to data processing and telecommunication services (20 ILCS 405/405-10; 20 ILCS 405/405-20; 20 ILCS 405/405-250; 20 ILCS 405/405-255; 20 ILCS 405/405-260; 20 ILCS 405/405-270; and 20 ILCS 405/405-410). To fulfill its responsibilities, the Department operates the Central Computer Facility (CCF), the Communications Center, and branch facilities. Through its facilities, the Department provides data processing services to approximately 100 user agencies (see Appendix B).

The Department is mandated to manage or delegate the management of the procurement, retention, installation, maintenance, and operation of all electronic data processing equipment used by State agencies to achieve maximum economy consistent with development of adequate and timely information in a form suitable for management analysis, in a manner that provides for adequate security protection and back-up facilities for that equipment.

The Department functions as a service organization providing computing and telecommunication resources for State agencies' use. The Department and the agencies that use the Department's computer resources share the responsibility for maintaining the integrity and security of computerized data and functions. The Third Party Review addressed controls which were included in the Department's Description of Control. The control associated with the midrange environment for the 11 consolidated agencies was not included in the Department's Description of Control and, therefore, not included in our review. In addition, we did not review the controls over the 11 consolidated agencies' environments or other user agencies. As a result of our review, we identified numerous control areas that should be reviewed and addressed by user agencies and their internal and external auditors (see Appendix A).

We reviewed data processing general controls at the Department. We performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific control objectives and procedures we considered necessary in the circumstances to evaluate the controls.

We also reviewed or confirmed application controls for the following systems maintained by the Department for State agencies' use:

- Accounting Information System;
- Central Payroll System;
- Central Inventory System; and
- Central Time and Attendance System.

We identified several control deficiencies that appear in pages 36 through 185 of the report.

The content of the report and individual controls were discussed with the Department throughout the course of the review. The Department concurred with the conclusions and recommendations contained in the body of the report.

We will review progress towards the implementation of our recommendations during the next Third Party Review.

SERVICE ORGANIZATION - DESCRIPTION OF CONTROLS

The following Description of Controls section (pages 5 through 33) consists of text provided by the Department of Central Management Services.

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
BUREAU OF COMMUNICATION AND COMPUTER SERVICES
DESCRIPTION OF CONTROLS

Personnel

The Department has the following controls in place to ensure the Department is adequately staffed with qualified individuals and provide an appropriate training program.

- A detailed organizational chart is maintained.
- Shared Services provides BCCS monthly reports citing the employees name and the due date of the evaluation. Monthly, BCCS personnel sends these reports to managers.
- Performance evaluation dates are tracked in BCCS Personnel database.
- Personnel hires are subject to the educational requirements, experience, and the specialized skills defined in position descriptions.
- Upon termination of an employee, communication occurs between the Division Manager/manager/supervisor and Workforce Development and Logistics Manager to assess filling the vacancy.
- CMS Policy Manual is given to all new full time employees. Updates to the Personnel manual or policies are e-mailed to BCCS staff. Employees are required to sign an acknowledgement form.
- Boilerplate language is included in vendor contracts regarding:
  Compliance with the Law
  Background check
  Confidentiality
- Training objectives are defined by supervisor and employee during the evaluation process.
- BCCS Workforce and Logistics Office maintain a spreadsheet of staff and their training requested and received.

Strategic Planning

The Department has the following controls in place to ensure the IT resources are in line and support the mission and objective of the Department.

- Strategic Planning Document.
- Information Gathering - BCCS managers and technical subject matter experts meet and request information on a regular basis from our existing vendors, other technology providers, and industry experts (Gartner, etc.) to monitor technology trends, existing services and to ensure that our services are competitive.

- Priority Meetings - The BCCS Executive Team and other key leaders in the BCCS organization hold Leadership Priority Meetings on a regular basis to track the progression of all priority projects and procurements.
- Architectural Review Board Meeting – BCCS conduct ARB meetings with consolidated agencies, Illinois State Police, Department of Children and Family Services and the Department of Corrections to provide updates on technology initiatives, discuss technology needs and issues as well as share strategic plans.
- Competitive Procurement - BCCS utilizes the competitive procurement process to ensure that the technology equipment, services and support are competitive and meet the needs of customers
- IT Governance - BCCS utilizes the IT Governance Process to ensure that proposed IT projects align with strategic plans
- Executive Planning Sessions – As needed, members of the BCCS Leadership team meet to exchange and share information. The team then uses this information along with other pertinent information to establish and make necessary alternation to Bureau strategies.
- Telecommunication Coordinator Meetings – Each agency must establish at least one agency telecommunication coordinator to order BCCS telecommunication related services. BCCS conducts Telecommunication Coordinator Meetings to share information and to give agencies the opportunity to provide input on needed services.
- CIO Forum – BCCS conducts periodic meetings with State Agency CIOs and Senior IT managers to share information on broad issues that may affect the use of technology in Illinois Government. The participants can present topics and provide input on what is presented.
- A set of guiding principles were established to assist in aligning projects and activities with the BCCS mission and objectives. BCCS leadership continues to work with the CIO of the State, and other IT Leaders to identify opportunities to improve the overall delivery of IT services based upon the guiding principles.
- BCCS Leadership Team is responsible for reviewing and addressing changes in management that would affect achieving the Bureau’s mission and objectives. Inadequate staffing and competency levels can have a direct impact on the bureau’s ability to meet the mission.
- BCCS staffs actively participate in a variety of meetings and committees such as the Human Services Framework, Illinois Terrorism Task Force Committees, etc. Through BCCS participation we can work to ensure changes in technology / management are considered in meeting the goals and objectives.

IT Governance

The Department has the following controls in place to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.

- The IT Governance Policy defines the scope, roles and responsibilities of the process.
- BCCS Leadership discusses strategies and objectives in the regularly held BCCS Priorities Meetings.

- IT Governance reviews Governance documents and procurements and communicates / works with stakeholders as necessary relative to strategies and objectives.
- IT Governance stays in communication with the State CIO relative to strategies and objectives.
- The Governance website, www.illinois.gov/governance, provides up-to-date governance information for stakeholders.
- IT Governance meets with stakeholders in person and via conference calls.
- The EPM Portal provides access to agency staff designated by state agencies to view and maintain information relative to their chartered projects.

Billing-SSRF and CRF

The Department is statutorily authorized to provide IT and telecommunication services to State agencies, boards, and commissions. The agencies are billed for services provided and remit payment to the Statistical Services Revolving Fund (SSRF) and the Communications Revolving Fund (CRF).

SSRF

- The Komand system is utilized to compile the SSRF billings. The system provides a means for charging resource utilization back to users.
- The Komand procedures assist users of the system.
- The SSRF Billing procedures assist staff with monthly billings.
- Reports are produced and verified against each other to ensure the accuracy of the billings.
- An Edit Check is completed to ensure the completeness and accuracy of each billing.

CRF

- The EMS11and AIS systems are utilized to compile the CRF billings.
- The CRF Billing procedures assist staff with the monthly billings.
- At the end of each billing, verification is performed to ensure the accuracy of the billings.
- Reports from each source are verified against each other to ensure the accuracy of information.

Outstanding Accounts/Billing Credits

- The Fiscal Operation Policy outlines the process for the collection of outstanding accounts.
- Delinquency letters are sent out when the criteria is met for the number of days invoice is past due. An account aging analysis is sent out on a quarterly basis.
- Requests for billing credits must be submitted in writing.
- All requests must be approved in writing.
- Approved billing credits are sent to Shared Services for processing.
- Shared Services processes the ARCM request form and posts the credit to the appropriate account in ARPS.

Billing Rates

- All expenditures are coded to cost centers and assigned to services through a cost accounting model
- Revenues for each service are compared to costs to determine the appropriateness of individual rates
- In order to comply with the federal requirements (A-87), an analysis is performed annually to determine profit/loss for each service. Excess revenues are subject to reimbursement to the federal government.

Vendor Management

The Department has the following controls in place to ensure compliance with third party software vendor's agreements

- The Department has a contract tool in the EPM system to alert staff when software contracts expire.
- The Department has procedural steps thru the Enterprise Service Request (ESR) process to ensure license compliance for all new software moves, adds or additions.
- The Department follows the Department's Fiscal Operating Policies and Procurement Guidelines established by BOSSAP.

Service Reporting and Service Delivery and Implementation

The Department has the following controls in place to ensure the effective communication between the Department and its customers regarding IT services and the level of services.

- The BCCS IT Services are defined within in the BCCS Service Catalog using a fairly consistent format which describes "What's Included", "What You Can Expect", "How You Can Help", "Need More Information", "Service Order Information" and rate information, when available, per service.
- The BCCS Service Catalog is used to define the level of IT service a customer can expect for defined services.
- The BCCS Service Site - Agency Reporting allows our customers to monitor BCCS performance as it relates to their agency.
- As of October 2009 agencies have the ability to run BCCS Service Performance Reports on demand from the BCCS Service Site.
- Agency direct access to the Remedy system allows generation of reports.
- The Service Reporting Team, Service Delivery and Implementation Team, CSC Quality Assurance team, and EUC Quality Assurance produce reports to identify trends, assessing and updating management on the information.

Internal Audit

The Department has the following controls in place to ensure that Information Technology (IT) issues are addressed through the internal audit process.

- The statewide Information Technology (IT) audit function is part of the Illinois Office of Internal Audit (IOIA), which addresses those entities under the Governor's jurisdiction. IT is addressed on a statewide basis, which reduces duplication of efforts and increase efficiencies.
- IOIA performs various types of IT audits including system development audits, application audits, special audits, and internal audits.
- The Fiscal Control and Internal Auditing Act (30 ILCS 10/2003 (a) (3)) mandates IOIA review the design of major new electronic data processing systems and major modifications to those systems. IOIA has established a process for identifying major new systems and major changes to existing systems for system development audits to determine which systems development projects are major and require an audit.

Agency Relations-

The Department has the following controls in place to ensure that information is identified, captured and communicated in an appropriate form, timeframe, and appropriate parties.

- The Department utilizes the following methods to ensure agencies are made aware of significant events/changes:
    - The Department coordinates changes for the Bureau website, www.bccs.illinois.gov, which serves as a central location for communicating available services including the Service Catalog, key contact information, forms and guides for requesting services, announcements/bulletins, and a variety of other Bureau information.
    - The Department also maintains the CIO Service Site at cms.partner.illinois.gov/bccs/Service/default.aspx, where all consolidated agency communications are stored and maintained.
    - The quarterly customer-focused newsletter is published to provide another vehicle for sharing information with our customers. The newsletter is distributed to telecommunications and IT customers via email and is also posted to the Bureau website.
- The Department's AR mailbox, CMS.BCCS.agencyrelations@illinois.gov, is an email box that allows customers to document their questions or concerns. A link to this mailbox is available from the BCCS website.
    - The Department's AR staff monitors the mailbox on a regular basis to address any customer questions or concerns. They research any issues that they cannot immediately address to provide timely, accurate responses.

Continuous Service

The Department has the following controls in place to minimize the risk of disruption of services for its mainframe processing environment.

- The Recovery Methodology provides guidance and materials for the restoration of the various environments.
- The Recovery Activation Plan provides instructions and actions required when recovering CMS/BCCS computing facilities and services.
- The Department has a process where user agencies periodically update the categorization of Criticality and Recovery Time objectives provided in the Business Reference Module (BRM).
- The IT Recovery Policy outlines the individual agency's responsibility to update the BRM with critical resources and timeframes for recovery.
- The Department has contracted with a recovery vendor to provide an alternate recovery data processing facility.
- The Department has contracted with a vaulting vendor to store in its vault backup data and recovery procedures required to restore critical IT infrastructure.
- The Department conducts periodic exercises to help ensure recovery requirements can be met.

Customer Management Center

The Customer Management Center (CMC) provides 24/7 network support for the State of Illinois. Additionally, after 5 p.m. and during non-business hours, the CMC provides help desk support for voice, wireless, and data services.

The Department has the following controls in place to ensure that customer queries, questions and problems are investigated and timely resolved.

- Incident tickets are initiated by a constituent call or discovered by a proactive monitoring system.
- ICN Remedy is utilized to log/track incident tickets.
- The CMC Sharepoint site contains methods and procedures to assist staff with incident tickets.
    - MP ICN Remedy Ticket Procedure and MP CMS Remedy Login Procedure
- ICN Remedy ticket logs and reports are utilized in identifying problem trends and recurring problems.
    - Reviews are completed by supervisors who may escalate to internal, external teams.
- The CMC Sharepoint site contains methods and procedures for the management of vendors.
- The CMC monitors the IT infrastructure utilizing a monitoring system.
    - The CMC Sharepoint site contains procedures for responding to alarms.

Communications Solution Center (CSC)

The CSC is responsible for providing Tier 1 support for Telecommunications (excluding Illinois Century Network and Radio) and IT services.

The Department has the following controls in place to ensure that customer queries, questions and problems are investigated and timely resolved.

- The CSC is a single point of contact (SPOC) where client solutions are handled for different technologies and simplifying end user support.
- The CSC is responsible for managing timelines and the value of the products and services offered through the CSC Service Desk and the vendors and internal teams supporting those products and services.
- The CSC has processes and guidelines in place for enterprise-wide management, escalation and notifications, and other operational needs.

Telecommunications Service Desk

The Telecommunications Service Desk is responsible for maintenance and provisioning of voice, video, data and wireless systems and services for State agencies, departments, constitutional officers, commissions, boards, universities and institutions.

The Department has the following controls in place to ensure that customer queries, questions and problems are investigated and timely resolved.

- The Telecommunications Service Desk handles all calls for telecommunications services during regular business hours Monday thru Friday 8am through 5pm, excluding ICN and Internet calls which are routed directly to the CMC.
- All telecommunications service calls outside regular business hours and on holidays are handled by the CMC.
- The Help Desk records all reported incidents in the Remedy Help Desk module. Customers contact the Help Desk via phone to report an incident. The Help Desk is responsible for all reported incidents from the time reported until resolution and confirmation from the customer is achieved. Procedures exist for the Help Desk task.
- Monthly reports are generated from the Remedy system based on a fiscal year to track and monitor vendor performance levels for voice related services. These figures are reconciled with the appropriate vendor(s). The CSC managers and Quality Assurance staff attend a quarterly meeting with the vendor(s) to review task related reports.
- The Provisioning unit receives forms via email or mailed paper copies from the authorized agency coordinator. All telecommunications changes require a request form. Different forms are required for different services. Data requests require a Telecommunications Data/Intercity Service Request form (TDR); voice and cellular requests require a Telecommunications Service Request (TSR); paging requests require a Paging Service Request (PSR); IWIN requests require a Wireless Service Request (WSR) form.

- Each agency head delegates, in writing, a telecommunications coordinator(s) authorized to expend funds. The Telecom Coordinator database is maintained by the CSC Administration staff and an alternate. The agency coordinator is responsible for submitting the appropriate request forms to the Telecommunications Service Desk for all telecommunications changes. The CSC Provisioning staff is responsible for verifying the submitter is an authorized coordinator in the database. The coordinators can locate the instructions for completing these forms on the Telecom Web site (http://bccs.illinois.gov/telecom/) and are provided guidance by the Provisioning staff when necessary. Procedures exist for the Provisioning task.
- The agency coordinators have access to EMS and can check status of their agency orders only. The EMS system tracks ordered facilities and telecommunications equipment. The inventory module provides the asset's recurring monthly charge, location information, 'AU' code, maintenance vendor description, catalog description and model description in addition to user name, tag number and serial number if applicable to the inventory item. The inventoried asset's installation cost can be found for all rated catalog codes in the EMS Catalog Table. Anytime an inventoried piece of equipment is installed, removed or moves from one location to another, an order is entered into the EMS system to update the system inventory.
- Tagged data equipment is received and tagged by Business Services' warehouse staff while tagged voice equipment is sent directly to the site. A Property Control Form (PCF) is completed for newly tagged voice systems and attached to the original invoice before it is sent to Business Services for processing and entry into the Common Inventory System (CIS). The voice system is tagged by the Consulting and Procurement staff at the time of acceptance. Tagged data and voice equipment listed in EMS is reconciled to the listed equipment in CIS annually by Business Services. Discrepancies are reported to CSC management and investigated. Appropriate reconciliation is then taken.
- Monthly reports are generated from the EMS system based on a fiscal year to track and monitor vendor performance levels for completion of voice orders in the Springfield and Chicago dedicated areas, the non-dedicated areas, non-routine orders and the overall vendor performance levels. These figures are reconciled with the appropriate vendor(s). The CSC managers and Quality Assurance staff attend a quarterly meeting with the vendor(s) to review task related reports.
- The Consulting and Procurement unit provides agencies with an assigned Communications Systems Specialist 2 (CSS2). There is one Consulting and Procurement staff member in the JRTC Building in Chicago. The CSS2s work closely with the agency coordinators to consult and analyze their present and future telecommunications needs and design systems to meet those requirements in the most efficient and economical manner. The CSS2s are responsible for managing non-routine service requests. Procedures exist for the Consulting and Procurement unit tasks.
- This unit is also responsible for managing master contracts and site/service specific contracts for telecommunications equipment and services. Network Services assists this unit with the review of TDRs that are related to the ICN backbone and WAN requests for

the agencies statewide. The BCCS Shared Services teams are engaged on telecom requests for the Consolidated Agencies when systems require PCs, Servers, and connectivity to the CMS network.

IT Service Desk

The CSC IT Service Desk is responsible for providing Tier 1 IT technical and end user support to the consolidated agencies as well as the multiple boards, commissions and non-consolidated agencies. The IT Service Desk is the single point of contact for reporting IT incidents and requesting new services.

The Department has the following controls in place to ensure that customer queries, questions and problems are investigated and timely resolved.

- The IT Service Desk is staffed during normal business hours Monday thru Friday 8 am to 5 pm, with extended coverage from 8 am to 4 pm on Saturday and Sunday for HFS and DHS. Evening coverage for HFS and DHS is provided by production operations staff working at 120 West Jefferson in Springfield. Appropriate security is inherent to the tool used.
- Customers contact the IT Service Desk via phone or email to report an incident. The Service Desk staff opens a ticket in BCCS Remedy and records the category, type, and item (CTI), as well as the customer name, agency, contact and demographic information and a detailed incident description. If the IT Service Desk is unable to resolve the incident, the ticket is assigned to Tier 2 or Tier 3 support teams based on the CTI and/or predefined summary field. Procedures exist for the Help Desk task.
- The IT Service Desk receives an Enterprise Service Request form (ESR) from an authorized IT coordinator for all IT changes. The IT Service Desk has standardized on the ESR process and the intake of service requests in the Remedy system for all consolidated agencies. Service requests are submitted via email.
- Each agency head delegates, in writing, an IT coordinator(s) authorized to expend funds. The IT Coordinator database is maintained by Agency Relations. The IT coordinator is responsible for submitting the appropriate request forms to the IT Service Desk for all IT changes. The IT Service Desk staff is responsible for verifying the submitter is an authorized coordinator in the database. The coordinators can locate the instructions for completing these forms on the Bureau's Web site (http://bccs.illinois.gov/forms_it.htm) and are provided guidance by the IT staff when necessary. Procedures exist for the ESR processing task.

End User Computing

End User Computing (EUC) provides maintenance, support and security of the personal computer infrastructure and provides desktop and laptop services.

The Department has the following controls in place to ensure that customer queries, questions, and problems are investigated and resolved timely.

- The following policies are utilized to assist staff in their duties:
    - End User Computing Device Standard
    - CMS Desktop/Laptop Personal Computer Standard
    - EUC IT MAC Technical Assistant Procedure
    - IBM Technical Services Program (TSP) Time and Materials (T&M) Billing Sign-Off Procedure
- Remedy Action Request System is used to initially log incidents (help desk tickets) and requests (ESRs).
    - Versions of addendums are attached to ESRs providing the changing details associated with the ESR
    - The work log in Remedy is used for incidents and ESRs to document activity
    - The Remedy Action Request System audit trail for the incident or ESR will document a change in the assignment or status
    - Remedy Action Request System is used to capture the priority of the incident or ESR
    - Priorities are established by the customer at the time the incident or ESR is initiated with IT Service Desk
    - Customers can call the IT Service Desk for updates on any incident or ESR
    - Customers receive a system generated email from Remedy Action Request System when the status of an incident or ESR changes (confirmation is needed on what status changes generate an email)
- The work log within Remedy Action Request System is used by anyone that engages in the working of an incident or ESR to record the activity performed
- Tasks within Remedy Action Request System are used for ESRs that require multiple shared services teams to be engaged in the request
- Technical assessment is a task used to initially reach out to the customer to confirm request
- The Customer Satisfaction task is used by the IT Service Desk to confirm completion and customer satisfaction.

Quality Assurance

The Infrastructure Quality Assurance and Methods group act as facilitators for organizing, planning and controlling work activities for the Infrastructure Services Division related to Agency IT projects.

The Department has the following controls in place to ensure the ongoing performance monitoring against predefined objectives and implementation of a program for continuous improvement of IT services is achieved.

- Process and procedures that govern this process are located in the IQAM Guide.
- The EPM Portal and Remedy are utilized to monitor projects.

- The EPM Portal and meetings are utilized to communicate with the project owners.

Change Control

The Department has the following controls in place to ensure that changes are authorized, tested, approved, properly implemented and documented.

- The Change Management Policy and BCCS Remedy Change Management Guide to manage changes.
    - State of Illinois – Dept. of Central Management Services – Change Management Policy https://bccs.portal.illinois.gov/exec/centrep/ed/plcpub/Change_Management_Policy.pdf
    - BCCS Remedy Change Management Guide https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx
- The Remedy Action Request System is used to request and track changes.
- Changes are approved utilizing and/or in accordance with:
    - Remedy Action Request System
    - BCCS Remedy Change Management Guide
        - Business Owner Review
        - Validate Change Variables – Technical / Business

      https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx
    - State of Illinois – Dept. of Central Management Services – Change Management Policy https://bccs.portal.illinois.gov/exec/centrep/ed/plcpub/Change_Management_Policy.pdf
- The Remedy Action Request System ensures the proper authorization of changes are tracked
- The BCCS Remedy Change Management Guide ensures all changes are properly tested before being placed into production.
    - Validate Change Variables – Technical / Business (Change Management is responsible for ensuring Testing Documentation is attached to "High" Impact Changes; Shared Services Teams are responsible for level of testing)
- The BCCS Remedy Change Management Guide outlines the requirements for the follow-up once a change has been completed.
    - Resolve Change
    - Conduct Post Implementation Review https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx
- Several different communication mechanisms are in place to ensure all applicable parties are appropriately and timely notified of an upcoming change.
    - Change Advisory Committee Meeting
    - 30 Day Outage Report by Agency
    - Change Advisory Committee Meeting Minutes
    - Change Detail Report (Next 14 Days)

    - Enterprise Change Schedule (Next 90 Days)
- The Department has the following controls in place to manage the moves of hardware and/or software configuration changes into production.
    - Assess Request Content & Readiness (Technical and Business)
    - Change Request Approval
- The Department has the following controls in place for controlling emergency changes.
    - Authorization
        - State of Illinois – Dept. of Central Management Services – Change Management Policy. https://bccs.portal.illinois.gov/exec/centrep/ed/plcpub/Change_Management_Policy.pdf
        - BCCS Remedy Change Management Guide. https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx
    - Testing
        - Change Management is responsible for ensuring Testing Documentation is attached to "High" Impact Change Requests; Shared Services Teams are responsible for level of testing.
    - Approving
        - State of Illinois – Dept. of Central Management Services – Change Management Policy. https://bccs.portal.illinois.gov/exec/centrep/ed/plcpub/Change_Management_Policy.pdf
        - BCCS Remedy Change Management Guide. https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx
    - Implementation.
        - BCCS Remedy Change Management Guide. https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx

Security Administration

The Department has the following controls in place to ensure security is adequately addressed.

The following internal documents provide management with an overall security strategy and framework.

- A document entitled "Secure Illinois Strategy" exists which lays out a simple roadmap for Department security services.
- A document called the Security and Compliance Solutions Security Program updated on 12-15-09.
- A document entitled "Risk Management Framework" describes the approach for assessing and defining risk in the operation.

The following controls apply to users of Department services.

- Policies governing the computing environment have been developed and are available at http://bccs.illinois.gov/it_Policies.htm. The website is updated as policies are developed or changed. As of December 2009, the following policies were on the website.

  IT Policies
  - Data Classification Policy
  - Enterprise Desktop/Laptop Policy
  - General Security for Statewide IT Resources Policy
  - General Security for Statewide Network Resources Policy
  - IT (Information Technology) Recovery Policy
  - IT Resource Access Policy
  - Laptop Data Encryption Policy
  - Midrange Backup Policy
  - Statewide CMS/BCCS Facility Access Policy

  General Policies
  - Change Management Policy
  - Data Breach Notification Policy
  - ESI Retention Policy
  - IT Governance Policy
  - Mobile Device Security Policy
  - Wireless Communication Device Policy

  Policy update memos are distributed periodically to impacted users to announce updates to the policies.

- Security awareness is promoted by placing relevant information on an enterprise accessible web site http://bccs.illinois.gov/security/awareness.htm where security related news releases, tips, posters, and guidelines can be viewed. In addition, security related information is periodically emailed to user agency contacts.
- Security assessments are conducted by the Department's Technical Safeguards unit. Results of those assessments are made available to appropriate BCCS staff that has responsibility for remediation.
- Cyber security incident procedures exist and responses are addressed by Department's Technical Safeguards unit.
- Security authorization lists are routinely updated and reviewed on a bi-annual basis with the user agencies.
- Security alerts involving critical patches, vulnerabilities and new threats are routinely received via MS-ISAC Alerts and MS Patch Tuesday Alerts. This information is evaluated by the Technical Safeguards unit. If the information received warrants attention, the pertinent information is provided to necessary BCCS personnel for action. This is done to prevent security breaches and incidents.

- The ESR process for provisioning access is used to control user access to resources.

The following additional controls apply to Department staff members.

- Security Awareness Training – Security awareness training is provided on an annual basis to CMS employees (both State employees and contractors) via a third party (Webstart). The presentation is currently tailored general security topics, with increased specificity and details as the training program progresses.. The training is designed to raise the general understanding of computer security within the BCCS community.
- Compliance Acknowledgement Forms - Whenever new security policies are approved and distributed, the recipients must sign an acknowledgement form indicating that they have received and read the policy.
- RACF violations for BCCS staff are reviewed on an ongoing basis. Violation reports are provided to the individual responsible, requesting an explanation of the violation. These explanations are then reviewed for reasonableness.
- 90 day Stale RACF account report – This report is run on a regular basis to locate RACF Ids that have not been used within 90 days and may need to be removed. The list is generated and then reviewed by individuals within BCCS. Any Ids noted for deletion are revoked.
- 90 day Stale AD account report. This report is run from the Control Compliance Suite (CCS) and is currently being to monitor stale AD accounts within CMS. This list is reviewed by ISD and used for AD cleanup.

Physical Security

The Department has the following controls in place to ensure physical security controls exist to promote security.

Two primary facilities are used to conduct computer operations for the State; The Central Computer Facility (CCF) and the Communications Building.

- Physical security controls at the Central Computer Facility and the Communications Building in Springfield include:
  - Security guards;
  - Video cameras strategically located inside and outside the buildings;
  - Proximity card readers; and
  - Real property keys.

<u>Security Guards</u>

Security guard services are contracted and the buildings are staffed with 24/7 security guard protection. Fundamental activities of security guards include but may not be limited to access control, incident reporting, and perimeter patrol.

Security guard services and requirements are outlined in the following:
Special instructions - are instructions that are communicated via email to the security guards on duty and then included in the Pass Down Book for future review and reference.
Security Guards issue temporary badges (with limited access rights) to visitors, and to employees who forget their assigned access card. Those issued a temporary badge must sign the Building Admittance Register recording their name and badge number. Security Guards have been instructed to inventory temporary badges at the start of each shift to ensure accountability.

Video Surveillance
Networked video cameras monitor exterior doors and sensitive interior entrances. Security Guards as well as the Bureau Physical Security Coordinator have remote view capability for all networked cameras.

Proximity Card Readers (H/V System)
Proximity card readers that require authorized access cards are located throughout the interior and exterior of the buildings to control and restrict access. Access cards are issued to Department personnel based on business need and job responsibility.

The Bureau Physical Security Coordinator processes emailed access requests from designated authorities as identified in the Approval Authorization Matrix and Badge Production Matrix. The H/V System Administrator's Manual contains instructions to create the physical access card.

The H/V system records and logs the use of access cards. Reports can be produced to list who has access to what buildings and locations. In addition, audit trail reports that outline the use (time and location) of access cards can be produced.

Absentee limits and restrictions on employee pass-back are activated to help control physical access to buildings.

Access cards are FIPS 201-1 compliant and contain text that outlines cardholder responsibilities as well as instructions on what to do if a lost badge is found. Once the Physical Security Coordinator is notified of employee separation or other circumstance for disabling access, card access is disabled.

An additional control beyond disabling separated employee's access card, the direct supervisor is supposed to collect the employee's access card as outlined in the Department's Policy Manual.

Maintenance of Real Property Keys
The Bureau of Property Management (BOPM) is responsible for issuing and maintaining real property keys.

Preventative protection against environmental factors at the CCF and Communications facilities include fire suppression and detection systems. Fire suppression and detection systems on the third floor of the Central Computer Facility and at the Communications Building are installed and tested on a regular basis.

To mitigate the risk of a power failure, the Central Computer Facility is supplied by two different sources and is equipped with an uninterruptible power supply (UPS). Within an allotted time the Department's generators will engage. The Department has a service contract for the UPS to provide routine preventive maintenance and remedial services as required.

The H/V system control panels have their own UPS to provide power to the control panels, and the access control devices they support. A separate UPS module supplies uninterruptible power to certain electric locks.

Two other facilities are also used to conduct computer-related operations for the Department; the Harris Facility and the Clinton Facility.

- Physical security controls protecting the Department's assets housed at the Harris Facility include:
  - Security guards in the front entry way;
  - Video cameras strategically located inside and outside the building;
  - Proximity card readers requiring an active Access Card to allow entry; and
  - Limited access, brightly colored badges for use by individuals entering the building to pick up printed output from the I/O Control area.

- Physical security control protecting the Department's assets at the Clinton Facility include:
  - Security guards during business hours.
  - Cipher locks.

Operations-Systems Operation Center

The Department has the following controls in place to ensure data integrity and that the IT infrastructure can resist and recover from errors and failures.

- All procedures utilized by the Systems Operations Center (SOC) are documented in a central location called the D.P. Guide which resides on the groups SharePoint site as well as one hardcopy that is maintained in the event that the SharePoint site is unreachable.
- The Department monitors the IT infrastructure and related events utilizing:
  - Mainframe consoles for each of the mainframe systems to monitor all jobs; job performance; tape processing; system utilization, etc.
  - AOC – Automated Operations Control to monitor all teleprocessing and system tasks on all mainframe systems which are routed through the FOCAL POINT so that the SOC has access to the information in a centralized location which can be accessed from all workstations in the SOC.
  - HMC – Hardware Management Console for monitoring and maintenance of mainframe-attached hardware components.

  - TIVOLI – which monitors all network activity.
  - What's Up Gold – which monitors all routers, servers and server applications.
- Daily Shift Report is populated by the Systems Operations Center recording any outages and issues which occur during the course of each day. This is then distributed via an automated mechanism in the Focal application.
- Shift Change Checklists are completed at the beginning of each shift in Systems Operations Center to ensure that all systems are running as designed.
- The Department is continuously monitored and assessed to meet the goals of the Department utilizing:
  - SYSLOG – maintains logs of all activity on each of the mainframe systems.
  - Automation Logging which monitors Job and System Task Maintenance on the mainframe systems.
- The Remedy Change Management System is utilized to coordinate and implement changes.
- Remedy is utilized to record and monitor incident resolution.

Operations-Input/Output Control

The Input Control monitors all production jobs, while Output Control is responsible for printing and distribution of all documents and reports generated.

The Department has the following controls in place to ensure the operations environment meets the realization of the Department's mission and goals.

- Jobs processed in the production environment run through CA-Scheduler or are manually submitted. Emails are sent in requesting specific jobs to be run.
- Security software ensures only authorized individuals are allowed to submit requests.
- The Department utilizes legacy policy and procedures to monitor jobs.
- The daily shift reports document the abends. Agency contact information, when the job was corrected and the cause are reported.
- The Department maintains a Job Call List for agency contacts.
- I/O daily shift reports which contain abends are emailed to the applicable agency.
- All reports are printed in a secure environment and depending on the requirements for privacy, HIPPA, personal information, financial information, they are either packaged and properly labeled prior to being sent out.
- Memorandums document the security controls for the distribution of reports.
- The Focal System contains a listing of individuals authorized to pick up reports.
- If the reports and documents are handled by our automated distribution software they are protected by security software.
- Legacy policies and procedures are utilized for printing and distribution.
- Monthly job performance reports are produced and submitted to management for review.

Operations-Production Control

Production Control ensures the production processing activities are documented and executed in accordance with approved schedules.

The Department has the following controls in place to ensure the operations environment meets the realization of the Department’s mission and goals.

- Jobs processed in the production environment run through CA-Scheduler or are manually submitted.
- Security software ensures only authorized individuals are allowed to submit requests.
- Production Control reviews and monitors all processes and procedures to ensure they follow documented standards for each legacy agency.
- The daily shift reports document the abends. Agency contact information, when the job was corrected and the cause are reported.
- All reports are printed in a secure environment and depending on the requirements for privacy, HIPPA, personal information, financial information, they are either packaged and properly labeled prior to being sent out.
- If the reports and documents are handled by our automated distribution software they are protected by security software.

Operations-Library Services

Library Services consists of four units: Tape Library, tape Media, Library Support and Tape Administration.

The Department has the following controls in place to ensure the operations environment encourages the realization of the Department’s missions and goals and that appropriate policies and procedures have been developed to protect information assets.

- The ISD Media Guide and the ISD Library Guide assist staff in their duties.
- Security software is utilized to ensure the integrity of the media.
- Automated Tape Management System retains critical tape information for specified amounts of time.
- Tape Admin uses reports listing all cart information
- CCF Tape Library uses various reports for inventory which are verified twice a year
- CCF Tape Library release/receipt of media done only after verification is authenticated thru Authorization list. Movement of any media is recorded with transmittal forms or printed broadcasts.
- Library Support verify all backups (daily, weekly, and monthly) and production to test moves completed successfully. Library Support staff verify backups and moves by reviewing jcl condition codes. And resolving any problems associated to ensure successful completion.

- Tape Admin reviews cart statistical reports and assigns dedicated carts to designated individuals
- CCF Media use consoles to monitor mainframe processing, LSM functions, and servers.
- CCF Media/Tape Library report any LSM, server, or drive problems immediately to the SOC or designated Technical Support staff.
- Library Support complete and verify mainframe library maintenance when requested.
- Production libraries are protected by security software to allow only authorized moves.

Operations-Storage and Backup

The Department has the following controls in place to ensure the allocation, backup and removal of storage for the mainframe.

- The Enterprise Storage and Backup (ESB) Guide contains procedures to ensure z/OS cleanups, restores, and DASD additions and deletions are completed successfully.
  - The ESB Guide also includes Weekly/Daily Cleanups, DASD Addition Checklist, DASD Removal Checklist, DASD Return to Spare, DASDadd, and ADRDSSU Restore.
- CA-Scheduler is utilized for the scheduling of backups.
- z/OS Backups are performed on the mainframe operating system data.
  - System data is backed up daily and weekly with the weekly copies sent to the regional vault.
  - Backups of non-operating system files are also performed by HSM.
  - These backups are controlled by the SMS routines and are set by the customer at allocation time. When the customer allocates a new file, a management class is assigned which determines how long the data is kept.
- System Automation notifies ESB when storage falls below a pre-determined threshold for SMS storage.
- The Command Center notifies ESB when the threshold limit for private pools falls below a pre-determined limit.
- ESB monitor Private Pool resources and notify agencies once a pre-determined threshold is met.
- An Enterprise Service Request (ESR) is utilized in requesting large amounts of disk space for SMS Pools.
- A Remedy ticket is utilized for special requests for disk space.

System Software-Zero Downtime Virtual Machine (z/VM)

The Department has the following controls in place to ensure the z/VM operating system has been configured to and controlled to promote security and integrity.

- Security software and system options are implemented to protect resources and data.
- Assigned Department staff is responsible for software installation, maintenance, performance monitoring, and security.

- User IDs and passwords are utilized to control access to z/VM.
- Agency security software administrators must submit a request to z/VM staff for a user to have access to z/VM.
- Access to the z/VM Directory is limited to z/VM staff.

System Software-Zero Downtime Operating System (z/OS)

The Department has the following controls in place to ensure the primary operating system (z/OS) has been configured and controlled to promote security and integrity.

- Security software and system options are implemented to secure libraries, and protect resources and data.
- Assigned Department staff is responsible for software installation, maintenance, performance monitoring, and security.
- User IDs and passwords are utilized to control access to z/OS.
- Agency security software administrators must submit a request to CMS security software staff for a user to have TSO access.
- CPU utilization is monitored and managed through the regular production of Resource Monitoring Facility (RMF) reports.
    - RMF reports are stored on a secured drive and are available to management.
- System activity is recorded via the selection of System Management Facility (SMF) options.
- Access to system consoles and direct access storage devices (DASD) are restricted by physical and logical security controls.

System Software-Customer Information Control System (CICS)

The Department has the following controls in place to ensure CICS has been configured and controlled to promote security and integrity.

- Security software and system options are implemented to protect resources and data.
- Assigned Department staff is responsible for software installation, maintenance, performance monitoring, and security.
- Three different levels of CICS support for users are provided:
  Level One – The Department supports only the CICS software. The customer is responsible for all security for the customer owned CICS regions.
  Level Two – The Department supports the CICS software, and maintains CICS System Definition File (CSD)/table definitions for the customer. The customer supplies the definitions to the Department and controls the application support. The Department and the customer owning agency share security responsibilities.
  Level Three – The Department supports the CICS software, maintains CSD/table definitions, and supports both CICS and the application software for the agency. The Department is also responsible for security for these regions.

- Production regions are segregated from test and development regions to restrict access, based upon the various needs for each type of region.
    - Restricted access to sensitive CICS transactions is established over production regions.
    - Test regions have fewer access restrictions. Test regions allow programmers to test and debug against non-production files.

System Software-DataBase 2 (DB2)

The Department has the following controls in place to ensure DB2 has been configured and controlled to promote security and integrity.

- Security software and system options are implemented to protect resources and data.
- Assigned Department staff is responsible for software installation, maintenance, performance monitoring, and security.
- One user ID at each agency is authorized by the Department to coordinate the use of DB2 within the agency.
- Users are required to have a security software ID and password and authenticate successfully. After authentication, DB2 internal security verifies access rights to specific data.
- Production systems are segregated from test and development systems to restrict access, based upon the various needs for each type of system.

System Software-Information Management System (IMS)

The Department has the following controls in place to ensure IMS has been configured and controlled to promote security and integrity.

- Security software and system options are implemented to protect resources and data.
- Assigned Department staff is responsible for software installation, maintenance, performance monitoring, and security.
- Production regions are segregated from test and development regions to restrict access, based upon the various needs for each type of region.

Security Software – Resource Access Control Facility (RACF)

The Department has the following controls in place to ensure RACF has been configured and controlled to promote security and integrity.

- RACF is the primary tool for controlling and monitoring access, and options are implemented to protect resources and data.
- Assigned Department staff is responsible for the implementation and administration of RACF.
- Users are required to have a valid ID and password.

- Invalid access attempts are logged and reviewed on a routine basis.
- A RACF administrator at each agency is authorized by the Department to administer RACF use within the agency.
    - User agencies are responsible for protecting their program and data files
    - RACF administrators have the capability of producing the violation reports for their agency.
    - The Department requests verification of agency RACF coordinators on a semi-annual basis.

Network Services

Network Services consists of two teams; Network Operations and Enterprise Network Support. Network Services, with the assistance of the Field Operations and LAN Services divisions as necessary, provide telecommunications/network services to a variety of agencies, boards and commissions, educational institutions, and other governmental and non-profit entities.

The Department has the following controls in place to ensure that an appropriate security structure, and related policies and procedures are established to assure that the telecommunications/network environments are effectively controlled.

- To document its network architecture, network diagrams are maintained.
- ICN Remedy and EMS 11 are utilized to inventory data circuits currently being utilized.
- To ensure the networks are appropriately configured, the Department:
    - Has established standards.
    - Created configuration templates for core and distribution routers.
    - Utilizes Cisco Advanced Services quarterly reports.
- Authentication servers are utilized to control access and ensure only properly authenticated individuals are granted access to devices for configuration management and maintenance.
- The CMS Change Management process is utilized to ensure changes to the network infrastructure are accurately tracked and appropriately authorized.
- Firewall, router, and switch configurations are backed up via two servers.
    - The servers are backed up to tape weekly.
    - Backups are rotated off-site.
- SolarWinds Orion is utilized to monitor the network.

Network Services- IWIN

The Department and the Illinois State Police have joined efforts in providing the Illinois Wireless Information Network (IWIN).

The Department has the following controls in place to ensure an appropriate wireless information network security structure is established in order for information assets and resources to be adequately protected from unauthorized or accidental disclosure, modification, or destruction.

- The "Illinois Statewide Policy Manual," located on the CMS BCCS Catalog website at: http://bccs.illinois.gov/pdf/iwin/iwinpolicymanual.pdf outlines the responsibilities for the Department, ISP, local agency IWIN coordinator and the IWIN user, as well as appropriate usage, necessary certifications to obtain IWIN access and Motorola client functions.
- The IWIN network infrastructure utilizes redundant routers which connect servers to the provider network.
- The IWIN infrastructure is comprised of a multi-layer security approach. This approach secures access to the infrastructure from the IWIN user community by utilizing strong authentication such as user IDs, passwords, and unit IDs.
- TACACS Servers authenticate authorized individuals for device configuration and maintenance.

Network Services-Field Operations

Field Operations is responsible for provisioning of hardware and circuits for connections to the ICN as well as providing technical help desk support.

The Department has the following controls in place to ensure that customer queries, questions, and problems are investigated and resolved timely.

- The Remedy ticketing system and its internal functionality provides the tools and means by which customer incidents and service requests are logged, tracked, and updated with supporting documentation through resolution.
- Remedy ticket procedures require all tickets to be properly documented and worklog entries to be entered as work progress or resolution steps are performed.
- Various documents assist the process and means by which Field Operations handles the repair calls from customers via the Remedy Help Desk Case module.
- Weekly conference calls and review of trouble tickets helps identify trends and recurring problems.
- Domain Name Service – Non-Agency Process located on Field Ops master document library Sharepoint site.
- Master configuration templates exist for Agency and Non-Agency routers. Configurations of access routers are backed up and stored on servers located at the RTC offices and in Springfield.

Network Services-LAN Services

LAN Services is responsible for the installation, configuration, and support of the Department's LAN networking infrastructure, including: switches, routers, hubs, firewalls, wireless switches and inside cabling.

The Department has the following controls in place to ensure that information assets and resources are adequately protected from unauthorized or accidental disclosure, modification, or destruction.

- The Department's LAN Standards document outlines the standard/template setting for the LAN network.
- The Department maintained individual network topology maps for each network segment.
- The Department utilizes Solarwinds Orion to monitor the network and ensure configurations are appropriately backed up.
    - Reports of incidents are generated daily and distributed for appropriate review.
- TACACS is utilized to ensure only authorized individuals have appropriate access.
- The Change Management process is utilized for tracking and authorizing changes.

LAN Application Development

The LAN Application Development section is responsible for the development of custom and packaged Local Area Network (LAN) Based application software.

The Department has the following controls in place to ensure that a suitable structured systems development methodology exists and is utilized to ensure that applications are developed and/or modified in a manner that promotes consistency, integrity, and security and to ensure that applications satisfy management's intentions.

- This process is governed by IT Governance; therefore we follow the pertinent IT Governance process and associated policy.
- For changes made to LAN Applications, we follow the applicable sections of the EAA Systems Development Methodology, which includes the Rapid Application Development (RAD) Development Standards.
- Changes or enhancements to existing LAN Applications are tracked and authorized via Service Requests submitted through the Service Request Registration System (SRRS) or via an Enterprise Service Request (ESR) submitted through Remedy Change Management.
- The development security is controlled by Access Security Groups which, along with Drive Mapping, ensures that the individual developing the application does not move the change into the production environment.
- Management oversight, including authorization to move new or modified LAN Applications into production are controlled via the Service Request Registration System (SRRS) and Remedy Change Management

Interactive Systems (Web Services)

The Department provides a variety of internal and external web sites/applications in order for agencies to communicate their information to both the public and private sectors.

The Department has the following controls in place to ensure that a suitable structured systems development methodology exists and is utilized to ensure that web sites/applications are developed and/or modified in a manner that promotes consistency, integrity, and security and to ensure that applications satisfy management's intentions.

Content Management

- New web site developments utilize the Web Services Content Change Procedures in conjunction with the New Web Site Checklist.
- Web Services Application (Access) is used to authorize web content changes.
- Changes or enhancements are tested in accordance with Web Services Content Change Procedures and a business owner or Illinois Office of Information and Communication review ensure content changes are correct.
- Developers test for web accessibility in accordance with IITAA requirements using evaluation tools provided by DHS.
- Access to the production environment is controlled by:
    - Security access rights manage who can move the change.
    - Web Services Content Change Procedures in conjunction with Web Services application defines the process and records the name of the person that moved the change to production.
- Domain Name Service (DNS) Request Form with signatures for Requester and Server Admin ensure requests are properly authorized, documented and tracked.

Internet Applications

- This process is governed by IT Governance; therefore we follow the pertinent IT Governance process and associated policy.
- For changes made to Web Sites/Applications, we follow the applicable sections of the EAA Systems Development Methodology, which includes the Rapid Application Development (RAD) Development Standards.
- Changes or enhancements to existing Web Applications are tracked and authorized via Service Requests submitted through the Service Request Registration System (SRRS) or via an Enterprise Service Request (ESR) submitted through Remedy Change Management.
- Developers test for web accessibility in accordance with IITAA requirements using evaluation tools provided by DHS.
- Access to the production environment is controlled by:
    - Security access rights manage who can move the change.
    - An Enterprise Service Request (ESR) is submitted to move changes to Production.
- Domain Name Service (DNS) Request Form with signatures for Requester and Server Admin ensure requests are properly authorized, documented and tracked.

Accounting Information System (AIS)

AIS functions as an automated expenditure control and invoice/voucher processing system. AIS, in processing invoices, allocates invoice amounts into sub accounts; groups invoices, according to the Comptroller's Statewide Accounting Management System (SAMS) procedures, for the preparation of vouchers; and allows users to track cost centers. AIS interfaces with the Illinois Governmental Purchasing System (IGPS), the Accounts Receivable Posting System (ARPS), the Central Inventory System (CIS) and the Central Payroll System (CPS).

The Department has the following controls in place to ensure AIS promotes accuracy, security and integrity.

- AIS is secured using security software, in addition to internal security requirements.
  - Users must have an authorized ID and password to gain access.
  - Assignment and authorization of access rights is the responsibility of the user agency.
  - Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.
- Changes to AIS are controlled through the Enterprise Business Applications Methodology.
  - Changes are initiated through the use of a Service Request Form.
  - Changes are approved and tested before implementation into the production environment.
  - Changes are moved into production by the Library Control Group.
- Quality assurance procedures apply to significant developments and enhancements.
- The AIS User Manual, located on the State's Enterprise Web Server (Intranet), provides guidance on the use of the Accounting Information System.
- AIS transactions are entered online in a real-time environment, with the ability to batch transactions for processing at a later date. AIS was developed with edits that force correction of errors and completion of critical fields before a transaction is accepted. All data entry is performed by user agencies and is the responsibility of user agencies.
- AIS provides various online and batch reports to assist in the balance of transactions. A complete listing of the various reports is maintained in the AIS Users Manual. Retention of the various reports is the responsibility of the user agency.
- AIS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.
- A disaster recovery plan for AIS provides guidelines for restoration.

Central Payroll System (CPS)

CPS was designed to provide assistance in preparing payrolls for state agencies. The system will accommodate agencies which are governed by the Rules of the Personnel Code and agencies that are exempt from the Personnel Code (Non-Code Agencies). The payroll system is a tool to be used by qualified personnel with SAMS and payroll procedure knowledge. CPS enables state agencies to maintain automated pay records and provide a file that is submitted to the Comptroller's Office for the production of payroll warrants. CPS has an interface with Central Time and Attendance System (CTAS) and Accounting Information System (AIS).

The Department has the following controls in place to ensure CPS promotes accuracy, security and integrity.

- CPS is secured using security software, in addition to internal security requirements.
  - Users must have an authorized ID and password to gain access.
  - Assignment and authorization of access rights is the responsibility of the user agency.

    - Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.
- Changes to CPS are controlled through the Enterprise Business Applications Methodology.
    - Changes are initiated through the use of a Service Request Form.
    - Changes are approved and tested before implementation into the production environment.
    - Changes are moved into production by the Library Control Group.
- Quality assurance procedures apply to significant developments and enhancements.
- The CPS User Manual provides guidance on the use of the Central Payroll System.
- CPS has an edit feature designed to reject invalid information entered into the system. When invalid data has been entered into the system, an error message will appear at the top of the screen and the field that is in error will be highlighted. The system will not accept the entry until the error has been corrected or deleted. The Department has procedures in place to handle errors that occur during processing.
- The payroll vouchers/reports that are produced from the batch process are printed by the Department's Production Operations Services and delivered to Central Payroll.
    - Central Payroll separates the vouchers/reports for each agency to pickup or to be delivered by Mail Messenger, UPS, or Fed Ex.
    - Each agency must submit a list of individuals that are approved to pick up payroll related materials. This list is reviewed periodically by the user agencies.
    - The retention of these payroll vouchers/reports is the responsibility of the user agency.
- CPS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.
- Disaster Recovery guidance is included in the CPS User Manual.

Central Inventory System (CIS)

CIS is an automated inventory control system. CIS has the ability to utilize an optical scanner to read bar code labels during a physical inventory by using additional external software. CIS allows user agencies to maintain records of inventory and to comply with the Department's Property Control Division's rules of reporting and processing. CIS meets all the GASB-34 rules; it allows the user agencies the ability to accurately track depreciation on items that they specify.

The Department has the following controls in place to ensure CIS promotes accuracy, security and integrity.

- CIS is secured using security software, in addition to internal security requirements.
    - Users must have an authorized ID and password to gain access.
    - Assignment and authorization of access rights is the responsibility of the user agency.
    - Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

- Changes to CIS are controlled through the Enterprise Business Applications Methodology.
    - Changes are initiated through the use of a Service Request Form.
    - Changes are approved and tested before implementation into the production environment.
    - Changes are moved into production by the Library Control Group.
- Quality assurance procedures apply to significant developments and enhancements.
- The CIS User Manual provides guidance to the use of the Central Inventory System.
- Data is entered online by user agencies. CIS has several edit checks to alert users of errors. Errors must be corrected before the transaction is accepted.
- A Location Balance Report is run nightly to determine whether the previous day's transactions processed correctly. Additional reports are available to users. The accuracy and reconciliation of data is the responsibility of the user agency.
- CIS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Central Time and Attendance System (CTAS)

CTAS is an online system used to maintain "available benefit time". Additionally, CTAS allows user agencies to monitor whether usage of time is in accordance with state rules. CTAS provides for attendance information to be recorded using either the positive or exception methods. CTAS interfaces with the Central Payroll System.

The Department has the following controls in place to ensure CTAS promotes accuracy, security and integrity.

- CTAS is secured using security software, in addition to internal security requirements.
    - Users must have an authorized ID and password to gain access.
    - Assignment and authorization of access rights is the responsibility of the user agency.
    - Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.
- Changes to CTAS are controlled through the Enterprise Business Applications Methodology.
    - Changes are initiated through the use of a Service Request Form.
    - Changes are approved and tested before implementation into the production environment.
    - Changes are moved into production by the Library Control Group.
- Quality assurance procedures apply to significant developments and enhancements.
- The CTAS User Manual provides guidance to the use of the Central Time and Attendance Inventory System.
- Data is entered online by user agencies. CTAS has edit checks to alert users of errors. Transactions with errors will be rejected.

- CTAS provides online and batch reports that user agencies may use for reconciliation purposes. During the “close” process, CTAS generates error reports, reconciliationreports, and file maintenance activity reports. All transactions must be reconciled before the “close” process can be finalized. The accuracy and reconciliation of data is the responsibility of the user agency.
- CTAS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.
- CTAS Recovery procedures provide guidelines for restoration.

This Page Intentionally Left Blank

SERVICE AUDITOR
DESCRIPTION OF TESTS AND OPERATING EFFECTIVENESS

We reviewed or confirmed data processing general and application controls at the Department. Using the Department's Description of Controls as the foundation for our review, we performed tests to determine compliance with policies and procedures, conducted interviews, performed observations, and identified specific control objectives and procedures we considered necessary in the circumstances to evaluate the controls.

GENERAL CONTROLS
Control Objectives

General controls are those which apply to the entire computer operation. General controls are the methods, policies, and procedures adopted by an organization to ensure the overall environment surrounding the information systems is protected. General controls help ensure the protection of assets, promotion of administrative efficiency, and adherence to management's standards and intentions. Specific control objectives are imbedded in the Department's Description of Control.

The general controls review consisted of an evaluation of the controls in the following areas:

- Personnel
- Strategic Planning
- IT Governance
- Billing
- Vendor Management
- Service Reporting and Service Delivery and Implementation
- Internal Audit
- Agency Relations
- Continuous Services
- Customer Service
- Quality Assurance
- Change Control
- Security Administration
- Physical Security
- Operations
- System Software
- Network Services
- LAN Application Development
- Interactive Systems

The results of our review are included in the General Controls (pages 37 through 161) and Application Controls (pages 163 through 185) sections of this report.

PERSONNEL

EXISTING ENVIRONMENT

Department's Description of Control: A detailed organizational chart is maintained.

Tests Performed: Reviewed organizational chart.

Test Results: The Department of Central Management Services' (Department) Bureau of Communication and Computer Services (Bureau) was statutorily mandated to provide "use of electronic data processing equipment, including necessary telecommunications lines and equipment, available to local governments, elected State officials, State educational institutions, and all other governmental units of the State requesting them." (20ILCS 405/405-250)

The organizational chart listed 769 positions for the Bureau; however, there were 113 vacancies. Additionally, of the 113 vacancies, 28 were considered critical.

Throughout the audit process, the Department made reference to current and potential staffing and expertise concerns related the Department's ability to provide services. The staffing issue was included in the Strategic Planning, z/OS, DB2, and Security Administration controls.

A detailed organizational chart was maintained; however, it included numerous vacancies, including those identified as critical.

Department's Description of Control: Shared Services provides BCCS monthly reports citing the employees name and the due date of the evaluation. Monthly, BCCS personnel sends these reports to managers. Performance evaluation dates are tracked in BCCS Personnel database.

Tests Performed: Reviewed performance evaluation report and interviewed staff.

Test Results: Shared Services provided Bureau Personnel with monthly status reports outlining evaluation due dates. Personnel entered the information into the Bureau's Personnel database to track performance evaluations.

Although a tracking system existed, Bureau staff evaluations were not always completed in a timely manner.

Department's Description of Control: Personnel hires are subject to the educational requirements, experience, and the specialized skills defined in position descriptions.

Tests Performed: Reviewed job descriptions and interviewed staff.

Test Results: The position descriptions were created with educational requirements, experience, and specialized skills based on the position.

We reviewed two position descriptions, noting the educational requirements, experience, and skills were defined.

No significant exception noted.

Department's Description of Control: Upon termination of an employee, communication occurs between the Division Manager/manager/supervisor and Workforce Development and Logistics Manager to assess filling the vacancy.

Tests Performed: Reviewed vacancy levels, exit forms, and interviewed staff.

Test Results: Personnel developed a procedure to notify individuals to remove logical and physical access rights to data and facilities for employees that departed. The procedure included an exit checklist that was sent to the facilities' OA Coordinators to ensure all information was completed upon employee separation.

We reviewed the exit forms of all 22 individuals who separated during the audit period and found the majority of the forms were not properly completed or submitted timely.

In addition, management stated that contractors were not required to have an exit form completed.

The Department did not ensure exit forms were completed properly or timely.

Department's Description of Control: CMS Policy Manual is given to all new full time employees. Updates to the Personnel manual or policies are e-mailed to BCCS staff. Employees are required to sign an acknowledgement form.

Tests Performed: Reviewed acknowledgement forms and interviewed staff.

Test Results: Shared Services provided new employees the CMS Policy Manual. Additionally, when updates to the CMS Policy Manual occurred, acknowledgment forms were to be completed. Shared Services maintained the acknowledgment forms.

In December 2009, the CMS Policy Manual was updated. We selected 25 employees to ensure they had signed an Employee Acknowledgement of Policies form for the December 2009 update, noting no exceptions.

No significant exception noted.

Department’s Description of Control: Boilerplate language is included in vendor contracts regarding:

Compliance with the Law
Background check
Confidentiality.

Tests Performed: Reviewed contracts and interviewed staff.

Test Results: Vendor Management ensured the standard terms and conditions were included in the State of Illinois boilerplate, and were part of Department contracts.

We reviewed five contracts for boilerplate language regarding compliance with law, background check, and confidentiality, noting no exceptions.

No significant exception noted.

Department’s Description of Control: Training objectives are defined by supervisor and employee during the evaluation process.

Tests Performed: Reviewed evaluations and interviewed staff.

Test Results: According to management, training objectives were to be defined during the evaluation process. However, due to budget constraints, actual training had been limited.

We reviewed five evaluations, noting no exceptions.

No significant exception noted.

Department’s Description of Control: BCCS Workforce and Logistics Office maintain a spreadsheet of staff and their training requested and received.

Tests Performed: Reviewed training spreadsheet.

Test Results: BCCS Workforce and Logistics Office maintained a training spreadsheet, which documented training requested and received.

We reviewed the spreadsheet, noting the information maintained included: name of staff, date of training, title of training, location (in or out of state), length, and cost.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. However, to enhance its objectives, we recommend the Department:

- Perform a detailed review of the use of overtime, loss of key personnel, vacancies, and potential vacancies, with an emphasis on critical vacancies to ensure staffing is sufficient to meet goals, objectives, and operational needs.
- Ensure evaluations are performed in a timely manner.
- Ensure the exit checklists are appropriately completed to make certain and verify that access rights are removed and badges are returned upon employee separation.
- Require exit checklists be completed for contractors.

STRATEGIC PLANNING

EXISTING ENVIRONMENT

Department's Description of Control: Strategic Planning Document.

Tests Performed: Reviewed Strategic Planning Document.

Test Results: A Strategic Plan had not been developed since fiscal year 2008. In fiscal year 2008, the Bureau's Leadership Team assisted the Deputy Director in the development of the "FY08 Information Technology and Network Strategic Plan", dated January 22, 2008.

No significant exception noted; however, a current Strategic Plan had not been developed.

Department's Description of Control: Information Gathering - BCCS managers and technical subject matter experts meet and request information on a regular basis from our existing vendors, other technology providers, and industry experts (Gartner, etc.) to monitor technology trends, existing services and to ensure that our services are competitive.

Tests Performed: Interviewed staff.

Test Results: Individual managers gathered information and presented it to leadership when deemed necessary. The information gathered would vary based on the technology and staff expertise.

No significant exception noted.

Department's Description of Control: Priority Meetings - The BCCS Executive Team and other key leaders in the BCCS organization hold Leadership Priority Meetings on a regular basis to track the progression of all priority projects and procurements.

Tests Performed: Reviewed Priority Meetings agendas and interviewed staff.

Test Results: The Executive Team and other leaders held regular meetings to track the progress of projects and procurements.

We reviewed the Priority Meeting agendas, noting the meetings were held to review the strategies and objectives of new projects, projects completed, projects cancelled or closed, etc.

No significant exception noted.

Department's Description of Control: Architectural Review Board Meeting – BCCS conduct ARB meetings with consolidated agencies, Illinois State Police, Department of Children and Family Services and the Department of Corrections to provide updates on technology initiatives, discuss technology needs and issues as well as share strategic plans.

Tests Performed: Reviewed Architectural Review Board (ARB) agendas.

Test Results: Architectural Review Board conducted meetings which provided updates on various projects and plans.

We reviewed the ARB meeting agendas, noting the meetings addressed infrastructure updates, verification and validation request for proposal, initiatives, and various other topics. It appeared the meetings provided updates on technology initiatives, discussed technology needs and issues as well as shared strategic plans.

No significant exception noted.

Department's Description of Control: Competitive Procurement - BCCS utilizes the competitive procurement process to ensure that the technology equipment, services and support are competitive and meet the needs of customers

Tests Performed: Interviewed staff.

Test Results: The Department utilized procurement process controls in the Remedy System to ensure procurement processes were followed.

No significant exception noted.

Department's Description of Control: IT Governance - BCCS utilizes the IT Governance Process to ensure that proposed IT projects align with strategic plans.

Tests Performed: Reviewed projects, strategic plan, and interviewed staff.

Test Results: The Department utilized the IT Governance process to ensure projects were aligned with strategic plans.

We selected one project, Midrange Recovery, to ensure the project aligned with the strategic plan, noting no exceptions.

No significant exception noted.

Department's Description of Control: Executive Planning Sessions – As needed, members of the BCCS Leadership team meet to exchange and share information. The team then uses this information along with other pertinent information to establish and make necessary alternation to Bureau strategies.

Tests Performed: Interviewed staff.

Test Results: The Leadership team met on an as needed basis to exchange and share information and make alterations to Bureau strategies.

No significant exception noted.

Department's Description of Control: Telecommunication Coordinator Meetings – Each agency must establish at least one agency telecommunication coordinator to order BCCS telecommunication related services. BCCS conducts Telecommunication Coordinator Meetings to share information and to give agencies the opportunity to provide input on needed services.

Tests Performed: Interviewed staff.

Test Results: The Department conducted Telecommunication Coordinator Meetings to share information and to give agencies the opportunity to provide input on needed services.

The Department maintained a listing of agency telecommunication coordinators who were responsible for ordering telecommunication related services.

No significant exception noted.

Department's Description of Control: CIO Forum – BCCS conducts periodic meetings with State Agency CIOs and Senior IT managers to share information on broad issues that may affect the use of technology in Illinois Government. The participants can present topics and provide input on what is presented.

Tests Performed: Reviewed CIO Forum agendas.

Test Results: The Department had held two meetings; August and November 2009, with CIOs and Senior IT managers.

The meetings appeared to share information on broad issues that may affect the use of technology in Illinois Government.

No significant exception noted.

Department's Description of Control: A set of guiding principles were established to assist in aligning projects and activities with the BCCS mission and objectives. BCCS leadership continues to work with the CIO of the State, and other IT Leaders to identify opportunities to improve the overall delivery of IT services based upon the guiding principles.

Tests Performed: Reviewed the IT Guiding Principles and interviewed staff.

Test Results: The IT Guiding Principles, dated August 2008, were defined as policy statements which identified the role of IT and how it supported business needs. The IT Guiding Principles were utilized in the decision making processes to reduce time and expense and to promote consistency in the IT decision-making processes.

No significant exception noted.

Department's Description of Control: BCCS Leadership Team is responsible for reviewing and addressing changes in management that would affect achieving the Bureau's mission and objectives. Inadequate staffing and competency levels can have a direct impact on the bureau's ability to meet the mission.

Tests Performed: Reviewed BCCS Leadership Team meeting agendas.

Test Results: We reviewed the BCCS Leadership Team meeting agendas for the period of July 2009 through January 2010, nothing they had met several times each month.

These meetings addressed staffing vacancies, contracts, salaries, hiring contractors, along with various other topics. The meetings addressed changes in management that would have an affect achieving the Bureau's mission and objectives, including staffing levels.

The BCCS Leadership team had identified staffing deficiencies, including critical position vacancies, and formally communicated these concerns to the Department's Director and the Governor's Office. For additional information on staffing levels, see the Personnel control.

No significant exception noted.

Department's Description of Control: BCCS staffs actively participate in a variety of meetings and committees such as the Human Services Framework, Illinois Terrorism Task Force Committees, etc. Through BCCS participation we can work to ensure changes in technology / management are considered in meeting the goals and objectives.

Tests Performed: Interviewed staff.

Test Results: The Department actively participated in a variety of meetings to ensure changes in technology were considered to help user agencies meet goals and objectives.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. Although strategic planning activities were being conducted, the Department should enhance its process to ensure Strategic Plans are current, updated at least annually, and address at least three years.

IT GOVERNANCE

EXISTING ENVIRONMENT

Department Description of Control: The IT Governance Policy defines the scope, roles and responsibilities of the process.

Tests Performed: Reviewed the IT Governance Policy.

Test Results: The Department developed an IT Governance Policy (Policy), dated December 15, 2008. The purpose of the Policy was to "define the ITG scope, roles and responsibilities." The Policy stated each agency should establish procedures and assign responsibilities to specific agency personnel to achieve policy compliance.

IT Governance was defined as the process of qualifying agency submitted initiatives as projects by ensuring alignment with the enterprise architecture and registering compliance requirements.

IT Governance applied to business-sponsored projects that met the following criteria:

- New business functionality was being added,
- A move to a new or updated platform was being made,
- An old system was being replaced,
- A system was being in-sourced or outsourced either partially or completely, or
- The work had enterprise implications.

IT Governance would determine if all information technology initiatives were compliant with the State's enterprise architecture. Agencies were required to submit procurement specifications that involved third parties before an IT Governance Charter would be approved.

Agencies were able to apply to the State Chief Information Officer for a waiver when a chartered initiative had been denied.

No significant exception noted.

Department Description of Control: BCCS Leadership discusses strategies and objectives in the regularly held BCCS Priorities Meetings.

Tests Performed: Reviewed meeting agendas and interviewed staff.

Test Results: The Priority Meetings primary purpose was to review new projects, projects completed, projects cancelled or closed. These meetings tracked the progression of all priority projects and procurements.

No significant exception noted.

Department Description of Control: IT Governance reviews Governance documents and procurements and communicates / works with stakeholders as necessary relative to strategies and objectives.

Tests Performed: Reviewed project documentation and interviewed staff.

Test Results: The IT Governance staff reviewed the project charter and the business and technical requirements. IT Governance would also determine if there were existing resources available for the project within the enterprise wide environment.

For procurements, IT Governance would review and approve the architecture and alignment documentation and business technical information. IT Governance would determine if the project was aligned with current infrastructure availability and the Technical Reference Model.

We reviewed a project for the project charter, business requirements, technical requirements, and the deployment package, noting no exceptions.

No significant exception noted.

Department Description of Control: IT Governance stays in communication with the State CIO relative to strategies and objectives.

Tests Performed: Interviewed staff.

Test Results: IT Governance staff would contact the State's Chief Information Officer by email or phone to discuss strategies and objective.

No significant exception noted.

Department Description of Control: The Governance website, www.illinois.gov/governance, provides up-to-date governance information for stakeholders.

Tests Performed: Reviewed website.

Test Results: The IT Governance website provided governance information. The website had the following documents available:

- State of Illinois Guiding Principles,
- What was Governance,
- When was Governance Needed,
- What is the Governance Process, and
- Template downloads.

Additionally, the website had contact information, announcements, news and frequently asked questions.

No significant exception noted.

Department Description of Control: IT Governance meets with stakeholders in person and via conference calls.

Tests Performed: Interviewed staff.

Test Results: IT Governance staff would hold conference calls to aide in the review of projects or to assist with problems. Additionally, agencies would contact or meet with IT Governance staff throughout a project.

No significant exception noted.

Department Description of Control: The EPM Portal provides access to agency staff designated by state agencies to view and maintain information relative to their chartered projects.

Tests Performed: Interviewed staff.

Test Results: Six agencies had requested, and been granted, access to the Enterprise Program Management (EPM) Portal; Department of Transportation, Department of Healthcare and Family Services, Department of Human Services, Department of Revenue, Department of Central Management Services and Department of Financial and Professional Regulations.

Agencies that had not requested access were provided with updates on chartered projects by IT Governance staff.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

BILLING
SSRF and CRF

EXISTING ENVIRONMENT

Background Provided by the Department: The Department is statutorily authorized to provide IT and telecommunication services to State agencies, boards, and commissions. The agencies are billed for services provided and remit payment to the Statistical Services Revolving Fund (SSRF) and the Communications Revolving Fund (CRF).

Statistical Services Revolving Fund

Department Description of Control: The Komand system is utilized to compile the SSRF billings. The system provides a means for charging resource utilization back to users.

Tests Performed: Reviewed Komand procedures and interviewed staff.

Test Results: The KOMAND system provided a means to bill user agencies for utilization of the various environments and applications.

From July 2009 through April 2010, the Department billed user agencies approximately $101,469,791.

No significant exception noted.

Department Description of Control: The Komand procedures assist users of the system.

Tests Performed: Reviewed Komand procedures.

Test Results: The Department maintained the Komand System Manuals, Version 6, to assist users with the compilation of user agency invoices and reports.

No significant exception noted.

Department Description of Control: The SSRF Billing procedures assist staff with monthly billings. Reports are produced and verified against each other to ensure the accuracy of the billings. An Edit Check is completed to ensure the completeness and accuracy of each billing.

Tests Performed: Reviewed the 2010 SSRF ISD/IMS Monthly Billing procedures.

Test Results: The Department developed the 2010 SSRF ISD/IMS Monthly Billing procedures (updated monthly to include data from current bills), which provided guidance on the completion and reconciliation of the monthly billings.

The Department utilized several reports to assist with the accuracy of the billing information. The "Edit Check" process was routinely completed to promote billing completeness and accuracy.

We reviewed the billing process and system data for the months of November and December 2009 and were able to trace the Edit Check to the detailed reports. However, we found the source data for some services for consolidated agencies lacked accuracy. In these cases, information pertaining to PCs/laptops, servers, and software licenses for consolidated agencies had not been verified to ensure validity.

The Department had established a process to review billing accuracy; however, a process to ensure billings accurately reflected some services rendered to consolidated agencies had not been established.

Communication Revolving Fund

Department Description of Control: The EMS11and AIS systems are utilized to compile the CRF billings.

Tests Performed: Reviewed CRF Billing Overview and interviewed staff.

Test Results: According to the CRF Billing Overview, approximately 90% of the CRF billings were generated through the EMS system; the remaining 10% were generated through AIS. The EMS billing system and AIS allowed for re-rated charges as well as pass-thru charges.

From July 2009 through April 2010, the Department billed user agencies approximately $75,122,657.

No significant exception noted.

Department Description of Control: The CRF Billing procedures assist staff with the monthly billings.

Tests Performed: Reviewed CRF Billing Overview and Process.

Test Results: The Department developed the CRF Billing Overview and Process, not dated to guide staff with the monthly billing process.

Each month several vendors provide information utilized to produce agency telecommunication billings. The CRF Billing Overview and Process provided detailed instructions for the loading of vendor data and the reconciliation of the data and billings.

No significant exception noted.

Department Description of Control: At the end of each billing, verification is performed to ensure the accuracy of the billings. Reports from each source are verified against each other to ensure the accuracy of information.

Tests Performed: Reviewed CRF Billing Overview and Process, reconciliations and interviewed staff.

Test Results: Several reports were generated and reconciled each month to ensure the completeness and accuracy of the billings.

We reviewed the various reports and reconciliations for the CRF billings for November and December 2009, noting no exceptions.

No significant exception noted.

Outstanding Accounts/Billing Credits

Department Description of Control: The Fiscal Operation Policy outlines the process for the collection of outstanding accounts.

Tests Performed: Reviewed Fiscal Operation Policy.

Test Results: The Department's Fiscal Operations Policy required the "collection of unpaid agency receivables, referral of unpaid receivables to alternative collection efforts and write-off of accounts receivable as uncollectible."

No significant exception noted.

Department Description of Control: Delinquency letters are sent out when the criteria is met for the number of days invoice is past due. An account aging analysis is sent out on a quarterly basis.

Tests Performed: Reviewed delinquency notices and interviewed staff.

Test Results: The Department sent out delinquency notices at various times during the billing period. We reviewed the delinquency notices for the week of February 1, 2010, noting the notices included a listing of all delinquent invoices and amounts.

According Business Service staff, no accounts had been turned over to the Comptroller's off-set system.

As of April 30, 2010, the Department had outstanding accounts receivable of $30,883,075 and $23,015,884 for the SSRF and CRF, respectively.

No significant exception noted.

Department Description of Control: Requests for billing credits must be submitted in writing. All requests must be approved in writing.

Tests Performed: Reviewed credit requests and interviewed staff.

Test Results: In the event the Department and agency determined an inappropriate charge had been assessed, the agency could request a credit. We reviewed documentation associated with 20 issued credits, noting no exceptions.

No significant exception noted.

Department Description of Control: Approved billing credits are sent to Shared Services for processing. Shared Services processes the ARCM request form and posts the credit to the appropriate account in ARPS.

Tests Performed: Interviewed staff.

Test Results: Upon approval by Business Services, billing credits were sent to the Shared Services Center for processing.

No significant exception noted.

Billing Rates

Department Description of Control: All expenditures are coded to cost centers and assigned to services through a cost accounting model. Revenues for each service are compared to costs to determine the appropriateness of individual rates.

Tests Performed: Reviewed methodology, rate analysis, and interviewed staff.

Test Results: The Department assigned cost center codes to expenditures and revenues in order to determine the appropriateness of rates.

Annually, the Department conducted analysis of the cost centers in order to forecast the rates for the upcoming fiscal year. Additionally, mid-year the Department conducted a review of the rates to determine if adjustments were required.

The Department prepared a forecast for the fiscal year and conducted a mid-year review of the rates.

No significant exception noted.

Department Description of Control: In order to comply with the federal requirements (A-87), an analysis is performed annually to determine profit/loss for each service. Excess revenues are subject to reimbursement to the federal government.

Tests Performed: Interviewed staff.

Test Results: Annually, the Department submitted the State of Illinois Statewide Cost Allocation Plan to the Federal Department of Human Services. The Allocation Plan outlined the Department's analysis of costs and revenues by service center.

At the time of our review, the Department was in the process of completing the FY09 Plan for submission.

During the fiscal year the Department paid the federal Department of Health and Human Services $4,005,106 from the CRF and $10,635,652 from the SSRF to settle paybacks for FY06-FY08 Plan audits.

No significant exception noted; however, paybacks to the federal government were significant.

OVERALL CONCLUSION

The Department had a process to develop and review billings to user agencies. However, the source data for some services for consolidated agencies had not been verified to ensure validity. To ensure the accuracy of the billings, the Department should develop a process to ensure billings accurately reflect services rendered. In addition, the Department should develop an appropriate methodology to reduce paybacks to the federal government.

VENDOR MANAGEMENT

EXISTING ENVIRONMENT

Department Description of Control: The Department has a contract tool in the EPM system to alert staff when software contracts expire.

Tests Performed: Reviewed EPM Portal, emails, and interviewed staff.

Test Results: The EPM Portal system contained contract information; contract number, contract value, start and end dates, business owner, vendor information and contract status.

Depending on the type of contract, sole source or small procurement, an email notification was sent out to the applicable individuals indicating contract expiration.

We reviewed three emails noting the emails contained the contract expiration date, determination of need, and the person to contact for renewal.

No significant exception noted.

Department Description of Control: The Department has procedural steps thru the Enterprise Service Request (ESR) process to ensure license compliance for all new software moves, adds or additions.

Tests Performed: Reviewed the Remedy Software Asset Tasks (Vendor Management-Quick Reference), prior audit reports, and interviewed staff.

Test Results: The Department developed the Remedy Software Asset Tasks (Vendor Management-Quick Reference), dated September 10, 2009. The Quick Reference documented the process utilized for license inventory tracking through the Remedy Enterprise Service Request (ESR) process.

Per discussion with Vendor Management, the Remedy ESR process to track license inventory had not been placed into production.

Additionally, even though software inventory problems were identified in prior year reviews and audits, the Department had not conducted a reconciliation of software, identifying the actual number of licenses in use versus the number of licenses purchased from each vendor.

Although procedural steps existed for license inventory tracking, the procedural steps had not been fully implemented and a reconciliation of software had not been conducted.

Department Description of Control: The Department follows the Department's Fiscal Operating Policies and Procurement Guidelines established by BOSSAP.

Tests Performed: Reviewed Fiscal Operating Policies and Procurement Guidelines and interviewed staff.

Test Results: The Department had developed the Fiscal Operating Policies and Procurement Guidelines. However, per discussion with Vendor Management staff, they did not utilize any specific section of the Guidelines. Instead of using the Guidelines, Vendor Management staff would create a request and forward it to the procurement mailbox.

Vendor Management did not follow the Fiscal Operating Policies and Procurement Guidelines.

OVERALL CONCLUSION

Vendor Management had not implemented procedures to ensure it met its goals and objectives. To ensure an adequate framework exists in controlling and monitoring software usage, the Department should:

- Implement a mechanism to effectively monitor software usage for compliance with contract requirements.
- Ensure Vendor Management follows the Fiscal Operating Policies and Procurement Guidelines.

SERVICE REPORTING and SERVICE DELIVERY and IMPLEMENTATION

EXISTING ENVIRONMENT

Department's Description of Control: The BCCS IT Services are defined within in the BCCS Service Catalog using a fairly consistent format which describes "What's Included", "What You Can Expect", "How You Can Help", "Need More Information", "Service Order Information" and rate information, when available, per service.

Tests Performed: Reviewed BCCS Service Catalog.

Tests Results: The BCCS Service Catalog identified five services: Network Services, Telecommunication Services, Application Services, Computing Services, and Business Services.

We reviewed the five service sites noting each service identified "What's Included", "What You Can Expect", "How You Can Help", "Need More Information", "Service Order Information" and rate information.

No significant exception noted.

Department's Description of Control: The BCCS Service Catalog is used to define the level of IT service a customer can expect for defined services.

Tests Performed: Reviewed the BCCS Service Catalog and interviewed staff.

Tests Results: The BCCS Service Catalog did not identify or define the level of IT service a user would expect for the defined services.

Additionally, management stated the Department had not defined service levels. The Department was working towards defining service levels.

No significant exception noted; however, the Department had not defined IT service levels.

Department's Description of Control: The BCCS Service Site - Agency Reporting allows our customers to monitor BCCS performance as it relates to their agency.

Tests Performed: Reviewed the BCCS Service Site and interviewed staff.

Tests Results: The BCCS Service Site provided announcements on various topics, links to other BCCS divisions, contact information for each agency CIO, and frequently asked questions.

In addition, the site included performance information for each agency.

No significant exception noted.

Department's Description of Control: As of October 2009 agencies have the ability to run BCCS Service Performance Reports on demand from the BCCS Service Site. Agency direct access to the Remedy system allows generation of reports.

Tests Performed: Reviewed BCCS Service Performance Reports and the BCCS Service Site.

Tests Results: The BCCS Service Site provided the consolidated agencies a step by step processing tool on how to run performance reports. The agencies had the ability to run these reports on demand.

The reports included information on: Enterprise Service Requests (ESR) hardware install service requests, ESR software install requests, ESR security changes service requests, ESR security deletes, ESR network changes, ESR network install, ESR application changes, ESR application installs, incident PC hardware, incident printer hardware, incident network LAN, incident security password, incident security permission, and incident software desktop.

We reviewed the above reports for the Department of Human Services, noting the reports included performance indicators and trend analysis for services.

No significant exception noted.

Department's Description of Control: The Service Reporting Team, Service Delivery and Implementation Team, CSC Quality Assurance team, and EUC Quality Assurance produce reports to identify trends, assessing and updating management on the information.

Tests Performed: Reviewed reports and interviewed staff.

Tests Results: We reviewed reports from the Service Reporting Team, Service Delivery and Implementation Team, CSC Quality Assurance and EUC Quality Assurance, noting the reports identified trends and were utilized to discuss issues with Department management.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives; however, the Department should define an acceptable level of IT services users can expect as outlined in its Description of Control.

INTERNAL AUDIT

EXISTING ENVIRONMENT

Department Description of Control: The statewide Information Technology (IT) audit function is part of the Illinois Office of Internal Audit (IOIA), which addresses those entities under the Governor's jurisdiction. IT is addressed on a statewide basis, which reduces duplication of efforts and increase efficiencies. IOIA performs various types of IT audits including system development audits, application audits, special audits, and internal audits.

Tests Performed: Reviewed listing of projects, annual report, and interviewed staff.

Test Results: Agencies were required to submit a listing of new system developments or major modifications, and the status of existing projects to IOIA each quarter.

It was the agencies' responsibility to inform IOIA of new system developments or major modifications.

The IOIA performed various types of IT audits during the audit period.

No significant exception noted.

Department Description of Control: The Fiscal Control and Internal Auditing Act (30 ILCS 10/2003 (a) (3)) mandates IOIA review the design of major new electronic data processing systems and major modifications to those systems. IOIA has established a process for identifying major new systems and major changes to existing systems for system development audits to determine which systems development projects are major and require an audit.

Tests Performed: Reviewed the annual report.

Test Results: We reviewed the FY09 annual report, noting 102 risk assessments were performed during the year. The risk assessments were used to determine if IOIA classified a project as a major system development or modification. After the risk assessment, 11 projects resulted in pre-implementation or post-implementations audits to be scheduled in 2010.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

AUDITOR’S NOTE

Pursuant to Public Act 96-795, effective July1, 2010, the internal auditors consolidated under Executive Order 2003-10 will be transferred to the individual agencies. It will be the responsibility of the internal auditors at their respective agencies to conduct audits in accordance to the Fiscal Control and Internal Auditing Act (30 ILCS 10) beginning in fiscal year 2011.

AGENCY RELATIONS (AR)

EXISTING ENVIRONMENT

Department's Description of Controls: The Department utilizes the following methods to ensure agencies are made aware of significant events/changes:

- The Department coordinates changes for the Bureau website, www.bccs.illinois.gov, which serves as a central location for communicating available services including the Service Catalog, key contact information, forms and guides for requesting services, announcements/bulletins, and a variety of other Bureau information.
- The Department also maintains the CIO Service Site at cms.partner.illinois.gov/bccs/Service/default.aspx, where all consolidated agency communications are stored and maintained.
- The quarterly customer-focused newsletter is published to provide another vehicle for sharing information with our customers. The newsletter is distributed to telecommunications and IT customers via email and is also posted to the Bureau website.

Tests Performed: Reviewed Bureau website, CIO Service Site, and quarterly newsletters.

Test Results: During our review of the Bureau's website located at www.bccs.illinois.gov, we noted the website contained the following information: Service Catalog, key contact information, forms and guides for requesting services, announcements/bulletins, and a variety of other Bureau information.

In reviewing the CIO Service Site, we determined the site contained separate sections for each of the consolidated agencies, and communications were stored and maintained for each agency. Communications included switch maintenance, deployments, rates, and outages.

During our review, we identified two Pulse Newsletters and four Cybertip Newsletters that were published during the audit period.

No significant exception noted.

Department's Description of Controls: The Department's AR mailbox, CMS.BCCS.agencyrelations@illinois.gov, is an email box that allows customers to document their questions or concerns. A link to this mailbox is available from the BCCS website.

- The Department's AR staff monitors the mailbox on a regular basis to address any customer questions or concerns. They research any issues that they cannot immediately address to provide timely, accurate responses.

Tests Performed: Reviewed the Bureau's website and interviewed staff.

Test Results: The Bureau's website contained a link to the AR mailbox -- CMS.BCCS.agencyrelations@illinois.gov.

AR staff monitored the mailbox and if necessary forwarded questions or concerns to subject matter experts for follow-up and response.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

EXISTING ENVIRONMENT

Department's Description of Control: The Recovery Methodology provides guidance and materials for the restoration of the various environments.

Tests Performed: Reviewed Methodology and interviewed staff.

Test Results: The Department developed the State of Illinois, Department of Central Management Services, Bureau of Communication and Computer Services, Recovery Methodology (Methodology), effective January 1, 2010.

The purpose of the Methodology was to provide direction and recommendations to "produce effective and detailed instructions" for the recovery of systems and services.

The Methodology provided guidance to agencies in conducting a Business Impact Analysis, identifying critical applications, and defining recovery time objectives.

The Methodology outlined two criteria for determining the classification of an application; recovery category and recovery stage.

The categories were defined as:

- Category One-Human Safety-applications which have a direct impact on the lives of citizens and employees.
- Category Two-Welfare/Human Safety-applications which have a direct impact on the well-being of citizens and employees.
- Category Three-Non-welfare/Human Services-a human resource service which has a direct impact on the well-being of citizens and employees.
- Category Four-Administrative Functions and Processes-applications which support state processes.
- Category Five-Specific Agency Functions and Processes-maintenance of specific processes.

Additionally, the Methodology identified the recovery time objective (maximum time agencies can be without resources) for each recovery stage.

- 0 to 72 hours -- Stage Zero,
- 72 to 168 hours -- Stage One, and
- > 168 hours -- Stage Two.

The Methodology stated all Stage Zero, Category One applications would be recovered first. After the recovery of the Stage Zero applications, all remaining Category One applications would be recovered. In the event there was additional space, Category Two applications would be recovered.

No significant exception noted.

Department's Description of Control: The Recovery Activation Plan provides instructions and actions required when recovering CMS/BCCS computing facilities and services.

Tests Performed: Reviewed Recovery Activation Plan**,** recovery packets, and interviewed staff.

Test Results: The Department developed the State of Illinois, Department of Central Management Services, Bureau of Communication and Computer Services, Recovery Activation Plan (Plan), effective January 1, 2010.

The purpose of the Plan was to provide "instructions and actions required when recovering CMS/BCCS computing facilities and services." The Plan was limited to events affecting CMS/BCCS computing facilities and services.

The Plan provided guidance regarding the assessment of damage to the restoration of services at the off-site vendor location. Our review of the Plan revealed the inclusion of employees who were no longer with the Department.

The Plan made reference to "recovery packets" which provided detailed instruction for the restoration of the environment.

The Department developed recovery packets for:

- Mainframe Recovery Packet (updated January 22, 2009),
- Distributed System Packet (updated January 19, 2010),
- Network Recovery Packet (updated January 11, 2010), and
- Recovery Services Exercise (documentation from December 2009 test).

Each recovery packet stated, "this document covers the various resources needed to restore the Information Technology (IT) infrastructure system for identified critical applications at an alternate site in the event of sustained unavailability of the production IT system."

The Recovery Activation Plan existed and was dated January 1, 2010; however, it contained outdated information on staff members who had left the Department prior to the January 2010 update.

Department's Description of Control: The Department has a process where user agencies periodically update the categorization of Criticality and Recovery Time objectives provided in the Business Reference Module (BRM).

Tests Performed: Reviewed Methodology, BRM, quarterly recovery audio conference agenda, and interviewed staff.

Test Results: During the quarterly CMS/BCCS recovery services audio conference, agencies were reminded to enter/update the categorization and prioritization of critical applications in the BRM.

The Methodology outlined two criteria for determining the classification of an application; recovery category and recovery stage (based on recovery time objective). During our review, we noted the BRM contained fields for the recovery category and the recovery stage.

No significant exception noted.

Department's Description of Control: The IT Recovery Policy outlines the individual agency's responsibility to update the BRM with critical resources and timeframes for recovery.

Tests Performed: Reviewed IT Recovery Policy and interviewed staff.

Test Results: The Department developed the State of Illinois, Department of Central Management Services, IT (Information Technology) Recovery Policy (Policy), effective October 1, 2009. The purpose of the Policy was to "direct the creation of supporting procedures, methods, and process documentation and identify roles, responsibilities, and resources" to recovery information systems hosted by the Department.

The Policy stated each agency was responsible for "developing and maintaining appropriate business continuity plans, application recovery scripts, designated application information updates to the BRM, recovery exercise procedures and schedules, and on-going communications with CMS."

The Department was to define and maintain the criticality classification and recovery time objective ranges. Additionally, based on agency information, the Department was to collect and maintain the criticality class and recovery time objective ranges.

In addition, the Department was to maintain the IT infrastructure for recovery of agency designated and justified systems. The agencies were to coordinate with the Department for testing, which should be conducted at least annually.

No significant exception noted.

Department's Description of Control: The Department has contracted with a recovery vendor to provide an alternate recovery data processing facility.

Tests Performed: Reviewed recovery service provider contracts.

Test Results: The Department had a contract with an out-of-state disaster recovery service provider to provide recovery services in the event of a major regional disaster with prolonged outages.

According to the contract, in the event of a disruption, the State would activate the agreement with the recovery service provider required to supply mainframe recovery services, resources, personnel and other supplies and services to ensure recovery of essential information processing capabilities.

The contract expires in December 2011.

In addition, the Department entered into a two year contract for “securing a highly available alternate data center/failover site and services to recover CMS hosting obligations.” The contract would provide the Department floor space, electricity, security, and telecommunication services.

The contract stated it would be the responsibility of the Department to procure the hardware and software in order to run the applications which would be hosted at the facility.

No significant exception noted.

Department’s Description of Control: The Department has contracted with a vaulting vendor to store in its vault backup data and recovery procedures required to restore critical IT infrastructure.

Tests Performed: Reviewed vaulting vendor contract, and off-site storage facility.

Test Results: The Department utilized an off-site storage facility to maintain backups and disaster recovery material.

We reviewed the physical security controls, noting they appeared to be generally acceptable.

No significant exception noted.

Department’s Description of Control: The Department conducts periodic exercises to help ensure recovery requirements can be met.

Tests Performed: Reviewed the Recovery Methodology, Activation Plan, exercise documentation, critical application listing, and interviewed staff.

Test Results: The Department conducted regional and local recovery tests as defined in the Recovery Methodology.

According to the Activation Plan, “Stage 0, Category One applications/functions recovery plan must be exercised annually to ensure their recoverability.”

According to the Methodology, “exercises involving CMS/BCCS computing facilities and services must be scheduled in advance with the following documentation:

- ESR with dates for exercise,
- Exercise plan, including application and functionality to exercise, hardware requirements, connectivity requirements, backup/tape recovery requirements,
- Application recovery scripts,
- User rehearsal scripts, and
- Exercise documentation including results, contingencies, changes, remediation steps, and corrective action plan.”

The Department conducted testing of its computing facility and services at the recovery service provider's site in December 2009.

Our review of exercise documentation indicated the four agencies, including the Department, with Stage Zero, Category One applications participated in the exercise. However, we noted one Stage Zero, Category One was not part of the testing. Additionally, the application had not been tested at the local facility.

The exercise documentation did not meet the documentation requirements outlined in the Methodology. Specifically, the exercise plans, and exercise documentation was lacking. In addition, exercise documentation indicated problems had been encountered; however, a corrective action plan had not been developed.

In August and October 2009, three agencies conducted three separate exercises at a local recovery site. However, the exercise documentation did not meet the documentation requirements outlined in the Methodology. Specifically, the documentation did not contain an ESR, recovery scripts, and exercise documentation.

A recovery test was performed in December 2009; however, all Stage Zero, Category One applications were not included in the test and supporting documentation did not meet the requirements outlined in the Methodology. Additionally, local recovery tests were performed; however, exercise documentation lacked detailed information.

OVERALL CONCLUSION

Correspondence from the Acting Deputy Director in April 2010 stated "Over the past year, BCCS has improved on Continuity Services for CMS and State agencies… It is the Department's intent to continue to diligently pursue providing and improving continuity recovery services." Also, as outlined in the Control, the Department has made improvements in the capabilities to provide continuous service.

However, we continue to believe it is imperative the Department have in place a comprehensive framework to promote and apply disaster recovery services. To promote a comprehensive recovery framework, the Department should ensure:

- The Recovery Activation Plan is updated to reflect the current environment.
- All Stage Zero, Category One applications participate in the recovery exercises.
- Documentation supporting recovery exercises contains appropriate and required detailed information as outlined in the Methodology.

From a broad overview perspective, the Department should:

- Ensure the necessary components (plans, equipment, and facilities) are available to provide for the continuation of critical computer operations in the event of a disaster.
- Conduct comprehensive tests of the applications on an annual basis.

CUSTOMER MANAGEMENT CENTER (CMC)

EXISTING ENVIRONMENT

Background Provided by the Department: The CMC provides 24/7 network support for the State of Illinois. Additionally, after 5 p.m. and during non-business hours, the CMC provides help desk support for voice, wireless, and data services.

Department's Description of Control: Incident tickets are initiated by a constituent call or discovered by a proactive monitoring system.

Tests Performed: Reviewed tickets, procedures, and interviewed staff.

Test Results: Incident tickets were created in ICN Remedy by the CMC staff as a result of either a phone call or an alarm from the monitoring system.

No significant exception noted.

Department's Description of Control: ICN Remedy is utilized to log/track incident tickets. The CMC Sharepoint site contains methods and procedures to assist staff with incident tickets.

- MP ICN Remedy Ticket Procedure and MP CMS Remedy Login Procedure.

Tests Performed: Reviewed procedures, Sharepoint site, ICN Remedy tickets, and interviewed staff.

Test Results: The Department utilized ICN Remedy to log and track incident tickets.

The CMC Sharepoint site contained the following procedures; MP ICN Remedy Ticket Procedures and the MP CMS Remedy Login Procedure.

The Department developed the MP ICN Remedy Ticket Procedures, last reviewed October 2008 and the MP CMS Remedy Login Procedure, last reviewed December 2008 to provide guidance on logging into ICN Remedy and the creation and resolution of tickets. However, we noted the ICN Remedy Ticket Procedures did not include a process to ensure sensitive transactions (such as those involving security settings) generated from incident tickets were approved by authorized staff.

We reviewed 25 ICN Remedy tickets for completeness and timeliness, noting the tickets were properly completed and the tickets were on average resolved within 5.44 days.

No significant exception noted; however, the Remedy Ticket Procedures did not include a process to ensure sensitive transactions generated from incident tickets were approved by authorized staff.

Department's Description of Control: ICN Remedy ticket logs and reports are utilized in identifying problem trends and recurring problems.

- Reviews are completed by supervisors who may escalate to internal, external teams.

Tests Performed: Reviewed tickets and interviewed staff.

Test Results: Logs and reports of ICN Remedy tickets were utilized to identify trends and recurring problems. The reports were reviewed by supervisors on a case by case basis. Additionally, the supervisor would escalate a problem if warranted.

No significant exception noted.

Department's Description of Control: The CMC Sharepoint site contains methods and procedures for the management of vendors.

Tests Performed: Reviewed policies and tested tickets.

Test Results: The CMC Sharepoint site contained the CMC M&P: Managing Escalation and Carriers procedures (last revised August 8, 2008). The procedures identified general escalation information along with guidance on escalating issues to vendors.

We reviewed 49 of 49 CMS Remedy tickets, which had been escalated, noting the work logs captured information regarding problems and resolutions. Additionally, we noted it took 22 days on average to resolve an escalated ticket.

No significant exception noted.

Department's Description of Control: The CMC monitors the IT infrastructure utilizing a monitoring system.

- The CMC Sharepoint site contains procedures for responding to alarms.

Tests Performed: Reviewed procedures and interviewed staff.

Test Results: The CMC, along with the Systems Operations Center and Field Operations utilized various monitoring systems, including Solarwinds and WhatsUpGold. During non-business hours (after 5:00 pm, weekends, and holidays) the CMC was responsible for monitoring these alarms.

The CMC SharePoint Site contained the CMC: M&P After Hours Server Support procedure, dated February 2, 2009 to assist in responding to Solarwinds and WhatsUpGold alarms.

Upon notification of an alarm, an ICN Remedy ticket was created and a CMS Remedy ticket was created.

See the Communications Solution Center control for review of the CMS Remedy tickets.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. However, to enhance the Department’s controls, the Department should include a process in the MP ICN Remedy Ticket Procedures to ensure sensitive transactions generated from incident tickets are approved by authorized staff.

COMMUNICATIONS SOLUTION CENTER (CSC)

EXISTING ENVIRONMENT

Background Provided by the Department: The CSC is responsible for providing Tier 1 support for Telecommunications (excluding Illinois Century Network and Radio) and IT services.

Department Description of Control: The CSC is a single point of contact (SPOC) where client solutions are handled for different technologies and simplifying end user support.

Test Performed: Interviewed staff.

Test Results: The CSC was the point of contact for technological and end user support.

No significant exception noted.

Department Description of Control: The CSC is responsible for managing timelines and the value of the products and services offered through the CSC Service Desk and the vendors and internal teams supporting those products and services.

Test Performed: Interviewed staff.

Test Results: The CSC was responsible for services offered through the CSC Service Desk and supporting the products and services.

No significant exception noted.

Department Description of Control: The CSC has processes and guidelines in place for enterprise-wide management, escalation and notifications, and other operational needs.

Tests Performed: Reviewed methods and procedures and interviewed staff.

Test Results: The Department developed several methods and procedures to address enterprise-wide management, escalation and notifications, and other operational needs.

No significant exception noted.

Telecommunications Service Desk

Background Provided by the Department: The Telecommunications Service Desk is responsible for maintenance and provisioning of voice, video, data and wireless systems and services for State agencies, departments, constitutional officers, commissions, boards, universities and institutions.

Department’s Description of Control: The Telecommunications Service Desk handles all calls for telecommunications services during regular business hours Monday thru Friday 8am through 5pm, excluding ICN and Internet calls which are routed directly to the CMC. All telecommunications service calls outside regular business hours and on holidays are handled by the CMC

Tests Performed: Interviewed staff.

Test Results: The Telecommunications Service Desk was responsible for telecommunication calls during regular business hours. The CMC was responsible for ICN, Internet, and after-hours service calls. The CMC was also responsible for telecommunications service calls outside of regular business hours and on holidays. See the CMC control for additional information.

No significant exception noted.

Department's Description of Control: The Help Desk records all reported incidents in the Remedy Help Desk module. Customers contact the Help Desk via phone to report an incident. The Help Desk is responsible for all reported incidents from the time reported until resolution and confirmation from the customer is achieved. Procedures exist for the Help Desk task.

Tests Performed: Reviewed procedures, Remedy tickets, and interviewed staff.

Test Results: The Department developed the Remedy User Guide, dated June 2007 and the Telecom Help Desk – Remedy Procedures/Cliff Notes, dated June 4, 2009 to assist help desk staff in the creation of Remedy tickets.

We reviewed the Telecom Help Desk – Remedy Procedures/Cliff Notes, noting it did not include a process to ensure sensitive transactions generated from incident tickets, such as those involving security settings, were approved by authorized staff.

Upon notification from the user, the help desk staff created an incident ticket within Remedy.

We reviewed 25 Remedy tickets, noting the tickets were completed appropriately and work logs captured information regarding the problem and resolution.

No significant exception noted; however, the Telecom Help Desk – Remedy Procedures/Cliff Notes did not include a process to ensure sensitive transaction generated from incident tickets were approved by authorized staff.

Department's Description of Control: Monthly reports are generated from the Remedy and EMS systems based on a fiscal year to track and monitor vendor performance levels for voice related services. These figures are reconciled with the appropriate vendor(s). The CSC managers and Quality Assurance staff attend a quarterly meeting with the vendor(s) to review task related reports.

Tests Performed: Reviewed reports and meeting agendas.

Test Results: Each month reports were generated from the Remedy and EMS systems in order to track and monitor vendor performance. The Department utilized the reports to determine if the vendor met stated performance levels.

We reviewed reports from July 2009 to March 2010 to determine the year to date percentages of completed orders, noting each vendor on average completed approximately 98% of the services requested by the Department.

In addition, the CSC manager and the Quality Assurance staff met with the vendors to review the reports and discuss performance levels. We reviewed quarterly meeting agendas with the three vendors, noting the Department conducted quarterly meetings with two vendors and conducted one meeting with a third vendor.

No significant exception noted.

Department's Description of Control: The Provisioning unit receives forms via email or mailed paper copies from the authorized agency coordinator. All telecommunications changes require a request form. Different forms are required for different services. Data requests require a Telecommunications Data/Intercity Service Request form (TDR); voice and cellular requests require a Telecommunications Service Request (TSR); paging requests require a Paging Service Request (PSR); IWIN requests require a Wireless Service Request (WSR) form.

Each agency head delegates, in writing, a telecommunications coordinator(s) authorized to expend funds. The Telecom Coordinator database is maintained by the CSC Administration staff and an alternate. The agency coordinator is responsible for submitting the appropriate request forms to the Telecommunications Service Desk for all telecommunications changes. The CSC Provisioning staff is responsible for verifying the submitter is an authorized coordinator in the database. The coordinators can locate the instructions for completing these forms on the Telecom Web site (http://bccs.illinois.gov/telecom/) and are provided guidance by the Provisioning staff when necessary. Procedures exist for the Provisioning task.

Tests Performed: Reviewed procedures, Agency Registration forms, website, and interviewed staff.

Test Results: The Department developed several procedures for the provisioning tasks. The procedures addressed entering in inventory items, changes, duplicates, manual billing, multiple services and inquiry only processes.

Additionally, the Department maintained various telecommunication forms and instructions on the Telecom website.

The Department maintained the Telecom Coordinator database which listed agency coordinators authorized to expend funds.

We reviewed 25 telecommunication change requests, noting all had been appropriately completed and authorized by a Telecom Coordinator.

No significant exception noted.

Department’s Description of Control: The agency coordinators have access to EMS and can check status of their agency orders only. The EMS system tracks ordered facilities and telecommunications equipment. The inventory module provides the asset’s recurring monthly charge, location information, ‘AU’ code, maintenance vendor description, catalog description and model description in addition to user name, tag number and serial number if applicable to the inventory item. The inventoried asset’s installation cost can be found for all rated catalog codes in the EMS Catalog Table. Anytime an inventoried piece of equipment is installed, removed or moves from one location to another, an order is entered into the EMS system to update the system inventory.

Tests Performed: Reviewed EMS system, EMS Catalog Table, reconciliations, access rights, and interviewed staff.

Test Results: The Expense Management System (EMS) tracked orders, facilities, and telecommunications equipment. We reviewed EMS, noting the following fields were available: asset’s recurring monthly charge, location information, ‘AU’ code, maintenance vendor description, catalog description and model description in addition to user name, tag number and serial number if applicable to the inventory item.

Additionally, we reviewed the EMS Catalog Table, noting the table included the following information: catalog number, description, type, group, status, maximum quantity, effective date, disabled date and billing summary and the inventoried asset’s installation cost for all rated catalog codes.

Annually, the Department conducted a reconciliation of EMS and the Central Inventory System, to ensure inventoried equipment that was installed, removed, or moved from one location to another was accurately reflected.

In addition, agency coordinators had access to EMS and checked the status of their agency orders only.

We reviewed 25 Department employees that had update access to EMS, noting no exceptions.

No significant exception noted.

Department’s Description of Control: Tagged data equipment is received and tagged by Business Services’ warehouse staff while tagged voice equipment is sent directly to the site. A Property Control Form (PCF) is completed for newly tagged voice systems and attached to the original invoice before it is sent to Business Services for processing and entry into the Common Inventory System (CIS). The voice system is tagged by the Consulting and Procurement staff at the time of acceptance. Tagged data and voice equipment listed in EMS is reconciled to the listed equipment in CIS annually by Business Services. Discrepancies are reported to CSC management and investigated. Appropriate reconciliation is then taken.

Tests Performed: Reviewed equipment procedures, Property Control Forms, and inventory listings.

Test Results: The Department developed the Remedy "Soft Launch" CSC Provisioning Request Non Routine CSS Level 1 & 2 procedures dated April 27, 2010, which governed the process of tagging new voice equipment.

A Property Control Form (PCF) was to be completed for new voice systems, attached to invoices, then sent to Business Services for processing. The newly tagged equipment was then entered into the Central Inventory System (CIS).

We reviewed six newly tagged pieces of equipment for the PCF and entry into CIS, noting one was not completed. The item was received and installed on October 16, 2009 and as of April 15, 2010 the item still had not been entered into the system.

Annually, the Department reconciled EMS inventory listing and the CIS inventory listing. The reconciliation for fiscal year 2009 was completed on January 4, 2010. Discrepancies were reported to CSC management and investigated.

During our review, we noted the EMS inventory listing and the CIS inventory listing reconciled.

No significant exception noted; however, the Department had not completed all property control forms and did not enter all newly tagged inventory items into the Central Inventory System.

Department's Description of Control: The Consulting and Procurement unit provides agencies with an assigned Communications Systems Specialist 2 (CSS2). There is one Consulting and Procurement staff members in the JRTC Building in Chicago. The CSS2s work closely with the agency coordinators to consult and analyze their present and future telecommunications needs and design systems to meet those requirements in the most efficient and economical manner. The CSS2s are responsible for managing non-routine service requests. Procedures exist for the Consulting and Procurement unit tasks.

Tests Performed: Reviewed procedures, provisioning tickets, and interviewed staff.

Test Results: The Department employed nine CSS2s, with one member located in the Thompson Center. The Consulting and Procurement staff worked with agency coordinators to analyze telecommunication needs. To manage non-routine service requests, the Department developed the Remedy "Soft Launch" CSC Provisioning Request Non Routine CSS Level 1 & 2 'procedures' dated April 27, 2010 to assist staff when entering provisioning requests into the Remedy Provisioning module.

We reviewed 25 provisioning tickets, noting appropriate approvals were maintained.

No significant exception noted.

Department's Description of Control: This unit is also responsible for managing master contracts and site/service specific contracts for telecommunications equipment and services. Network Services assists this unit with the review of TDRs that are related to the ICN backbone and WAN requests for the agencies statewide. The BCCS Shared Services teams are engaged on telecom requests for the Consolidated Agencies when systems require PCs, Servers, and connectivity to the CMS network.

Tests Performed: Reviewed listing of contracts and contract renewals, procedures, and interviewed staff.

Test Results: To ensure telecommunication requests were reviewed and the appropriate Shared Services teams were engaged, including Network Services, the Department utilized the Remedy "Soft Launch" CSC Provisioning Request Non Routine CSS Level 1 & 2 'procedures' dated April 27, 2010.

The Consulting and Procurement Unit managed 38 master contracts and site/service specific contracts for telecommunications equipment and services.

No significant exception noted.

IT Service Desk

Background Provided by the Department: The CSC IT Service Desk is responsible for providing Tier 1 IT technical and end user support to the consolidated agencies as well as multiple boards, commissions and non-consolidated agencies. The IT Service Desk is the single point of contact for reporting IT incidents and requesting new services.

Department's Description of Control: The IT Service Desk is staffed during normal business hours Monday thru Friday 8 am to 5 pm, with extended coverage from 8 am to 4 pm on Saturday and Sunday for HFS and DHS. Evening coverage for HFS and DHS is provided by production operations staff working at 120 West Jefferson in Springfield. Appropriate security is inherent to the tool used.

Tests Performed: Interviewed staff.

Test Results: The IT Service Desk was staffed during business hours, Monday through Friday (7am to 5pm). Additional coverage was available for HFS and DHS on Saturday and Sunday (8am to 4pm). Additionally, the IT Service Desk provided after hours support for business critical situations for all consolidated agencies.

The IT Service Desk had taken 127,956 calls over 42 weeks, averaged 3,046 calls per week, and 609 calls per day since July, 1, 2009.

The Department utilized Remedy as the tool for managing help desk incidents/service requests. The Remedy administration features determined which application modules were accessed by each individual user. Each user was assigned a floating or fixed license based on need and given the appropriate application permissions (i.e. read, write, modify, delete) based on their job function or role.

No significant exception noted.

Department's Description of Control: Customers contact the IT Service Desk via phone or email to report an incident. The Service Desk staff opens a ticket in BCCS Remedy and records the category, type, and item (CTI), as well as the customer name, agency, contact and demographic information and a detailed incident description. If the IT Service Desk is unable to resolve the incident, the ticket is assigned to Tier 2 or Tier 3 support teams based on the CTI and/or predefined summary field. Procedures exist for the Help Desk task.

Tests Performed: Reviewed procedures, Remedy User Guide, Remedy incident tickets, and interviewed staff.

Test Results: The Department had developed several methods and procedures to assist staff with the operations of the CSC. In addition, the Department developed the Remedy User Guide to assist with the creation of Remedy tickets.

Users contacted the IT Service Desk to report incidents. The IT Service Desk staff recorded the incident and subsequently updated the customer information within Remedy.

In the event the IT Service Desk staff was unable to resolve the problem, the ticket was escalated to a Tier 2 and Tier 3 support team member.

We reviewed 25 incident tickets documented within the Remedy Help Desk module, noting tickets maintained the CTI, customer name, agency, contact, description, and were appropriately completed.

No significant exception noted.

Department's Description of Control: The IT Service Desk receives an Enterprise Service Request form (ESR) from an authorized IT coordinator for all IT changes. The IT Service Desk has standardized on the ESR process and the intake of service requests in the Remedy system for all consolidated agencies. Service requests are submitted via email.

Tests Performed: Reviewed instructions and procedures, IT Coordinator lists, ESRs, and interviewed staff.

Test Results: The Department developed the Enterprise Service Request (ESR) Instructions, dated May 14, 2009. The Instructions provided guidance to the agency and the IT Service Desk staff on the completion of an ESR.

An ESR provided "the end user a means to request standard or routine software or hardware related additions, moves or changes to their desktop system." An ESR was required for IT changes. After the receipt of the ESR, the IT Service Desk staff were to create a Remedy change management ticket with the category type as "service request", assign it to the appropriate team, and attach the ESR.

According to the Remedy User Guide, IT Service Desk staff were charged with reviewing ESRs for completeness and accuracy. In addition, the Department developed several procedures to assist staff in the completion of Remedy tickets, ESRs and addendums.

We reviewed 25 service requests, noting nine did not maintain an ESR.

An ESR was not completed for all service requests.

Department's Description of Control: Each agency head delegates, in writing, an IT coordinator(s) authorized to expend funds. The IT Coordinator database is maintained by Agency Relations. The IT coordinator is responsible for submitting the appropriate request forms to the IT Service Desk for all IT changes. The IT Service Desk staff is responsible for verifying the submitter is an authorized coordinator in the database. The coordinators can locate the instructions for completing these forms on the Bureau's Web site (http://bccs.illinois.gov/forms_it.htm) and are provided guidance by the IT staff when necessary. Procedures exist for the ESR processing task.

Tests Performed: Reviewed procedures, website, Agency Registration Contact Form, service requests and interviewed staff.

Test Results: The Department had developed several procedures for the Enterprise Service Request process, in addition to several procedures addressing the following: internet access, Remedy access, credit adjustments, network services, modifications, mainframe security requests, and Sharepoint site development. The procedures and forms were located on the Department's website http://bccs.illinois.gov/forms_it.htm and were utilized to provide support and guidance to users.

In addition, the Department maintained the IT Coordinator database which listed agency coordinators authorized to expend funds.

Of the 16 service requests available for our review, all were authorized by an IT Coordinator.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. However, to enhance the Department's controls, the Department should:

- Ensure an ESR is properly completed for all service requests.
- Include a process in the Telecom Help Desk – Remedy Procedures/Cliff Notes to ensure sensitive transactions generated from incident tickets are approved by authorized staff.
- Ensure all Property Control Forms for newly tagged inventory items are completed and adequately entered into the Central Inventory System.

END USER COMPUTING (EUC)

EXISTING ENVIRONMENT

Background Provided by the Department: EUC provides maintenance, support and security of the personal computer infrastructure and provides desktop and laptop services.

Department's Description of Control: The following policies are utilized to assist staff in their duties:

- End User Computing Device Standard
- CMS Desktop/Laptop Personal Computer Standard
- EUC IT MAC Technical Assistant Procedure
- IBM Technical Services Program (TSP) Time and Materials (T&M) Billing Sign-Off Procedure.

Tests Performed: Reviewed standards and procedures, personal computers, monthly reconciliations, and interviewed staff.

Test Results: The Department had developed several standards and procedures which addressed naming convention standards, standards for setting up desktop/laptops in the Illinois.gov domain, reviewing an ESR, and billing processes.

- End User Computing Device Standard, effective January 26, 2009,
- CMS Desktop/Laptop Personal Computer Standard, dated May 19, 2008,
- EUC IT MAC Technical Assistant Procedure, effective September 22, 2009, and
- IBM Technical Services Program (TSP) Time and Materials (T&M) Billing Sign-Off Procedure, effective November 12, 2008.

We reviewed the CMS Desktop/Laptop Personal Computer Standard for compliance noting:

The CMS Desktop/Laptop Personal Computer Standard required all personal computers within the Illinois.gov domain to comply with security policies and be configured with latest antivirus updates and security patched. However, our review indicated antivirus and security patches had not been timely applied to hundreds of personal computers. Additionally, we noted the standard was only applied to approximately 10% of the personal computers in which EUC supported under the Illinois.gov domain.

In addition, exceptions to the CMS Desktop/Laptop Personal Computer Standard were required to have an ESR showing justification for the change. However, we identified 920 personal computers that were exempt from requirements that did not have a properly completed ESR.

The Department had developed standards and procedures designed to provide security over personal computers; however, the Department had not complied with all the requirements in the CMS Desktop/Laptop Personal Computer Standard.

Department's Description of Control: Remedy Action Request System is used to initially log incidents (help desk tickets) and requests (ESRs).

- Versions of addendums are attached to ESRs providing the changing details associated with the ESR.
- The work log in Remedy is used for incidents and ESRs to document activity.
- The Remedy Action Request System audit trail for the incident or ESR will document a change in the assignment or status.
- Remedy Action Request System is used to capture the priority of the incident or ESR.
- Priorities are established by the customer at the time the incident or ESR is initiated with IT Service Desk.
- Customers can call the IT Service Desk for updates on any incident or ESR.
- Customers receive a system generated email from Remedy Action Request System when the status of an incident or ESR changes (confirmation is needed on what status changes generate an email).
- The work log within Remedy Action Request System is used by anyone that engages in the working of an incident or ESR to record the activity performed.
- Tasks within Remedy Action Request System are used for ESRs that require multiple shared services teams to be engaged in the request.
- Technical assessment is a task used to initially reach out to the customer to confirm request.
- The Customer Satisfaction task is used by the IT Service Desk to confirm completion and customer satisfaction.

Tests Performed: Reviewed incidents, service requests, and interviewed staff.

Test Results: When the service desk received a call from a user regarding a technical problem; a help desk ticket was created within Remedy and assigned to EUC. EUC evaluated and worked to resolve the problem. Upon completion, the Remedy ticket and work log were updated.

We reviewed 25 tickets to determine compliance with the following: Remedy ticket numbers, ESRs, work log, audit trail, priority, tasks, technical assessments, and customer satisfaction. We noted general compliance with the requirements with the exception of the completion the Customer Satisfaction task.

No significant exception noted; however, the Customer Satisfaction task was not always properly completed.

OVERALL CONCLUSION

Although the Department had developed standards and procedures designed to provide maintenance, support and security over the personal computer infrastructure, some provisions had not been effectively implemented.

The Department should ensure it is complying with all provisions of the standards and procedures over the personal computer infrastructure. Specifically, the Department should ensure:

- The Department's standards and procedures are appropriately applied to all personal computers in the Illinois.gov domain supported by the Department.
- All tasks outlined in the Remedy Action Request System or ESR process are properly completed.

QUALITY ASSURANCE

EXISTING ENVIRONMENT

Background Provided by the Department: The Infrastructure Quality Assurance and Methods (IQAM) group act as facilitators for organizing, planning and controlling work activities for the Infrastructure Services Division related to Agency IT projects.

Department's Description of Control: Process and procedures that govern this process are located in the IQAM Guide.

Tests Performed: Reviewed the IQAM Guide, project documentation, and interviewed staff.

Test Results: The Department established the IQAM Guide (officially named ISD Charter Review Procedure) in March 2006, and last updated January 2010. The Guide outlined the process to introduce projects into infrastructure services.

We reviewed three projects to ensure compliance with the IQAM Guide, noting no exceptions.

No significant exception noted.

Department's Description of Control: The EPM Portal and Remedy are utilized to monitor projects.

Tests Performed: Reviewed listings in the EPM Portal and Remedy, and interviewed staff.

Test Results: During our review, we obtained a listing of completed projects from the EPM Portal and a listing of completed projects from the Remedy Project Module. The EPM Portal listing indicated 16 completed projects and the Remedy Project Module indicated 33 completed projects.

No significant exception noted.

Department's Description of Control: The EPM Portal and meetings are utilized to communicate with the project owners.

Tests Performed: Reviewed EPM Portal and meeting minutes.

Test Results: We reviewed the EPM Portal noting various tracking, status, and approvals were maintained for projects.

In addition, we reviewed three projects being facilitated by IQAM, noting meetings were utilized to communicate with user agencies.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

CHANGE CONTROL

EXISTING ENVIRONMENT

Department's Description of Control: The Change Management Policy and BCCS Remedy Change Management Guide to manage changes.

- State of Illinois – Dept. of Central Management Services – Change Management Policy https://bccs.portal.illinois.gov/exec/centrep/ed/plcpub/Change_Management_Policy.pdf
- BCCS Remedy Change Management Guide https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx

Tests Performed: Reviewed the Change Management Policy, the BCCS Remedy Change Management Guide, and interviewed staff.

Tests Results: The Department developed the Change Management Policy (Policy), effective December 15, 2008, and the BCCS Remedy Change Management Guide (Guide), last reviewed July 13, 2009. The Policy and Guide provided guidance on documenting changes and entering/tracking changes in the Remedy Action Request System (System).

According to the Policy, "infrastructure changes for all technology platforms and systems of the CMS/BCCS managed infrastructure and environment" were to follow the Policy. The Policy defined a change as "any alteration to the state or configuration of any production software or hardware under BCCS management and support. This would include adding new functionality, repairing or removing functionality."

Exceptions to the Policy required authorization of the BCCS Chief Technology Officer (CTO). During our review, we identified one exception to the Policy, noting the exception obtained the CTO's approval.

The Guide stated the purpose was to "standardize the actions, behaviors and responsibilities related to the processing of Change Requests for utilizing the Remedy Change Management application."

The Guide defined the authorization and approval processes, roles and responsibilities, emergency changes, and user involvement for specified changes. The Guide stated testing plans were only required for high impact changes and the level of testing was the responsibility of the Shared Services Team.

Although the Change Management Unit was responsible for the majority of the primary functions covered by this review; several other related functions, such as Web Services, Enterprise Business Application Services, DOT, DHS and DHFS mainframe, and networks for non-state agencies followed different processes for change management.

Specifically we found that changes to the Department's mainframe operating system followed the Department's change management process.

Although an established procedure existed, several additional functions related to the Department's primary services did not follow the established Change Management Policy or Guide.

Department's Description of Control: The Remedy Action Request System is used to request and track changes.

Tests Performed: Reviewed Remedy Action Request System (System), BCCS Remedy Change Management Guide (Guide), change requests, and interviewed staff.

Tests Results: The Department utilized the Remedy Action Request System to request and track changes.

The Guide was divided into nine sections, which identified "specific instructions/requirements." Our review of the Guide indicated deliverables and affected resources were to be identified, along with the quantifying the impact of the change. However, the Guide did not outline the requirements to achieve these objectives.

Additionally, the Guide stated back out plans, implementation plans, and test plans were required for high impact changes; however, specific documentation requirements were not outlined.

We reviewed a sample of change tickets for compliance with the Guide, noting:

- 50 of 50 change request complied with the general requirements of the Guide.
- 30 of 31 medium and high impact changes contained the required information in the task section.
- 25 of 25 high impact changes had a back out plan, implementation plan and test plan.

No significant exception noted; however, one medium/high impact change did not meet the requirements outlined in the Guide. In addition, we noted the documentation requirements were not always outlined.

Department's Description of Control: Changes are approved utilizing and/or in accordance with:

- Remedy Action Request System
- BCCS Remedy Change Management Guide
  - Business Owner Review
  - Validate Change Variables – Technical / Business

  https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx
- State of Illinois – Dept. of Central Management Services – Change Management Policy https://bccs.portal.illinois.gov/exec/centrep/ed/plcpub/Change_Management_Policy.pdf

The Remedy Action Request System ensures the proper authorization of changes are tracked.

Tests Performed: Reviewed Remedy Action Request System (System), BCCS Remedy Change Management Guide (Guide), Change Management Policy (Policy), change requests, and interviewed staff.

Tests Results: The purpose of the Business Owner Review Section of the Guide was to standardize proposed change review by Business Owners. The Business Owners would review the deliverable, affected resources, and the impact of the proposed change identified by the technician and/or manager. If any concerns or issues were identified, the technician documented these concerns.

The Validate Change Variables-Technical/Business Section of the Guide outlined three levels of required approvals:

- Level 1-Technical Approval,
- Level 2-Enterprise Change Management Business Approval, and
- Level 3-Change Advisory Committee Business Approval.

Each level of approval was responsible for reviewing specific items associated with a request. After a level was approved, the System indicated the next steps in the approval process.

The Policy did not provide guidance on the approval of requests.

The approvals were documented and managed within the System. The process of managing and updating the list of individual who were authorized to approve was conducted via the Enterprise Service Request process. We reviewed the listing of approvers and authorizers, noting the listing had individuals who no longer were employed by the Department.

We reviewed 50 changes completed during the audit period, noting each had the appropriate approvals documented in the System.

No significant exception noted; however, the approver listing had not been updated to reflect personnel changes.

Department's Description of Control: The BCCS Remedy Change Management Guide ensures all changes are properly tested before being placed into production.

- Validate Change Variables – Technical / Business (Change Management is responsible for ensuring Testing Documentation is attached to "High" Impact Changes; Shared Services Teams are responsible for level of testing)

Tests Performed: Reviewed BCCS Remedy Change Management Guide (Guide), Mainframe Application Testing procedures, and change requests.

Tests Results: The Create Change Request Section of the Guide required a test plan for high impact requests. The omission of a test plan required the approval from the CTO.

Additionally, the Create Change Request Section indicated the level of testing was the responsibility of the Shared Services Team. However, specific documentation requirements were not outlined.

The Validate Change Variables-Technical/Business Section of the Guide indicated the Technical and ECM approvers were to review each request to ensure the required documentation was attached, including the test plan for high impact requests.

The Department had developed the Mainframe Application Testing procedures, which outlined the testing requirements before being moved into production.

Department staff stated there were no procedures for the testing of mainframe operating system releases/enhancements.

We reviewed 25 closed requests that were identified as high impact to ensure each contained a test plan, noting no exceptions.

No significant exception noted; however testing and documentation requirements were not always well-defined.

Department's Description of Control: The BCCS Remedy Change Management Guide outlines the requirements for the follow-up once a change has been completed.

- Resolve Change
- Conduct Post Implementation Review
  https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx

Tests Performed: Reviewed the BCCS Remedy Change Management Guide (Guide), Change Management Policy (Policy), change requests, and PIR spreadsheet.

Tests Results: The Policy defined a post implementation review (PIR) as a "standard method to follow up with the change owner and/or customer on the results of a change request."

According to the Conduct PIR Section of the Guide, for non-emergency changes an incident form was to be completed and for emergency changes resolution information was to be documented. The incident report was to be attached to the change ticket and the resolution information was to be documented in the work log. However, the Guide did not indicate the specific information which was to be recorded in the incident form or the resolution information. In addition, the Guide did not require communication with the owner or users.

Additionally, each post implementation review was to be logged into the PIR spreadsheet.

We reviewed all 26 emergency changes which required resolution information, noting the information was contained in the request. In addition, we reviewed seven major outage change tickets, noting no exceptions. We noted the depth of documentation was lacking.

Additionally, we noted 23 of the 26 emergency changes and seven major outage changes were included on the PIR spreadsheet.

Although PIRs were conducted, the depth of documentation and communication was lacking. In addition, we found three emergency changes were not included on the PIR spreadsheet.

Department's Description of Control: Several different communication mechanisms are in place to ensure all applicable parties are appropriately and timely notified of an upcoming change.

- Change Advisory Committee Meeting
- 30 Day Outage Report by Agency
- Change Advisory Committee Meeting Minutes
- Change Detail Report (Next 14 Days)
- Enterprise Change Schedule (Next 90 Days)

Tests Performed: Reviewed the Change Advisory Committee Meeting minutes, 30 Day Outage Report by Agency, Change Detail Report (Next 14 Days), the Enterprise Change Schedule (Next 90 Days), and interviewed staff.

Tests Results: The Department utilized several different mechanisms to communicate with all applicable parties regarding upcoming changes.

- Change Advisory Committee (CAC) Meeting,
- 30 Day Outage Report by Agency,
- Change Advisory Committee Meeting Minutes,
- Change Detail Report (Next 14 Days), and
- Enterprise Change Schedule (Next 90 Days).

According to Change Management staff, each agency had access to the Change Management Sharepoint site in order to view the reports and meeting minutes. Additionally, staff stated an email was sent out to all agencies identifying the changes to be discussed at the upcoming CAC meeting and the email included a link to the Sharepoint site.

Change Advisory Committee (CAC) meeting and meeting minutes

The Department conducted weekly CAC meetings and maintained meeting minutes. These meetings addressed upcoming changes and included: CAC approval; change group; summary; requester name; users affected by location; planned change date; change impact; change work log, etc.

30 Day Outage Report by Agency

The Department provided a 30 Day Outage Report by Agency, which had been completed and updated on a weekly basis. The report included: agency affected, outage start date, change ID, summary, count of changes with planned downtime, and estimated down time in minutes.

Change Detail Report (Next 14 Days)

The Department provided a Change Detail Report (Next 14 days), which had been completed and updated on a weekly basis. The report included the total number of changes to be completed during the next 14 days, total number that were considered emergency changes, change ID, change status, impact, planned start and end dates, change description, change supervisor, etc.

Enterprise Change Schedule (Next 90 Days)
The Department provided an Enterprise Change Schedule (Next 90 Days), which had been completed and updated on a weekly. The report was divided up into two separate reports, one for the Mainframe Group and another for all other changes. The report included total number of changes for the next 90 days, change ID, impact, status, estimated downtime, assigned, group, supervisor name, etc.

No significant exception noted.

Department's Description of Control: The Department has the following controls in place to manage the moves of hardware and/or software configuration changes into production.

- Assess Request Content & Readiness (Technical and Business)
- Change Request Approval

Tests Performed: Reviewed BCCS Remedy Change Management Guide (Guide), Remedy Action Request System (System), change requests, and interviewed staff.

Tests Results: The System was to document infrastructure changes and some application program moves directed by the consolidated agencies. The application program moves were the user entities' responsibility. To control what hardware and software changes were made, staff utilized the Validate Critical Change Variables Section of the Guide and the System maintained the approval process to ensure proper approvals were obtained prior to making the change.

We reviewed 50 change requests for proper approvals, noting no exceptions.

No significant exception noted.

Department's Description of Control: The Department has the following controls in place for controlling emergency changes.

- Authorization
    - State of Illinois – Dept. of Central Management Services – Change Management Policy https://bccs.portal.illinois.gov/exec/centrep/ed/plcpub/Change_Management_Policy.pdf
    - BCCS Remedy Change Management Guide https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx
- Testing
    - Change Management is responsible for ensuring Testing Documentation is attached to "High" Impact Change Requests; Shared Services Teams are responsible for level of testing.
- Approving
    - State of Illinois – Dept. of Central Management Services – Change Management Policy https://bccs.portal.illinois.gov/exec/centrep/ed/plcpub/Change_Management_Policy.pdf

    - BCCS Remedy Change Management Guide https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx
- Implementation.
    - BCCS Remedy Change Management Guide https://bccs.portal.illinois.gov/exec/centrep/isd/is/Pages/cng.aspx

Tests Performed: Reviewed the Change Management Policy (Policy), BCCS Remedy Change Management Guide (Guide), and emergency change requests.

Tests Results: According to the Policy an emergency was defined as "a change that does not present notification to the formal process in advance of implementation." Emergency changes will only be acceptable in the event of a system failure or the discovery of security vulnerability." The Policy also stated "all emergency changes will be reviewed and documented."

The Create Change Request Section of the Guide stated, "Emergency Changes are unscheduled changes. They are only acceptable in the event of a system failure or the discovery of security vulnerability. They follow all change management processes / procedures except they may be implemented in advance of approval in order to correct the failure in a timely manner."

We reviewed all 26 emergency changes to ensure they were completed, approved and were appropriately categorized as emergency change tickets, noting no exceptions. In addition, we noted all emergency changes identified the help desk incident number.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. To enhance controls the Department should:

- Ensure policies, procedures and guides provide clear and consistent controls over the change process.
- Ensure all changes to the Department's environment follow the Change Management Policy and Guide, and are tracked in the Remedy Action Request System.
- Ensure the listing of approvers is reviewed and updated.
- Develop testing and documentation requirements for specific actions outlined in the Policy and Guide.

SECURITY ADMINISTRATION

EXISTING ENVIRONMENT

Background Provided by the Department: The following internal documents provide management with an overall security strategy and framework.

Department's Description of Control: A document entitled "Secure Illinois Strategy" exists which lays out a simple roadmap for Department security services.

Tests Performed: Reviewed the Secure Illinois Strategy, and interviewed staff.

Test Results: The Department developed a security roadmap, Secure Illinois, dated May 18, 2009. The Department identified six areas and outlined specific projects and target dates, including several completion dates in 2009. According to the Chief Security Officer, none of the projects had been completed due to lack of resources or other priorities.

A security roadmap had been developed; however, several projects had not been finalized within the indicated timeframes.

Department's Description of Control: A document called the Security and Compliance Solutions Security Program updated on 12-15-09.

Tests Performed: Reviewed the Security and Compliance Solutions Security Program and interviewed staff.

Test Results: The Department developed the Security and Compliance Solutions Security Program (Program), effective December 15, 2009 in order to "provide guidance for establishing and maintaining a security program for the enterprise." The Program stated the operations, recommendations, and safeguards applied to any and all resources managed by the Department.

The Program outlined four goals and objectives:

- Promote secure information technology operations environment,
- Protect confidentiality, integrity and availability of data,
- Coordination/communication, and
- Identify and provide guidance on risk management, business continuity, and audits.

Per the Chief Information Security Officer, the Security Program was a work in progress.

The Department had developed guidelines for the establishing and maintaining a security program; however, the Security Program was still a work in progress.

Department's Description of Control: A document entitled "Risk Management Framework" describes the approach for assessing and defining risk in the operation.

Tests Performed: Reviewed the Risk Management Framework and interviewed staff.

Test Results: The Department developed the Risk Management Framework, dated December 15, 2009. The Framework described the “strategy, classifications, and treatment approach that CMS/BCCS had adopted to manage IT risk inherent in the delivery of services.” The objective of the Framework was to “economically, effectively, and efficiently reduce risk that is common among IT providers.”

The scope of the Framework was limited to the following areas:

- “Organizations typical in government, specifically to Illinois,
- Resources defined in the published policy as IT resources managed by CMS/BCCS,
- Risks inherent to providing IT functionality in a service organization operating in a government environment, and
- Risk defined as the potential that a vulnerability will be successfully exploited resulting in loss, damage, or other negative consequence.”

The Framework outlined the tasks, deliverables and strategy to be utilized in identifying and assessing risk.

According to the Chief Information Security Officer, the Department had not conducted any formal risk assessments during the audit period.

The Department had developed a limited-scope framework for assessing risk; however, no formal risk assessments had been completed.

Background Provided by the Department: The following controls apply to users of Department services.

Department’s Description of Control: Policies governing the computing environment have been developed and are available at http://bccs.illinois.gov/it_Policies.htm. The website is updated as policies are developed or changed. As of December 2009, the following policies were on the website.

IT Policies

- Data Classification Policy
- Enterprise Desktop/Laptop Policy
- General Security for Statewide IT Resources Policy
- General Security for Statewide Network Resources Policy
- IT (Information Technology) Recovery Policy
- IT Resource Access Policy
- Laptop Data Encryption Policy
- Midrange Backup Policy
- Statewide CMS/BCCS Facility Access Policy

General Policies

- Change Management Policy
- Data Breach Notification Policy
- ESI Retention Policy
- IT Governance Policy
- Mobile Device Security Policy
- Wireless Communication Device Policy

Tests Performed: Reviewed policies, procedures, standards, memos, BRM, background checks, revocation requests, inspected laptops, inventory listing, Remedy Asset System, and interviewed staff.

Test Results: The Department had developed and published the following policies on its website.

Information Technology Policies

- Data Classification Policy, effective December 15, 2008 and revised January 1, 2010
- Enterprise Desktop/Laptop Policy, effective December 15, 2008
- General Security for Statewide IT Resources Policy, effective December 15, 2008 and revised January 1, 2010
- General Security for Statewide Network Resources Policy, effective December 15, 2008 and revised January 1, 2010
- IT (Information Technology) Recovery Policy, effective October 1, 2009
- IT Resource Access Policy, effective December 1, 2007
- Laptop Data Encryption Policy, effective December 1, 2007 and revised January 1, 2010
- Midrange Backup Policy (TSM Shared Services), effective December 1, 2007
- Statewide CMS/BCCS Facility Access Policy, effective December 15, 2008 and revised January 1, 2010

General Policies

- Change Management Policy, effective December 15, 2008
- Data Breach Notification Policy, effective December 1, 2007 and revised January 1, 2010
- Electronically Stored Information Retention Policy, effective February 15, 2009
- IT Governance Policy, effective December 15, 2008
- Mobile Device Security Policy, effective October 1, 2009
- Wireless Communication Device Policy, effective December 15, 2008 and revised January 1, 2010
- Action Plan for Notification of a Security Breach, effective August 31, 2007
- Recovery Methodology, effective January 1, 2010

We reviewed the policies and implementation practices and found the following:

- The policies contained sections requiring the designation of responsibility to implement, monitor, audit, track, and validate compliance with the policies and procedures; however, we found implementation and monitoring processes at the Department lacking.

- The Data Classification Policy provided guidelines for data owners to classify their data into one of three categories; Public, Official Use Only, or Confidential. However, the Department had not classified its own applications or data.
- Although the Laptop Data Encryption Policy required all new laptops issued after the effective date of the Policy be equipped with full disk encryption; the Department deployed several new laptops in FY 10 without full disk encryption, in violation of the Policy.
- The Mobile Device Security Policy stated "Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including discharge, may involve civil or criminal litigation, and may involve restitution, fines, and/or penalties." However, we noted not all agencies which utilized the Department's services had been notified.

Upon notification of these issues, the Department's Chief Information Security Officer provided written updates that included the following:

- A lack of resources was a major cause for many of these issues. The Department had been operating under severe resource constraints that have impaired the ability to complete projects on time, undertake necessary risk assessments, or monitor policy compliance.
- Data Classification and resource custodian responsibility projects have been initiated. The Department has completed the initial phase of these projects by extracting information on applications from the BRM.
- Encryption software was installed on the identified laptops and the laptop deployment and installation process was being updated to improve the consistent installation of encryption software on new laptops.
- Procedures to distribute policy announcement memo and to update the Department's contact list have been updated to improve the quality and accuracy of policy notifications.

According to each policy, in order to implement this policy, CMS establishes procedures and designates responsibility to specific personnel. Based on our review of policy compliance and assignments, it appeared that the establishment of procedures and the designation of responsibility had not been effectively implemented.

According to each policy, each agency should also establish procedures and assign responsibilities to specific agency personnel to achieve policy compliance. However, the Chief Information Security Officer stated the Department had no authority over the agencies internal operations in order to ensure compliance with various policies and procedures.

Although the Department had developed policies and procedures designed to provide a security strategy and framework, all provisions had not been effectively developed or implemented. Even though several of the policies and procedures had been in effect since 2007, the Department and its internal users did not conform to several policy requirements.

Department's Description of Control: Policy update memos are distributed periodically to impacted users to announce updates to the policies. Security awareness is promoted by placing relevant information on an enterprise accessible web site http://bccs.illinois.gov/security/awareness.htm where security related news releases, tips, posters, and guidelines can be viewed. In addition, security related information is periodically emailed to user agency contacts.

Tests Performed: Reviewed memos, announcements, communications, website, and distribution listing.

Test Results: In September 2009 and January 2010, the Director of the Department issued memos regarding policy updates to Department employees.

On October 7, 2009, the Chief Information Security Officer sent a memorandum via email to the "Illinois IT community" stating the BCCS' website had been updated with the policies and announcing the proclamation of October as National Cyber Security Awareness Month.

The Department developed a website where security related news releases, tips, posters and guidelines could be viewed.

In addition, the Department held a Cyber Security Summit in October 2009.

We reviewed the distribution listing for the memorandum noting one consolidated agency's Chief Information Officer did not receive the memorandum. Additionally, we noted not all agencies which utilized the Department's services had been properly notified of the Policy update or awareness program.

The Department had processes to communicate with its user community; however, a means to ensure all users were notified had not been developed.

Department's Description of Control: Security assessments are conducted by the Department's Technical Safeguards unit. Results of those assessments are made available to appropriate BCCS staff that has responsibility for remediation.

Tests Performed: Reviewed security assessments and interviewed staff.

Test Results: The Technical Safeguards Unit conducted security assessments that included discovery enumeration, vulnerability assessments, and website assessments. Upon completion of the assessments, the Technical Safeguards Unit made available to the appropriate staff the assessment results.

During calendar year 2009, the Technical Safeguards Unit focused on website vulnerabilities and high risk vulnerabilities. The Technical Safeguards Unit worked with Department and agency personnel to rectify the high risk vulnerabilities.

According to the assessment status report, the Department was still in the process of remediating identified risks, including some dating back to calendar year 2007.

Although a framework for conducting security assessment existed, according to assessment status reports, the Department was still in the process of remediating identified risks, including some dating back to 2007.

Department's Description of Control: Cyber security incident procedures exist and responses are addressed by Department's Technical Safeguards unit.

Tests Performed: Reviewed cyber security incident procedures, CIRT events and interviewed staff.

Test Results: The Department developed the Critical Incident Response Procedure, dated March 12, 2009. The Procedures outlined the flow of the investigation, along with the requirements for notification of the various parties. The Procedures documents the severity level of an incident; one through five, with five being the most critical.

The Procedure required a Critical Incident Response Team (CIRT) incident report to be completed for each incident.

We reviewed five CIRT events, noting each had an incident report completed.

No significant exception noted.

Department's Description of Control: Security authorization lists are routinely updated and reviewed on a bi-annual basis with the user agencies.

Tests Performed: Reviewed memorandums, agency updates, and interviewed staff.

Test Results: Bi-annually the Department staff made requests to agencies to update the security authorization listings. The Department requested agencies to update the authorization listings in June 2009 and March 2010.

No significant exception noted.

Department's Description of Control: Security alerts involving critical patches, vulnerabilities and new threats are routinely received via MS-ISAC Alerts and MS Patch Tuesday Alerts. This information is evaluated by the Technical Safeguards unit. If the information received warrants attention, the pertinent information is provided to necessary BCCS personnel for action. This is done to prevent security breaches and incidents.

Tests Performed: Reviewed security communications and interviewed staff.

Test Results: The Department's Technical Safeguards unit received security alerts via MS-ISAC and MS Patch Tuesday alerts. The alerts were sent to Department personnel, state webmasters and state ISAC members.

No significant exception noted.

Department's Description of Control: The ESR process for provisioning access is used to control user access to resources.

Tests Performed: Reviewed IT MAC Request Matrix, IT MAC Process Flow, and interviewed staff.

Test Results: The Department and some consolidated agencies utilized the ESR process within Remedy for requesting user access to resources. However, we noted two consolidated agencies which had the ability to bypass the ESR process and establish access for their employees. See the Communications Solution center Control for additional information.

Additionally, the agency security software coordinators were responsible for granting mainframe access rights to their agency employees.

Although a process for the provisioning of access had been developed, the process was not utilized by all agencies.

Background Provided by the Department: The following additional controls apply to Department staff members.

Department's Description of Control: Security Awareness Training – Security awareness training is provided on an annual basis to CMS employees (both State employees and contractors) via a third party (Webstart). The presentation is currently tailored general security topics, with increased specificity and details as the training program progresses. The training is designed to raise the general understanding of computer security within the BCCS community.

Tests Performed: Reviewed security awareness training presentation and participant listing.

Test Results: The Department developed a security awareness training presentation which documented general security topics.

During our review, we selected 25 Department employees to determine if they had completed the security awareness training, noting no exceptions.

No significant exception noted.

Department's Description of Control: Compliance Acknowledgement Forms - Whenever new security policies are approved and distributed, the recipients must sign an acknowledgement form indicating that they have received and read the policy.

Tests Performed: Reviewed compliance acknowledgement forms and policies.

Test Results: In October 2009, the Department issued two new policies; the Mobile Device Policy and the IT Recovery Policy.

We reviewed the compliance acknowledgment forms for 25 Department employees, noting each had completed a form.

No significant exception noted.

Department's Description of Control: RACF violations for BCCS staff are reviewed on an ongoing basis. Violation reports are provided to the individual responsible, requesting an explanation of the violation. These explanations are then reviewed for reasonableness.

Tests Performed: Reviewed violation reports, procedures, and interviewed staff.

Test Results: The Department had a procedure in place for the monitoring of security violations.

Department staff ran violation reports daily and each violation was to be reviewed and addressed.

We noted the Department ran the violation report for December 4, 2009; however, there was no indication of the request, receipt, or review of violations expectations as outlined in the Description of Control.

Although the Department ran RACF violation reports, there was no indication of review or follow-up.

Department's Description of Control: 90 day Stale RACF account report – This report is run on a regular basis to locate RACF Ids that have not been used within 90 days and may need to be removed. The list is generated and then reviewed by individuals within BCCS. Any Ids noted for deletion are revoked.

Tests Performed: Reviewed the 90 day stale RACF report and interviewed staff.

Test Results: The Department periodically generated a report indicating the RACF accounts which had not been utilized for 90 days or more. The report was disseminated to data owners; however, data owners did not normally request that any IDs be disabled.

No significant exception noted.

Department's Description of Control: 90 day Stale AD account report. This report is run from the Control Compliance Suite (CCS) and is currently being to monitor stale AD accounts within CMS. This list is reviewed by ISD and used for AD cleanup.

Tests Performed: Reviewed the 90 day stale AD account report and interviewed staff.

Test Results: The Department generated the stale AD account report once for the audit period. Information regarding stale accounts were submitted to agencies.

No significant exception noted.

OVERALL CONCLUSION

Although the Department has developed policies and procedures designed to provide an overall security strategy and framework, all provisions have not been effectively developed or implemented.

It is incumbent upon the Department to ensure mechanisms have been developed to effectively implement, monitor, audit, track, and validate compliance with the policies and procedures both internally and for user agencies.

To promote compliance with the policies and procedures throughout State Government, the Department should ensure it is complying with all necessary provisions in its own environment.

Specifically, the Department should:

- Develop a process to ensure implementation of appropriate policies and procedures internally.
- Develop a process to promote communication to and implementation of appropriate policies and procedures at user agencies.
- Complete the risk assessment as outlined the Risk Management Framework to ensure adequate security controls are implemented, and to determine compliance with any applicable federal, state, or other requirements.
- Ensure the timely remediation of security vulnerabilities and issued classified as high risk.
- Review requirements outlined in all security documents to ensure they meet Department needs.
- Analyze all current security projects and determine the priority for completion and update deadlines as appropriate.
- Ensure the RACF violation reports are reviewed and properly analyzed as outlined the Description of Control.

PHYSICAL SECURITY

EXISTING ENVIRONMENT

Background Provided by the Department: Two primary facilities are used to conduct computer operations for the State; the Central Computer Facility (CCF) and the Communications Building.

Physical Security controls at the Central Computer Facility and the Communications Building in Springfield include:

- Security guards;
- Video cameras strategically located inside and outside the buildings;
- Proximity card readers; and
- Real property keys.

Department's Description of Control: Security guard services are contracted and the buildings are staffed with 24/7 security guard protection. Fundamental activities of security guards include but may not be limited to access control, incident reporting, and perimeter patrol.

Tests Performed: Reviewed contract, General Orders, security guard reports, and interviewed staff.

Test Results: Effective September 25, 2009, the Department entered into a contract with a security firm to provide security guard services to select facilities, including the CCF and Communications Buildings. The contract was valid through June 30, 2012. The contract required at least one guard be on duty 24/7 at both buildings and outlined security guard duties and responsibilities associated with patrolling, incident response/reporting, and access control.

To assist security guards in daily functions, the contract required the creation of General Orders and site specific Post Orders. At the time of review, General Orders, dated December 2009, had been developed and provided general guidance and responsibilities; however, site specific Post Orders had not been developed and approved for both buildings. The security firm anticipated completion of the Post Orders by April 2010.

Based on observations and review of reports, the CCF and Communications Buildings were protected by security guards 24/7. Security guards were documenting activity noted during their shift, patrolling the interior and exterior of the facilities, and assisting in controlling access to the buildings.

No significant exception noted; however, site specific Post Orders had not been developed.

Department's Description of Control: Security guard services and requirements are outlined in the following:

- Special instructions - are instructions that are communicated via email to the security guards on duty and then included in the Pass Down Book for future review and reference.

Tests Performed: Reviewed Pass Down Books.

Test Results: The security guard's Pass Down Books at the CCF and Communications Buildings contained special instructions and reminders; however, the CCF Book was last updated on September 25, 2009 and the Communication Building Book had only two entries after August 2006.

The Pass Down Books had not been routinely updated to ensure security instructions were effectively communicated.

Department's Description of Control: Security Guards issue temporary badges (with limited access rights) to visitors, and to employees who forget their assigned access card. Those issued a temporary badge must sign the Building Admittance Register recording their name and badge number. Security Guards have been instructed to inventory temporary badges at the start of each shift to ensure accountability.

Tests Performed: Reviewed temporary badges, Badge Inventory sheets, Building Admittance Registers, H/V System, and interviewed staff.

Test Results: The Department maintained temporary badges with varying levels of access privileges; 13 types of badges for the CCF and 12 types of badges for the Communications Building. Depending on the type of access rights previously defined within the Hirsch Velocity (H/V) System for the individual, security guards issued the appropriate temporary badge. A visitor (V) badge, which contained no access rights, was maintained for both buildings.

Individuals receiving a temporary badge were required to sign the Building Admittance Register prior to receiving a temporary badge from the security guard. We reviewed the Building Admittance Registers for the first week of December 2009, noting the registers contained name and badge number for each entry.

Additionally, for the same week in December 2009, we selected 30 individual issued temporary badges at the CCF and 25 individuals issued temporary badges at the Communications Building and compared them to the access privilege defined in the H/V System, noting all appeared to have been issued the appropriate badge.

Security guards were to inventory temporary badges at the start of each shift and document the results on the respective buildings Badge Inventory sheets. We reviewed the Badge Inventory sheets for one week in December 2009, noting the sheets were being completed and no significant exceptions were noted regarding missing badges.

No significant exception noted.

Department's Description of Control: Networked video cameras monitor exterior doors and sensitive interior entrances. Security Guards as well as the Bureau Physical Security Coordinator have remote view capability for all networked cameras.

Tests Performed: Inspected buildings and interviewed staff.

Test Results: Video cameras were strategically placed throughout the interior and surrounding the exterior of both the CCF and Communications Buildings. Video feeds were monitored at a console located at the security guard desks. We viewed the digital video feeds, noting cameras were generally positioned to allow for clear unobstructed views and images were generally clear.

In addition, since the system was connected to both the CCF and Communications Buildings, security guards at each facility had the ability to review cameras at their facility and the other facility. The Physical Security Coordinator also had the capability to remotely view the cameras.

Video was saved to a Network Video Recorder located in the CCF Data Center.

No significant exception noted.

Department's Description of Control: Proximity card readers that require authorized access cards are located throughout the interior and exterior of the buildings to control and restrict access.

Tests Performed: Inspected buildings and interviewed staff.

Test Results: The H/V System was utilized to control and restrict access to the CCF and Communications Buildings. Proximity card readers were installed on the building's exterior doors and strategically throughout the interior of each building.

In addition to other sensitive areas, at the CCF, the H/V System controlled and restricted access to the Data Center hosting the Tape Library, tape cleaning room, Systems Operations Center, PKI room, and telecommunications room.

In addition to other sensitive areas, at the Communications Building, the H/V System controlled and restricted access to the ICN network room, server and telecommunications rooms, and NCC/Technical Safeguards lab.

No significant exception noted.

Department's Description of Control: Access cards are issued to Department personnel based on business need and job responsibility. The Bureau Physical Security Coordinator processes emailed access requests from designated authorities as identified in the Approval Authorization Matrix and Badge Production Matrix. The H/V System Administrator's Manual contains instructions to create the physical access card.

Tests Performed: Reviewed policies and procedures.

Test Results: We requested the Approval Authorization Matrix and the Badge Production Matrix and were provided CMS Identification Badge, Access Codes and Facility Key (Issuance Policy) and a Badge Information (Document), respectively.

Upon review, we noted the actual process used to assign and approve access cards differed from the processes outlined in the Description of Control and the documents provided.

In addition to the information provided in the Description of Control and the documents provided, we noted the following documents also contained procedures regarding the creation, modification, and revocation of access cards:

- Statewide CMS/BCCS Facility Access Policy,
- Access Internal Policy, and
- Revocation Internal Policy.

See Security Administration control for additional information regarding the additional policies and procedures for the processing of access cards and associated access privileges, as well as testing of new access cards.

The H/V System Administrator's Manual contained instructions to create the physical access card.

Although processes existed, we found several differing policies and procedures for the granting and revocation of physical access rights.

Department's Description of Control: The H/V system records and logs the use of access cards. Reports can be produced to list who has access to what buildings and locations. In addition, audit trail reports that outline the use (time and location) of access cards can be produced.

Tests Performed: Review of H/V Administrator's Guide and interviewed staff.

Test Results: The H/V System had the capabilities to create various reports. Reporting capabilities included, but were not limited to, reports showing location and time an access card was utilized, as well as who had access to the building and various locations within the building.

Reports were not generated on a routine scheduled basis; however, reports were generated as needed and per management request.

No significant exception noted.

Department's Description of Control: Absentee limits and restrictions on employee pass-back are activated to help control physical access to buildings.

Tests Performed: Reviewed policies and procedures, H/V System, inspected buildings, and interviewed staff.

Test Results: The CMS Identification Badge, Access, Codes and Facility Keys Issuance Policy outlined the requirements for access cards to be set with an absentee limit with exceptions approved on a case by case basis. We reviewed the H/V System, noting absentee limits were established to disable access cards after a period of inactivity.

In addition, upon review of the H/V System and observations of staff, we noted the Department had implemented pass-back technology to help prevent individuals from following ("piggy backing") others into the CCF and Communications Buildings.

No significant exception noted.

Department's Description of Control: Access cards are FIPS 201-1 compliant and contain text that outlines cardholder responsibilities as well as instructions on what to do if a lost badge is found.

Tests Performed: Reviewed access cards, FIPS 201-1, and interviewed staff.

Test Results: FIPS 201-1 required the front of the access to card include a photograph, name, employee affiliation, organizational affiliation, and an expiration date. Upon review of access card and comparison against FIPS 201-1, we noted all of the required features for the front of the access card were included. However, the back of the card did not contain either the Issuer Identification or the Agency Card Serial Number as required by FIPS 201-1.

However, we noted the back of the access card outlined the cardholder responsibilities as well as instructions on what to do if a lost badge was found.

No significant exception noted; however, access cards were not compliant with all of the FIPS 201-1 requirements.

Department's Description of Control: Once the Physical Security Coordinator is notified of employee separation or other circumstance for disabling access, card access is disabled.

An additional control beyond disabling separated employee's access card, the direct supervisor is supposed to collect the employee's access card as outlined in the Department's Policy Manual.

Tests Performed: Reviewed policies and procedures, departed employee and contractor listings, access listings, H/V System, exit checklists, and interviewed staff.

Test Results: According to the Department's Policy Manual -- Employee Separation, Chapter 2; Section 13, dated September 1, 1998, "All State owned items must be returned to the State when an employee separates service with the Department." Additionally, "Supervisors are responsible for collecting a separated employee's telephone credit cards, door and desk keys, parking lot stickers, Data Center admittance cards, identification cards, vehicles and special equipment."

In addition to the Department's Policy Manual, we noted the existence of the following additional procedures addressing separated employees:

- CMS Identification Badge, Access Codes, and Facility Keys Issuance Policy,
- Statewide CMS/BCCS Facility Access Policy, and
- Revocation Internal Policy.

See Security Administration control for additional information regarding the additional policies and procedures.

During our review of access to secure areas within the CCF and Communications Buildings, we noted that access for departed individuals (employees and contractors) generally appeared to be disabled. However, the processes utilized and those outlined in related policies and procedures, such as collecting badges, did not appear to be consistent, repeatable, or followed. See Security Administration control for information regarding revocation of badges.

The Department stated, since all access cards contained an expiration date and were set with an absentee limit, the Department did not believe it was necessary to review the H/V System for inactive accounts.

The Department had procedures in place regarding disabling access cards; however, associated policies related to departure were not generally followed.

Department's Description of Control: The Bureau of Property Management (BoPM) is responsible for issuing and maintaining real property keys.

Tests Performed: Reviewed key logs, departed employee listings, toured buildings, and interviewed staff.

Test Results: BoPM was responsible for issuing and maintaining real property keys. Keys were issued to individuals upon supervisory request, via email or conversation with appropriate BoPM staff. A key log was maintained to tracks keys as they were issued.

BoPM staff was also on the distribution listing for notification when an employee departed or transferred. Once notification was received, BoPM would check the key inventory to see if the individual was issued a key.

Upon review of real property key listings for the CCF and Communications Buildings we identified deficiencies in the tracking and maintaining of real property keys for the Department. Key inventories for the Communications and CCF Buildings did not accurately identify who had been assigned real property keys. In fact, at least seven master keys (which provided unlimited access to a facility) were unaccounted for.

Upon bringing the issue to the attention of the Department, the Department could not confirm, and provide evidence all grandmaster keys identified had been collected. As a result, the Department started a project to begin reconciling key inventories.

Procedures to effectively track and maintain real property keys at all buildings had not been implemented.

Department's Description of Control: Preventative protection against environmental factors at the CCF and Communications facilities include fire suppression and detection systems. Fire suppression and detection systems on the third floor of the Central Computer Facility and at the Communications Building are installed and tested on a regular basis.

Tests Performed: Reviewed contracts, inspection reports, inspected buildings, and interviewed staff.

Test Results: The Department maintained preventative maintenance and inspections contracts for the fire detection and suppression systems located in the CCF; however, at the time of our review a contract was not in place for the systems at the Communications Building. The Department anticipated having a preventative maintenance and inspection contract in place for the Communications Building by May 2010.

The CCF third floor computer room contained fire suppression and detection systems that were Underwriter Laboratory approved and utilized an environmentally friendly gaseous agent, FM-200. Upon review, we noted the system was last inspected in February 2010.

The Communications Building contained a fire detection and suppression system throughout the entire facility. Upon review, we noted the system was last inspected in November 2009.

Additionally, we noted the fire extinguishers for both facilities were inspected during FY10.

No significant exception noted; however, a preventative maintenance and inspection contract was not in place for the Communications Building's fire detection and suppression systems.

Department's Description of Control: To mitigate the risk of a power failure, the Central Computer Facility is supplied by two different sources and is equipped with an uninterruptible power supply (UPS). Within an allotted time the Department's generators will engage. The Department has a service contract for the UPS to provide routine preventive maintenance and remedial services as required.

Tests Performed: Reviewed contracts, inspection reports, and interviewed staff.

Test Results: To provide a sufficient supply of electricity, City Water Light and Power (CWLP) provided two electrical feeds to the CCF. In the event of power failure, the UPS would engage immediately drawing power from the battery farm and the generators.

The Department maintained preventative maintenance contracts for routine inspection and maintenance of the CCF UPS. Upon review of inspection reports, we noted some repair work was performed in Fall of 2009; however, no significant problems were identified.

Although the Communications Building was equipped with a UPS, at the time of our review, a preventative maintenance contract was not in place for routine inspection and maintenance.

However, per BoPM staff, the generator was started every Monday to ensure it functioned appropriately.

No significant exception noted; however, a preventative maintenance contract was not in place for the Communications Building UPS.

Department's Description of Control: The H/V system control panels have their own UPS to provide power to the control panels, and the access control devices they support. A separate UPS module supplies uninterruptible power to certain electric locks.

Tests Performed: Inspected control panels and interviewed staff.

Test Results: The UPS for the H/V System was the batteries located inside the control panels. An automated system monitored the batteries and if there was a problem, the system notified the Physical Security Coordinator and the building's security guard desk. In addition to the batteries located inside the control panels, the control panels were connected to the building's UPS systems to provide a second backup power supply.

No significant exception noted.

Background Provided by the Department: Two other facilities are also used to conduct computer-related operations for the Department; the Harris Facility and the Clinton Facility.

Department's Description of Control: Physical security controls protecting the Department's assets housed at the Harris Facility include:

- Security guards in the front entry way;
- Video cameras strategically located inside and outside the building;
- Proximity card readers requiring an active Access Card to allow entry; and
- Limited access, brightly colored badges for use by individuals entering the building to pick up printed output from the I/O Control areas.

Tests Performed: Reviewed departed employee and contractor listing, access listing, and interviewed staff.

Test Results: The Harris Facility computer room was located within a building occupied by the Department of Human Service (DHS). During our review, we found the following physical security controls were established to safeguard the Harris Facility:

- Security guards were on duty 24 hours a day, 7 days a week.
- Multiple video cameras were located inside and outside the building to provide viewable images for security guards. The surveillance system was upgraded and equipped with 16 video surveillance cameras strategically located inside and outside the facility, all of which were viewable by security guards. In addition, the video images are now recorded electronically onto a Network Video Recorder.
- Proximity card readers required an active access card for entry to restricted areas and were located throughout the facility.

- Brightly colored badges with limited access for use by individuals entering the building to pick up printed output from the I/O Control area were utilized.

No significant exception noted; however, since physical security of the Harris Facility was a shared responsibility between the Department and the Department of Human Services, we recommend the Department continue working with DHS to ensure access to restricted areas is adequately secured and restricted to authorized personnel.

Department's Description of Control: Physical security control protecting the Department's assets at the Clinton Facility include:

- Security guards during business hours.
- Cipher locks.

Tests Performed: Toured facility and interviewed staff.

Test Results: The Clinton facility was shared between the Department of Human Services, Department of Healthcare and Family Services, and the Department.

The entrance to the building was unlocked from 7:00am to 6:00pm. All employees were provided with an employee badge to permit access to the facility. A security guard monitored the entrance to the facility from 6:00am to 10:00pm. The guard verified that employees were displaying their badge and required that visitors signed-in and were escorted by an employee. A second guard patrolled the facility from 9:00am to 5:30pm.

After 6:00pm and until 7:00am the next morning, the facility was locked with Cipher locks. The facility was also equipped with an alarm system.

The facility was equipped with external and internal cameras that were monitored at the guard's desk. All cameras, with the exception of the loading dock cameras were functional at the time of review; however, the loading dock entrance was secured at all times and was equipped with an intercom system.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls (with the exception of the process of controlling real-property keys) were operating with sufficient effectiveness to achieve the control objective.

To enhance controls, the Department should:

- Review all policies and procedures associated with granting, modifying and revoking physical access rights, as well as the collection of access cards and assignment and collection of real property keys. Specifically, the Department should:
    - Ensure proper accounting for real-property keys, in particular master keys.
    - Develop a mechanism to locate and account for all master keys currently unaccounted for.
    - Ensure policies and procedures provide for a consistent, repeatable, and timely process.
    - Ensure the defined process aligns with management's intentions and are in the best interest of all parties involved.
    - Ensure the defined process includes routinely reviewing the appropriateness of individual's access rights and keys assigned.
    - Ensure the defined process includes procedures specific to contractors and their assigned access rights and keys.
    - Ensure the defined process outlines documentation necessary to provide for an adequate audit trail.
    - Ensure policies and procedures are approved and distributed to all appropriate individuals.
- Ensure information to assist in the performance of security guard duties is available and current.
- Ensure preventative maintenance and inspection contracts are maintained for the Communications Buildings Fire detection and suppression and UPS systems.
- Review the requirement for access cards to be FIPS 201-1 compliant. If necessary, ensure all access cards contain the minimum required elements on the front and back of the access cards.

Additionally, since physical security of the Harris Facility is a shared responsibility between the Department and the Department of Human Services, we recommend the Department continue working with DHS to ensure access to restricted areas is adequately secured and restricted to authorized personnel.

OPERATIONS - SYSTEM OPERATION CENTER

Department Description of Control: All procedures utilized by the Systems Operations Center (SOC) are documented in a central location called the D.P. Guide which resides on the groups SharePoint site as well as one hardcopy that is maintained in the event that the SharePoint site is unreachable.

Tests Performed: Reviewed the Data Processing (DP) Guide and interviewed staff.

Test Results: The Department maintained the DP Guide, each section dated separately, which contained information for commands, problems, troubleshooting, changes, and a description on how to take the mainframe systems down and bring them back up. The DP Guide was available on the Sharepoint site and a hardcopy was located in the System Operations Center.

No significant exception noted.

Department Description of Control: The Department monitors the IT infrastructure and related events utilizing:

- Mainframe consoles for each of the mainframe systems to monitor all jobs; job performance; tape processing; system utilization, etc.
- AOC – Automated Operations Control to monitor all teleprocessing and system tasks on all mainframe systems which are routed through the Focal Point so that the SOC has access to the information in a centralized location which can be accessed from all workstations in the SOC.
- HMC – Hardware Management Console for monitoring and maintenance of mainframe-attached hardware components.
- Tivoli – which monitors all network activity.
- What's Up Gold – which monitors all routers, servers and server applications.

Tests Performed: Reviewed DP Guide, visually reviewed tools, and interviewed staff.

Test Results: The Department utilized several tools to monitor the IT infrastructure and related events: Mainframe consoles, AOC, HMC, Tivoli, and What's Up Gold.

These monitoring systems were visually monitored by the Operations Center Staff 24 hours a day, 7 days a week.

The DP Guide provided staff guidance on the proper response to specific events.

No significant exception noted.

Department Description of Control: Daily Shift Report is populated by the Systems Operations Center recording any outages and issues which occur during the course of each day. This is then distributed via an automated mechanism in the Focal application.

Tests Performed: Reviewed Daily Shift Reports, Remedy tickets, and interviewed staff.

Test Results: The Daily Shift Reports recorded all activities which occurred (downtime, person contacted, action taken, etc) on each shift.

We reviewed Daily Shift Reports for October 12-19, 2009, noting they appeared to be completed appropriately. Additionally, we reviewed 25 problems indicated in the reports, noting they had a corresponding Remedy ticket.

The Daily Shift Reports were distributed via the Focal application to anyone requesting the applicable information.

No significant exception noted.

Department Description of Control: Shift Change Checklists are completed at the beginning of each shift in Systems Operations Center to ensure that all systems are running as designed.

Tests Performed: Reviewed the Shift Change Checklists and interviewed staff.

Test Results: Shift Change Checklists were utilized to aid in reviewing the status of the various operating systems and applications. The Shift Change Checklists were also utilized to determine if there were problems with systems or applications. We reviewed the Shift Change Checklists from October12-19, 2009, noting all had supervisory review and appeared to be appropriately completed.

No significant exception noted.

Department Description of Control: The Department is continuously monitored and assessed to meet the goals of the Department utilizing:

- SYSLOG – maintains logs of all activity on each of the mainframe systems.
- Automation Logging which monitors Job and System Task Maintenance on the mainframe systems.

Tests Performed: Interviewed staff.

Test Results: The SYSLOG recorded all messages written to, and all commands entered into the system console. The main use of the system generated log was for the historical value in reviewing problems or questions as to what did or did not occur and what commands were entered in response to prompts for action to be taken.

The Automation Logging recorded teleprocess, system operations and when systems were shut down and brought back up.

No significant exception noted.

Department Description of Control: The Remedy Change Management System is utilized to coordinate and implement changes.

Tests Performed: Reviewed Remedy Change Management Guide and interviewed staff.

Test Results: The Remedy Change Management module was utilized to record changes to the system. The Systems Operations Center staff members were not responsible for origination of tickets, rather completion of tasks assigned to them.

For additional information, see the Change Control review.

No significant exception noted.

Department Description of Control: Remedy is utilized to record and monitor incident resolution.

Tests Performed: Reviewed Remedy Change Management Guide and interviewed staff.

Test Results: The Remedy Help Desk module was utilized to record and monitor incident resolution. The type of problem, the description of the problem and the category, type and item was documented. The Systems Operation Center staff assigned the incident to a group and then the assigned group would be responsible for completion of the ticket.

For detailed testing of Remedy Help Desk tickets see the Customer Management Center control.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

OPERATIONS – INPUT/OUTPUT CONTROL

EXISTING ENVIRONMENT

Background Provided by the Department: The Input Control monitors all production jobs, while Output Control is responsible for printing and distribution of all documents and reports generated.

Department Description of Control: Jobs processed in the production environment run through CA-Scheduler or are manually submitted. Emails are sent in requesting specific jobs to be run.

Tests Performed: Reviewed emails and interviewed staff.

Test Results: Production Control monitored processing activities for the Department, DHS, IDOT, EPA, DHFS and DPH. Approved schedules were submitted through CA-Scheduler or manually for the Department, DHS, IDOT, EPA, and DPH. Manually submitted jobs were only accepted from authorized supervisors or managers of the agencies.

Agencies submitted manual job requests via email. However, we noted Production Control did not maintain a listing of individuals who were authorized to submit such requests. Production Control staff stated they knew who was authorized based on prior experience.

No significant exception noted; however, the Department relied on staff experience and did not maintain a listing to verify if requestors were authorized to submit manual job requests.

Department Description of Control: Security software ensures only authorized individuals are allowed to submit requests.

Tests Performed: Reviewed CA-Scheduler and interviewed staff.

Test Results: Security software was used to restrict the ability to submit production jobs through CA-Scheduler to authorized staff. The assignment of access rights to control an agency's job submissions was controlled by that agency's security software coordinator.

No significant exception noted.

Department Description of Control: The Department utilizes legacy policy and procedures to monitor jobs.

Tests Performed: Interviewed staff.

Test Results: The Department stated comprehensive and standardized policies and procedures had not been developed, and the Department followed individual agency legacy policies and procedures to monitor jobs. However, staff had been and continued to be cross trained in the agency legacy processes.

No significant exception noted; however, standardized policies and procedures had not been developed.

Department Description of Control: The daily shift reports document the abends. Agency contact information, when the job was corrected and the cause are reported. I/O daily shift reports which contain abends are emailed to the applicable agency.

Tests Performed: Reviewed daily shift reports and interviewed staff.

Test Results: Documentation for abends was recorded in the daily shift reports, which contained information on agency contacts, when the job was corrected, and the cause of the abend.

The Department, DHS, DHFS, IDOT, DPH, and EPA generally had the procedures to fix abends identified within the job. If the abend resolution was not identified in the warning, Production Control staff contacted the agency to obtain information to assist in problem resolution.

We reviewed the daily shift reports for the week of December 1, 2009, noting the reports contained information for abends and the corrective action taken.

The email notifications of the daily shift reports were not maintained; however, the daily shift reports were maintained on a Sharepoint site for retention purposes.

No significant exception noted.

Department Description of Control: The Department maintains a Job Call List for agency contacts.

Tests Performed: Viewed Job Call List and interviewed staff.

Test Results: A Job Call List was maintained to provide agency contact information. This list was updated by the user agencies.

No significant exception noted.

Department Description of Control: All reports are printed in a secure environment and depending on the requirements for privacy, HIPPA, personal information, financial information, they are either packaged and properly labeled prior to being sent out.

Tests Performed: Reviewed distribution checklist, Focal application, and interviewed staff.

Test Results: Reports were printed at the Department of Human Services, Harris Facility. See the Physical Security control for a review of the Harris Facility.

It was the agencies' responsibility to identify privacy requirements for reports and define the appropriate packaging and labeling prior to I/O Control distributing the reports.

Jobs that ran through the Output control were monitored by the I/O Control staff. When a report was printed it was placed in the agency labeled box. When an individual came to pick up a report they would need to show their drivers license. The Focal application was checked to determine if the individual was authorized to pick up a report.

When reports were to be mailed, they were packaged based on agency specification. This included sealed boxes or envelopes. The recipient of the mailings was determined by the banner page on the report which was set up by the agency.

We compared the distribution checklist for the week of October 12, 2009, to the listing of authorized individuals in the Focal application, noting no exceptions.

No significant exception noted.

Department Description of Control: Memorandums document the security controls for the distribution of reports.

Tests Performed: Reviewed memorandums.

Test Results: The Department distributed a memorandum to I/O managed agencies in November 2006 outlining the security controls for the distribution of reports. In April 2009, the Department issued a memorandum to its Fiscal Cash Management division outlining the security controls.

No significant exception; however, the Department last distributed a memorandum to I/O managed agencies in November 2006.

Department Description of Control: The Focal System contains a listing of individuals authorized to pick up reports.

Tests Performed: Reviewed sign-out sheets for the pick up of reports and Focal application.

Test Results: The Focal application contained a listing of individuals authorized to pick up reports. The Focal application was updated on a bi-annual basis by the Security and Compliance division and on an as needed basis by request of the user agency.

We reviewed the report distribution checkout list for the week of October 12, 2009 to determine if only authorized individuals picked up reports, noting no exceptions.

No significant exception noted.

Department Description of Control: If the reports and documents are handled by our automated distribution software they are protected by security software.

Tests Performed: Reviewed emails and interviewed staff.

Test Results: Security software restricted the ability to view or print reports to authorized staff. The authorization of access rights to view and print an agency's reports was the responsibility of each agency. After a valid authorization was received from an agency, Production Control staff applied the updated access rights.

Production Control changed access rights in the automated distribution software for an employee when an agency sent an email requesting a change in access rights. The emails included the security software ID of the employee, the report (if applicable) to be utilized and the action to be taken (access/removal for reports). The emails were to be sent from the manager/supervisor of the employee or have the manager/supervisor cc'd on the email. Production Control did not keep a list of managers/supervisors that were authorized to submit requests for changes in access rights in the automated distribution software.

No significant exception noted; however, the Department relied on staff experience and did not maintain a listing to verify if requestors were authorized to request changes to access rights to view or print reports.

Department Description of Control: Legacy policies and procedures are utilized for printing and distribution.

Tests Performed: Interviewed staff.

Test Results: The Department stated comprehensive and standardized policies and procedures had not been developed, and the Department used individual agency legacy policies and procedures to print and distribute documents. However, staff had been cross trained in the legacy processes.

No significant exception noted; however, standardized policies and procedures had not been developed.

Department Description of Control: Monthly job performance reports are produced and submitted to management for review.

Tests Performed: Reviewed monthly job performance reports and interviewed staff.

Test Results: The monthly reports contained information regarding printer meter readings for the Department, DHS, DHFS, and Comptroller printers.

During our review, we noted the October 2009 monthly job performance report documented downtime, printer status, and performance information.

The EPOS Manager reviewed these reports and also used performance information for inclusion in monthly billing and metrics reporting.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls that we were able to test were operating with sufficient effectiveness to achieve the control objective.

To strengthen the controls, we recommend the Department:

- Develop standardized Input and Output policies and procedures for use by all consolidated agencies.
- Develop a list of authorized individuals to submit jobs via email to ensure only authorized individuals are submitting requests for jobs, including a process or procedure that regularly reviews and updates the listing.
- Develop a list of authorized individuals that submit access rights requests for the automated distribution software to ensure only authorized individuals were able to request changes to access rights to view or print reports.
- At least annually distribute a memorandum to I/O managed agencies outlining the security control for the distribution of reports.

OPERATIONS – PRODUCTION CONTROL

EXISTING ENVIRONMENT

Background Provided by the Department: Production Control ensures the production processing activities are documented and executed in accordance with approved schedules.

Department Description of Control: Jobs processed in the production environment run through CA-Scheduler or are manually submitted.

Tests Performed: Reviewed emails and interviewed staff.

Test Results: Production Control monitored processing activities for the Department, DHS, DOT, EPA, DHFS and DPH. Approved schedules were submitted through CA-Scheduler or manually for the Department, DHS, DOT, EPA, and DPH. Manually submitted jobs were only accepted from authorized supervisors or managers of the agencies.

Agencies submitted manual job requests via email. However, we noted Production Control did not maintain a listing of individuals who were authorized to submit such requests. Production Control staff stated they knew who was authorized based on prior experience.

No significant exception noted; however, the Department relied on staff experience and did not maintain a listing to verify if requestors were authorized to submit manual job requests.

Department Description of Control: Security software ensures only authorized individuals are allowed to submit requests.

Tests Performed: Reviewed CA-Scheduler and interviewed staff.

Test Results: Security software was used to restrict the ability to submit production jobs through CA-Scheduler to authorized staff. The assignment of access rights to control an agency’s job submissions was controlled by that agency’s security software coordinator.

No significant exception noted.

Department Description of Control: Production Control reviews and monitors all processes and procedures to ensure they follow documented standards for each legacy agency.

Tests Performed: Reviewed Proc Acceptance Forms and interviewed staff.

Test Results: Production Control reviewed and monitored processing activities for the Department and the following agencies: DHS, DOT, EPA, HFS and DPH.

Standards manuals existed on a Sharepoint site, along with a hardcopy in the Production Control area for the Department, DOT, and DHS. Additionally, hardcopy standards manuals were maintained in the Production Control area for EPA and DPH.

Department staff stated comprehensive and standardized production control policies and procedures had not been developed, and the Department followed individual agency legacy policies and procedures.

When the Department, DHS, or DHFS' application unit submitted a new job or a change to an existing job, a Proc Acceptance Form was submitted. This Form included all signatures required before Production Control would make any changes or set up a new job.

We reviewed 25 Proc Acceptance Forms, noting no exceptions.

No significant exception noted; however, standardized production control policies and procedures had not been developed.

Department Description of Control: The daily shift reports document the abends. Agency contact information, when the job was corrected and the cause are reported.

Tests Performed: Reviewed daily shift reports and interviewed staff.

Test Results: Documentation for abends was recorded in the daily shift reports, which contained information on agency contacts, when the job was corrected, and the cause of the abend.

The Department, DHS, DHFS, DOT, DPH, and EPA generally had the procedures to fix abends identified within the job. If the abend resolution was not identified in the warning, Production Control staff contacted the agency to obtain information to assist in problem resolution.

We reviewed the daily shift reports for the week of December 1, 2009, noting the reports contained information for abends and the corrective action taken.

No significant exception noted.

Department Description of Control: All reports are printed in a secure environment and depending on the requirements for privacy, HIPPA, personal information, financial information, they are either packaged and properly labeled prior to being sent out.

Tests Performed: Reviewed distribution checklist, Focal application, and interviewed staff.

Test Results: Reports were printed at the Department of Human Services, Harris Facility. See the Physical Security control for a review of the Harris Facility.

It was the agencies' responsibility to identify privacy requirements for reports and define the appropriate packaging and labeling prior to I/O Control distributing the reports.

Jobs that ran through the Output control were monitored by the I/O Control staff. When a report was printed it was placed in the agency labeled box. When an individual came to pick up a report they would need to show their drivers license. The Focal application was checked to determine if the individual was authorized to pick up a report.

When reports were to be mailed, they were packaged based on agency specifications. This included sealed boxes or envelopes. The recipient of the mailings was determined by the banner page on the report which was set up by the agency.

We compared the distribution checklist for the week of October 12, 2009, to the listing of authorized individuals in the Focal application, noting no exceptions.

No significant exception noted.

Department Description of Control: If the reports and documents are handled by our automated distribution software they are protected by security software

Tests Performed: Reviewed emails and interviewed staff.

Test Results: Security software restricted the ability to view or print reports to authorized staff. The authorization of access rights to view and print an agency's reports was the responsibility of that agency. After a valid authorization was received from an agency, Production Control staff would apply the updated access rights.

Production Control would change access rights in the automated distribution software for an employee when an agency sent an email requesting a change in access rights. The emails included the security software ID of the employee, the report (if applicable) to be utilized and the action to be taken (access/removal for reports). The emails were to be sent from the manager/supervisor of the employee or have the manager/supervisor cc'd on the email. Production Control did not keep a list of managers/supervisors that were authorized to submit requests for changes in access rights in the automated distribution software.

No significant exception noted; however, the Department relied on staff experience and did not maintain a listing to verify if requestors were authorized to request changes to access rights to view or print reports.

OVERALL CONCLUSION

Based on the test results described above, the controls that we were able to test, were operating with sufficient effectiveness to achieve the control objective.

To strengthen the controls, we recommend the Department:

- Develop standardized production control policies and procedures for use by all consolidated agencies.
- Develop a list of individuals authorized to submit manual job requests to ensure only authorized individuals are submitting requests for jobs.
- Develop a list of individuals authorized to request updates to access rights to view or print jobs to ensure only authorized individuals are requesting changes to access rights.

OPERATIONS – LIBRARY SERVICES

EXISTING ENVIRONMENT

Background Provided by the Department: Library Services consists of four units: Tape Library, Tape Media, Library Support and Tape Administration.

Department Description of Control: The ISD Media Guide and the ISD Library Guide assist staff in their duties.

Tests Performed: Reviewed the ISD Media Guide and ISD Library Guide.

Test Results: The Department developed the ISD Media Guide, dated by section, which provided staff guidance with job duties. Specifically, the ISD Media Guide provided detailed information on the following processes:

- Monitoring tapes through the Tape Management System,
- Cleaning cartridges,
- Cartridge pull and review,
- Tape manual mounts, dismounts, and
- Service requests.

The Department had also developed the ISD Tape Library Guide, dated by section, which provided information for the step by step process in Tape Library's daily functions, including Library Services Vault Transmittal procedures.

During our review of the ISD Media and ISD Library Guides, we noted the Purpose, Authority and Owner sections were not always completed.

No significant exception noted; however, the ISD Media Guide and ISD Library Guide had some sections that were not completed.

Department Description of Control: Security software is utilized to ensure the integrity of the media.

Tests Performed: Interviewed staff.

Test Results: Access rights to media were controlled by agencies via security software.

No significant exception noted.

Department Description of Control: Automated Tape Management System retains critical tape information for specified amounts of time.

Tests Performed: Interviewed staff.

Test Results: The agencies were responsible for updating the Tape Management System (TMS) with retention periods for tapes.

No significant exception noted.

Department Description of Control: Tape Admin uses reports listing all cart information.

Tests Performed: Reviewed Tape Generation System (TGS), manually produced reports, tape listings, and interviewed staff.

Test Results: TGS and manually produced reports were used to document tape activities for the Department, DHS, DHFS, and IDOT.

The TGS and the manually produced reports pulled data from the Tape Management System. These reports were utilized to guide staff in agency requests in managing tapes or to handle any problems or issues that may arise.

We reviewed the TGS and the manually produced reports for February 18 and 19, 2010, noting the reports contained dates, report name, and appropriate detailed information regarding agency tapes.

No significant exception noted.

Department Description of Control: CCF Tape Library uses various reports for inventory which are verified twice a year.

Tests Performed: Reviewed inventory report and interviewed staff.

Test Results: The Tape Library used various reports for inventory such as the inventory listing, TMS report and Automated Cartridge System (ACS) report. The last inventory was conducted on October 6, 2009.

We reviewed the inventory documentation for October 6, 2009, noting the inventory reconciled.

No significant exception noted.

Department Description of Control: CCF Tape Library release/receipt of media done only after verification is authenticated thru Authorization list. Movement of any media is recorded with transmittal forms or printed broadcasts.

Tests Performed: Reviewed media transmittal forms, authorization list, and interviewed staff.

Test Results: Agencies were responsible for sending a request to release/receive media, which required a Media Transmittal Form or a broadcast via e-mail to the Media library staff. The forms listed the tape media volumes the agencies requested to have moved from the vault to the CCF library or vice versa.

When a transmittal form was received, the individual requesting the move was verified against the authorization list.

We reviewed 25 Media Check-In/Media Check-Out Transmittal Forms for February 26, 2010, to ensure the forms were correctly completed and to ensure individuals that picked up the media were authorized to do so by comparing the individuals who signed the forms to the authorization list, noting no exceptions.

No significant exception noted.

Department Description of Control: Library Support verify all backups (daily, weekly, and monthly) and production to test moves completed successfully. Library Support staff verify backups and moves by reviewing JCL condition codes. And resolving any problems associated to ensure successful completion.

Tests Performed: Reviewed moves to production and interviewed staff.

Test Results: Library Support conducted backups for the Department, DHS, DHFS, and IDOT. Backups were run through CA-Scheduler after hours. The next day Library Support verified the backups by looking up the job in Mobius. The staff verified the generation, volume and the JCL condition codes. This was the same process for daily, weekly, and monthly backups.

However, comprehensive and standardized policies and procedures did not exist for the verification of the backup process. Department staff generally used the individual agencies' legacy processes.

If there were problems during backups or moves to production the Library Support staff would take the appropriate action, based on experience, to resolve the problem. Since the problems were fixed as soon as possible they were not logged. Library Support staff would know that the problem was resolved because the job would finish.

The Department moved changes into production for the Department, DHS, DHFS, and IDOT. Department staff stated comprehensive and standardized policies and procedures for moves to production had not been developed. Department staff generally used the individual agencies' legacy processes.

We reviewed 75 moves to production, noting no exceptions.

No significant exception noted; however, standardized policies and procedures had not been developed to control moves to production or for verifying backups.

Department Description of Control: Tape Admin reviews cart statistical reports and assigns dedicated carts to designated individuals.

Tests Performed: Reviewed statistical reports and interviewed staff.

Test Results: The statistical reports were used as a tracking tool for cartridges (carts). Individuals were assigned carts after they emailed a request for carts. The carts were assigned based on security software ID of the individual requesting the carts.

We reviewed the statistical report for February 18, 2010 noting the report contained the following: number of production carts, copies of production carts, test carts, carts permanently assigned, scratches not available, scratch carts available, new carts added, carts on hold, carts at local vault, carts at the regional vault, carts coming from local vault, and carts going to the regional vault.

No significant exception noted.

Department Description of Control: CCF Media use consoles to monitor mainframe processing, LSM functions, and servers.

Tests Performed: Reviewed ISD Media Guide, ISD Library Guide, and interviewed staff.

Test Results: The ISD Media Guide and the ISD Library Guide provided guidance to staff regarding the monitoring of mainframe processing, Library Storage Module (LSM) functions, and servers.

The consoles were visually monitored by staff for mainframe processing, LSM functions and servers. The consoles showed messages for tape mounts, tape ejects, errors, etc.

No significant exception noted.

Department Description of Control: CCF Media/Tape Library report any LSM, server, or drive problems immediately to the SOC or designated Technical Support staff.

Tests Performed: Reviewed DP Guide and interviewed staff.

Test Results: The DP Guide provided staff guidance on reporting problems to various staff.

CCF Media/Tape Library contacted the System Operations Center for problems related to any LSM, server, or drive problem. The Systems Operation Center contacted the Technical Support staff, if applicable.

No significant exception noted.

Department Description of Control: Library Support complete and verify mainframe library maintenance when requested.

Tests Performed: Interviewed staff.

Test Results: The types of mainframe maintenance that Library Support completed were copying, backups, restores, rebuilding, deletions, reloads and renaming. The maintenance was mostly included within a move to production.

No significant exception noted.

Department Description of Control: Production libraries are protected by security software to allow only authorized moves.

Tests Performed: Reviewed move to production forms.

Test Results: Production libraries were protected by security software. See the Zero Downtime Operating System control for more detail.

The Department was responsible for select mainframe production libraries of the Department, DHS, DHFS, and IDOT. The Department was not responsible for other agency moves to production.

We reviewed 75 moves to productions that were performed by Library Support for specific production libraries to ensure appropriate approvals and authorizations were provided prior to the move of the changes into production, noting no exceptions.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. However, to enhance the Department's controls, the Department should:

- Develop standardized policies and procedures for moves to production. Specifically develop policies and procedures to identify minimum standards and processes required for each move to production request. In addition, these procedures should identify the roles and responsibilities of user agencies to ensure all moves to production are appropriately approved and authorized prior to moving the request into production.
- Develop standardized policies and procedures for verifying backups.
- Update the ISD Media Guide and ISD Library Guide and ensure all sections are completed.

OPERATIONS - STORAGE AND BACKUP

EXISTING ENVIRONMENT

Department Description of Control: The Enterprise Storage and Backup (ESB) Guide contains procedures to ensure z/OS cleanups, restores, and DASD additions and deletions are completed successfully.

- The ESB Guide also includes Weekly/Daily Cleanups, DASD Addition Checklist, DASD Removal Checklist, DASD Return to Spare, DASDadd, and ADRDSSU Restore.

Tests Performed: Reviewed ESB Guide procedures and interviewed staff.

Test Results: The Department developed the ESB Guide located on the ESB Sharepoint site. The Guide consisted of procedures utilized by ESB staff to help ensure that z/OS clean-up, restores, and DASD adds/deletes were completed successfully. The ESB Guide contained procedures including the BCCS/ISD Cleanup Procedures, DASD Addition Checklist, DASD Removal Checklist, DASD Return to Spare, DASD add, and ADRDSSU Restore.

ESB staff was responsible for the allocation, backup, and removal of storage (from disk to tape) for the Department's mainframe systems.

System Managed Storage (SMS) was used to manage Public (shared) and Private (agency-dedicated) Pools.

ESB staff was responsible for migrating data, deleting disk packs, and adding additional disk space when needed.

Department management issued a memorandum, dated October 16, 2009, to agency Chief Information Officers encouraging the use of the Disk Library for Mainframe (DLM) as opposed to 3480 and 3490 tape technology. According to the memo, the Department would no longer support 3480 tape technology as of June 30th, 2010, whereas the 3480 drives would be eliminated. In addition, all physical tape scratch pools and all automated tape mounts that were not vault related would need to be converted to the DLM by June 30, 2010.

No significant exception noted.

Department Description of Control: CA-Scheduler is utilized for the scheduling of backups.

Tests Performed: Reviewed backup schedule, listing of backups, and interviewed staff.

Test Results: ESB staff utilized CA-Scheduler for scheduling backups, including mainframe backups. ESB staff was responsible for monitoring CA-Scheduler to ensure the backups were performed and completed successfully.

We reviewed a listing of scheduled backups performed by the Department, noting no exceptions.

No significant exception noted.

Department Description of Control: z/OS Backups are performed on the mainframe operating system data.

- System data is backed up daily and weekly with the weekly copies sent to the regional vault.
- Backups of non-operating system files are also performed by HSM.
- These backups are controlled by the SMS routines and are set by the customer at allocation time. When the customer allocates a new file, a management class is assigned which determines how long the data is kept.

Tests Performed: Reviewed backup listings and interviewed staff.

Test Results: Full z/OS backups were performed of the mainframe systems data daily and weekly with the weekly by HSM with copies sent to the Regional Vault. Backups were controlled by the SMS routines and set by the user at allocation time. When a user allocated a new file, a management class was assigned to determine how long the data would be kept.

We reviewed a listing of backups rotated to the off-site storage location and confirmed rotation of backups to the offsite location was regularly performed.

In addition, Department staff stated ESB did not backup agency programs and data. User agencies were responsible for assuring their data was backed up with the exception of any user data residing on SMS.

We obtained a listing of current backups stored off-site and noted no exceptions. Also see Operations-Library Services control for additional information.

No significant exception noted.

Department Description of Control: System Automation notifies ESB when storage falls below a pre-determined threshold for SMS storage. The Command Center notifies ESB when the threshold limit for private pools falls below a pre-determined limit.

Tests Performed: Reviewed notification and interviewed staff.

Test Results: System Automation notified ESB when storage fell below a pre-determined threshold for SMS storage.

Department staff stated system automation monitored threshold limits. Prior to the threshold limit (high-end) being reached, system automation automatically generated an email to ESB staff alerting them of the limit being reached. Department staff stated the Command Center staff would call via telephone and send text message to ESB staff informing them of a critical situation if the lower end of the threshold was about to be reached. We reviewed a notification sent to ESB staff and confirmed the threshold was regularly monitored.

No significant exception noted.

Department Description of Control: ESB monitor Private Pool resources and notify agencies once a pre-determined threshold is met.

Tests Performed: Reviewed Private Pool list, email notification, and interviewed staff.

Test Results: ESB monitored Private Pool resources and notified agencies once a pre-determined threshold was met.

The Department provided a list of Private Pools managed by ESB. The list documented the system, pool name, pool description and criticality description. The list also documented actions to be taken. We reviewed notifications that were sent via email once a day to ESB staff when free space was 7% to 10% and every 15 minutes when free space was 0% to 6%. After normal working hours the Command Center notified the Resource Management On-Call staff when free space was 0% to 6%.

No significant exception noted.

Department Description of Control: An Enterprise Service Request (ESR) is utilized in requesting large amounts of disk space for SMS Pools.

Tests Performed: Reviewed ESR, Change Management Request**,** Remedy Help Desk tickets, and interviewed staff.

Test Results: Department staff stated an ESR was required for requesting large amounts of disk space in SMS Pools. Department staff also stated an ESR was completed when an agency was requesting storage. Once completed and approved, the ESR was submitted to the Change Management staff who documented the request in the form of a service request. Help Desk Tickets were also used when there was an emergency need for space when a storage pool ran low.

Department staff stated there was no criteria for differentiating between special requests for disk space and requests for large amount of disk space. ESB interprets disk space requests all the same. However, ESB differentiates between an ESR and Help Desk tickets. An ESR was required when an agency was requesting storage. Help Desk tickets were used when there was an emergency need for space when a storage pool ran low.

We reviewed a completed ESR used to document a request for large amount of storage; noting no significant exceptions. See Change Control and Communications Solution Center controls for additional information.

In addition, Department staff stated ESB staff was solely responsible for migrating data, deleting disk packs, and adding additional space.

No significant exception noted.

Department Description of Control: A Remedy ticket is utilized for special requests for disk space.

Tests Performed: Reviewed Help Desk ticket, and interviewed staff.

Test Results: Department staff stated special requests for disk space must be requested via a Help Desk ticket within Remedy. Help Desk tickets were also used when there was an emergency need for space when a storage pool ran low.

We reviewed a Help Desk ticket for requesting disk space; noting no significant exceptions. See Change Control and Communications Solution Center controls for additional information.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls appeared to be operating with sufficient effectiveness to achieve the control objectives.

SYSTEMS SOFTWARE - ZERO DOWNTIME VIRTUAL (z/VM)

EXISTING ENVIRONMENT

Department's Description of Control: Agency security software administrators must submit a request to z/VM staff for a user to have access to z/VM. User IDs and passwords are utilized to control access to z/VM.

Tests Performed: Reviewed process for granting access rights.

Test Results: During our review, we noted the following nine agencies utilized z/VM:

- Department of Healthcare and Family Services.
- Department of Children and Family Services.
- Department of Transportation.
- Department of Public Health.
- Department of Central Management Services.
- Department of Employment Security.
- Department of Human Services.
- Department of Revenue.
- Illinois Racing Board.

Authorized user agency representatives would send an electronic mail message to z/VM staff to request a z/VM User ID.

User IDs and passwords are utilized to control access to z/VM.

No significant exception noted.

Department's Description of Control: Security software and system options are implemented to protect resources and data. Access to the z/VM Directory is limited to z/VM staff.

Tests Performed: Reviewed security software reports and confirmed with Department staff.

Test Results: System options and parameters were implemented to protect data and resources.

In addition, we noted access to the z/VM directory was limited to z/VM staff.

No significant exception noted.

Department's Description of Control: Assigned Department staff is responsible for software installation, maintenance, performance monitoring, and security.

Tests Performed: Reviewed security reports, change tickets, and interviewed staff.

Test Results: During our review, we noted there were two Department staff responsible for software installation, maintenance, performance monitoring, and security.

System options and parameters were implemented to protect data and resources.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective.

SYSTEMS SOFTWARE - ZERO DOWNTIME OPERATING SYSTEM (z/OS)

EXISTING ENVIRONMENT

Department Description of Control: Assigned Department staff is responsible for software installation, maintenance, performance monitoring, and security.

Test Performed: Reviewed list of system programmers and areas of responsibility and interviewed staff.

Test Results: Assigned Department staff was responsible for software installation, maintenance, performance monitoring, and security. It appeared the Department had staffing issues in the systems support area that needed to be addressed. See the Personnel Control for additional information.

No significant exception noted.

Department Description of Control: System activity is recorded via the selection of System Management Facility (SMF) options.

Test Performed: Reviewed system recording options, security reports, and interviewed staff.

Test Results: The System Management Facility (SMF) recorded operating system activities. In addition, the Department had ensured recorded activities were adequately backed up.

No significant exception noted.

Department Description of Control: Agency security software administrators must submit a request to CMS security software staff for a user to have TSO access.

Test Performed: Reviewed process for requesting access and email notifications.

Test Results: Authorized user-agency representatives send an electronic mail message to security software staff to request TSO access.

No significant exception noted.

Department Description of Control: User ID’s and passwords are utilized to control access to z/OS.

Test Performed: Reviewed the DS Monitor report, System Options listing, and systems programmer access rights.

Test Results: Resource Access Control Facility (RACF) was active and utilized by the Department to control access to the z/OS operating environment. In order to gain access to the z/OS operating environment, a valid RACF user ID and password must be provided. The Department had established RACF user ID and password requirements regarding inactive user ID's, change intervals, and various password restrictions.

No significant exception noted.

Department Description of Control: Security software options are implemented to secure libraries, and protect resources and data.

Test Performed: Reviewed security profiles, system configurations, system options, and interviewed staff.

Test Results: Security software and system options were implemented to secure libraries, protect resources, and data.

Department Description of Control: CPU utilization is monitored and managed through the regular production of Resource Monitoring Facility (RMF) reports. RMF reports are stored on a secured drive and are available to management.

Test Performed: Reviewed RMF reports, and interviewed staff.

Test Results: The Department generated Remote Monitoring Facility (RMF) reports on routine basis to assist management in monitoring system resources and CPU utilization.

No significant exception noted.

Department Description of Control: Access to system console and direct access storage devices (DASD) are restricted by physical and logical security controls.

Tests Performed: Reviewed security profiles, system configurations, system options, and interviewed staff.

Test Results: Access to system console and direct access storage devices (DASD) was restricted by physical and logical security controls.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective.

SYSTEMS SOFTWARE - CUSTOMER INFORMATION CONTROL SYSTEM (CICS)

EXISTING ENVIRONMENT

Department Description of Control: Assigned Department staff is responsible for software installation, maintenance, performance monitoring and security.

Tests Performed: Reviewed documentation and interviewed staff.

Test Results: At the time of our review, the Department had assigned four staff responsible for software installation, maintenance, performance monitoring, and security.

No significant exception noted.

Department Description of Control: The Department offers three different levels of CICS support for customers, described as follows:

- **Level One** – The Department supports only the CICS software. The customer is responsible for all security for the customer owned CICS regions.
- **Level Two** – The Department supports the CICS software, and maintains CICS System Definition File (CSD)/table definitions for the customer. The customer supplies the definitions to the Department and controls the application support. The Department and the customer owning agency share security responsibilities.
- **Level Three** – The Department supports the CICS software, maintains CSD/table definitions, and supports both CICS and the application software for the agency. The Department is also responsible for security for these regions.

Tests Performed: Reviewed CICS regions and interviewed staff.

Test Results: There were 31 CICS regions (10 production, 9 test, and 12 development).

The Department provided CICS support for user agencies as follows:

Level One Support

- Department of Human Services (6 regions)
- Department of Employment Security (2 regions)
- Department of Corrections (2 regions)

Level Two Support

- Department of Central Management Services (6 regions)
- Illinois Student Assistance Commission (2 regions)
- Department of Revenue (13 regions)

Level Three Support

- No agencies currently receive Level Three Support.

No significant exception noted.

Department Description of Control: Production regions are segregated from test and development regions to restrict access, based upon the various needs for each type of region. Restricted access to sensitive CICS transactions is established over production regions. Test regions have fewer access restrictions. Test regions allow programmers to test and debug against non-production files.

Tests Performed: Reviewed region listings, general resource classifications and access rights to restricted commands.

Test Results: We obtained a listing of established CICS regions. The production CICS regions were separated from the test and development/training CICS regions. Restricted access to sensitive CICS transactions was established over production regions. Non-production regions (test and development/training regions) had fewer access restrictions to allow programmers to develop and test applications.

No significant exception noted.

Department Description of Control: Security software and system options are implemented to secure libraries, and to protect resources and data.

Tests Performed: Reviewed system options, settings, definitions and security reports; and interviewed staff.

Test Results: Security software and system options were implemented to secure libraries and protect resources and data. In addition, restricted access to sensitive CICS transactions was established.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls appear to be operating with sufficient effectiveness to achieve the control objective.

SYSTEMS SOFTWARE – DATABASE 2 (DB2)

EXISTING ENVIRONMENT

Department Description of Control: Security software and system options are implemented to protect resources and data.

Tests Performed: Reviewed subsystems, Installation Job Stream, and interviewed staff.

Test Results: Security software and system options were implemented to protect resources and data.

No significant exception noted.

Department Description of Control: Assigned Department staff is responsible for software installation, maintenance, performance monitoring, and security.

Tests Performed: Interviewed staff.

Test Results: Assigned Department staff was responsible for software installation, maintenance, performance monitoring, and security. Staff was assigned to monitor the performance and problems of DB2. It appeared the Department had staffing issues in the DB2 support area that needed to be addressed. See the Personnel control for additional information.

No significant exception noted.

Department Description of Control: One user ID at each agency is authorized by the Department to coordinate the use of DB2 within the agency.

Tests Performed: Reviewed Agency DB2 Coordinator list and interviewed staff.

Test Results: One user ID at each agency was authorized by the Department to coordinate the use of DB2 within the agency. We reviewed a list of DB2 Coordinators assigned by the user agencies, noting no exceptions.

No significant exception noted.

Department Description of Control: Users are required to have a security software ID and password and authenticate successfully. After authentication, DB2 internal security verifies access rights to specific data.

Tests Performed: Reviewed security reports and interviewed staff.

Test Results: DB2 was integrated with Resource Access Control Facility (RACF) security software. Users must have a valid RACF ID and password before they can gain access to the DB2 resources. Users were required to have a security software ID and password and authenticate successfully. After authentication, DB2 internal security verified access rights to specific data.

No significant exception noted.

Department Description of Control: Production systems are segregated from test and development systems to restrict access, based upon the various needs for each type of system.

Tests Performed: Reviewed subsystem documentation and interviewed staff.

Test Results: Production systems were segregated from test and development systems to restrict access, based upon the various needs for each type of system. We reviewed a list of DB2 subsystems for the Department, noting no exceptions.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

SYSTEMS SOFTWARE - INFORMATION MANAGEMENT SYSTEM (IMS)

EXISTING ENVIRONMENT

Department Description of Control: Security software and system options are implemented to protect resources and data.

Tests Performed: Reviewed system options, security reports, and interviewed staff.

Test Results: Security software and system options were implemented to protect resources and data. IMS was integrated with Resource Access Control Facility (RACF) security software. Users must have a valid RACF ID and password before they could gain access to IMS resources. User access to agency-specific IMS resources was controlled by the user agency RACF Coordinators.

No significant exception noted.

Department Description of Control: Production regions are segregated from test and development regions to restrict access, based upon the various needs for each type of region.

Tests Performed: Reviewed region listing and interviewed staff.

Test Results: Production regions were segregated from test and development regions to restrict access, based upon the various needs for each type of region.

Department personnel stated IMS resources were scheduled in CA-Scheduler for automatic backups. User agencies were responsible for ensuring their specific user agency databases/resources was being backed up.

No significant exception noted.

Department Description of Control: Assigned Department staff is responsible for software installation, maintenance, performance monitoring, and security.

Tests Performed: Reviewed monitoring report and interviewed staff.

Test Results: IMS personnel were responsible for software installation, maintenance, and security. Reports were generated and used by IMS personnel for performance monitoring of the IMS regions.

We reviewed a monitoring report that provided statistics regarding transaction processing including number of transactions, amount of time transactions utilized, number of reads, writes performed, and other information.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives.

SYSTEM SOFTWARE - SECURITY SOFTWARE

EXISTING ENVIRONMENT

Department Description of Control: RACF is the primary tool for controlling and monitoring access, and options are implemented to protect resources and data.

Tests Performed: Reviewed literature, security software reports, and interviewed staff.

Test Results: A security software package (Resource Access Control Facility - RACF) existed and was used to control and monitor access to Department resources.

No significant exception noted.

Department Description of Control: Assigned Department staff is responsible for the implementation and administration of RACF.

Tests Performed: Reviewed security software reports and interviewed staff.

Test Results: The Department assigned staff members with the primary responsibility to implement and administer security software. The access rights were appropriately assigned to these staff members.

No significant exception noted; however, we did note an excessive number of unused (revoked) IDs assigned to user agencies on the system.

Department Description of Control: Users are required to have a valid ID and password.

Tests Performed: Reviewed literature, security software reports, and interviewed staff.

Test Results: User IDs and passwords were used to identify and verify users and were key control mechanisms within RACF. RACF protected access and enforced user accountability over data and system resources by positively verifying the user’s authority to utilize that data or system resource, and by logging the user’s actions if a violation occurred.

No significant exception noted.

Department Description of Control: Invalid access attempts are logged and reviewed on a routine basis.

Tests Performed: Reviewed procedures, violation reports, and interviewed staff.

Test Results: The Department had a procedure in place for the monitoring of security violations. Department staff periodically reviewed violation reports.

No significant exception noted.

Department Description of Control: A RACF administrator at each agency is authorized by the Department to administer RACF use within the agency.

- User agencies are responsible for protecting their program and data files.
- RACF administrators have the capability of producing the violation reports for their agency.
- The Department requests verification of agency RACF coordinators on a semi-annual basis.

Tests Performed: Reviewed system menus and interviewed staff.

Test Results: Utilities were available for RACF administrators for maintenance of user IDs, access rights, and reports for their agency. User agencies were responsible for managing and maintaining access rights for security software, including protecting program and data files and producing violation reports for the agencies.

The Department sent out an authorization listing update request in June 2009. We noted 53% of the agencies submitted responses. See the Security Administration control for further details.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls are operating with sufficient effectiveness to achieve the control objective. However, to enhance the Department's controls, the Department should work with user agencies to decrease the number of unused (revoked) user IDs.

NETWORK SERVICES

EXISTING ENVIRONMENT

Background Provided by the Department: Network Services consists of two teams; Network Operations and Enterprise Network Support. Network Services, with the assistance of the Field Operations and LAN Services divisions as necessary, provide telecommunications/network services to a variety of agencies, boards and commissions, educational institutions, and other governmental and non-profit entities.

Department's Description of Control: To document its network architecture, network diagrams are maintained.

Tests Performed: Reviewed network diagrams, device configurations, and interviewed staff.

Test Results: To document its network architecture, network diagrams for the backbone segment depicting the network architecture and the placement of the core, distribution, access and egress routers were maintained.

Upon review and discussion with staff, network diagrams provided appeared to be, for the most part, accurate and complete. Additionally, during our review of diagrams and configurations we determined devices were placed in suitable logical positions.

No significant exception noted.

Department's Description of Control: ICN Remedy and EMS 11 are utilized to inventory data circuits currently being utilized.

Tests Performed: Interviewed staff.

Test Results: ICN Remedy and EMS were utilized to inventory data circuits currently being utilized. During the review, the Department was in the process of migrating records from ICN Remedy to EMS for billing purposes. The migration project was anticipated to be complete at the start of FY12. At that time, ICN Remedy would be discontinued.

No significant exception noted.

Department's Description of Control: To ensure the networks are appropriately configured, the Department:

- Has established standards.
- Created configuration templates for core and distribution routers.
- Utilizes Cisco Advanced Services quarterly reports.

Tests Performed: Reviewed network diagrams, device configurations, hardware and software vendor websites, configuration templates, Department websites, and interviewed staff.

Test Results: Network Services was responsible for installing, maintaining, managing and supporting the network utilizing sites strategically placed throughout the State.

The Department maintained configuration templates for core and distribution routers and other access devices. However, the Department had not established standards as outlined in the Description of Control.

The Department utilized the Cicso Advanced Services reports.

The network was divided logically into layers: Core, Distribution, and Acces. We reviewed the current electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. Upon review it appeared the configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

No significant exception noted; however, we noted some parameters which should be reviewed to ensure security issues are appropriately addressed. In addition, the Department had not established standards as outlined in the Description of Control.

Department's Description of Control: Authentication servers are utilized to control access and ensure only properly authenticated individuals are granted access to devices for configuration management and maintenance.

Tests Performed: Reviewed access rights, account parameters, device configurations, vendor website, and interviewed staff.

Test Results: Authentications servers were utilized to provide authorized access to devices maintained by Network Operations, Enterprise Network Support and Field Operations. Per review of the vendor website, the servers appeared to be using the current vendor recommended release.

The administrative architecture on these boxes was such that groups had been established with specific levels of administrative privileges for the individual's needs. Upon review, accounts with powerful access rights appeared to be appropriately assigned and utilized appropriate access restrictions.

We also reviewed device configurations for the IP addresses of defined external authentication servers and compared these IP addresses to the IP addresses of the three external authentication servers in production. Upon review of configuration files we noted a small number of devices that did not utilize any authentication servers.

No significant exception noted; however, all devices were not connected to an authentication server.

Department's Description of Control: The CMS Change Management process is utilized to ensure changes to the network infrastructure are accurately tracked and appropriately authorized.

Tests Performed: Interviewed staff.

Test Results: Network infrastructure changes followed the CMS Change Management process to ensure changes were tracked and appropriately authorized. See Change Control review for additional information.

No significant exception noted.

Department's Description of Control: Firewall, router, and switch configurations are backed up via two servers.

- The servers are backed up to tape weekly.
- Backups are rotated off-site.

Tests Performed: Reviewed device configurations, SolarWinds, and interviewed staff.

Test Results: One backup server was utilized to routinely backup device configurations. Three times weekly, backups were rotated to the off-site storage facility.

No significant exception noted.

Department's Description of Control: SolarWinds Orion is utilized to monitor the network.

Tests Performed: Reviewed SolarWinds, device configurations, and interviewed staff.

Test Results: SolarWinds was utilized to monitor the backbone core, distribution, and access devices.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. However, the complexity of the statewide network necessitates continual review and analysis to ensure security controls meet the Department's standards. To enhance the controls, Network Services should establish standards as outlined in the Description of Control and continually review security parameters to ensure security issues are adequately addressed.

NETWORK SERVICES - IWIN

EXISTING ENVIRONMENT

Background Provided by the Department: The Department and the Illinois State Police have joined efforts in providing the Illinois Wireless Information Network (IWIN).

Department's Description of Control: The "Illinois Statewide Policy Manual," located on the CMS BCCS Catalog website at: http://bccs.illinois.gov/pdf/iwin/iwinpolicymanual.pdf outlines the responsibilities for the Department, ISP, local agency IWIN coordinator and the IWIN user, as well as appropriate usage, necessary certifications to obtain IWIN access and Motorola client functions.

Tests Performed: Reviewed policies.

Tests Results: The Illinois Statewide IWIN Policy Manual (Manual), dated October 2008 and posted on the Internet, outlined the responsibilities for DCMS – IWIN Support Center, Illinois State Police, Local Agency IWIN Coordinators, and the IWIN user.

No significant exception noted.

Department's Description of Control: The IWIN network infrastructure utilizes redundant routers which connect servers to the provider network.

Tests Performed: Reviewed network diagrams, device configurations, and interviewed staff.

Tests Results: The IWIN infrastructure contained redundant routers and firewalls maintained by Network Services. See the Network Services control for additional information on firewalls and routers.

No significant exception noted.

Department's Description of Control: The IWIN infrastructure is comprised of a multi-layer security approach. This approach secures access to the infrastructure from the IWIN user community by utilizing strong authentication such as user IDs, passwords, and unit IDs.

Tests Performed: Interviewed staff.

Tests Results: The IWIN infrastructure was comprised of a multi-layer security approach consisting of application and network layer firewalls as well as software to control user access to IWIN infrastructure.

No significant exception noted.

Department’s Description of Control: TACACS Servers authenticate authorized individuals for device configuration and maintenance.

Tests Performed: Reviewed device configurations and interviewed staff.

Tests Results: Authentication servers were utilized to authenticate access to devices for configuration and maintenance.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective.

NETWORK SERVICES - FIELD OPERATIONS

EXISTING ENVIRONMENT

Background Provided by the Department: Field Operations is responsible for provisioning of hardware and circuits for connections to the ICN as well as providing technical help desk support.

Department's Description of Control: The Remedy ticketing system and its internal functionality provides the tools and means by which customer incidents and service requests are logged, tracked, and updated with supporting documentation through resolution.

Tests Performed: Reviewed ICN Remedy and interviewed staff.

Test Results: The Department utilized the ICN Remedy ticketing system to log, track, and document customer incidents and service requests.

No significant exception noted.

Department's Description of Control: Remedy ticket procedures require all tickets to be properly documented and worklog entries to be entered as work progress or resolution steps are performed. Various documents assist the process and means by which Field Operations handles the repair calls from customers via the Remedy Help Desk Case module.

Tests Performed: Reviewed the MP ICN Remedy Ticket Procedure, MP CMS Remedy Login Procedure, ICN Remedy Tickets, and interviewed staff.

Test Results: The Department had developed the following procedures to assist staff with logging into the Remedy system and the creation and resolution of tickets:

- MP ICN Remedy Ticket Procedures, last reviewed October 2008, and
- MP CMS Remedy Login Procedure, last reviewed December 2008.

We reviewed 25 ICN Remedy tickets for completeness and timeliness, noting no exceptions.

No significant exception noted.

Department's Description of Control: Weekly conference calls and review of trouble tickets helps identify trends and recurring problems.

Tests Performed: Reviewed meeting agendas and interviewed staff.

Test Results: Weekly meeting were held each Monday and were attended by staff from Network Services, CMC and Field Operations. Upon review of meeting agenda's for the month of March 2010, it appeared meetings discussed current projects and other issues needing attention.

No significant exception noted.

Department’s Description of Control: Domain Name Service – Non-Agency Process located on Field Ops master document library Sharepoint site.

Tests Performed: Reviewed procedure and Sharepoint site.

Test Results: The Domain Name Service – Non-Agency – Process procedure (dated June 19, 2009) located on the Sharepoint site provided procedures for maintaining DNS records for non-agency IP addresses and domains. Procedures require the utilization of ICN Remedy tickets to document the work associated with the non-agency IP address and domains.

No significant exception noted.

Department’s Description of Control: Master configuration templates exist for Agency and Non-Agency routers. Configurations of access routers are backed up and stored on servers located at the RTC offices and in Springfield.

Tests Performed: Reviewed network diagrams, device configurations, hardware and software vendor websites, configuration templates, access rights, account parameters, SolarWinds, and interviewed staff.

Test Results: Enterprise Network Support and Field Operations were responsible for installing, maintaining and managing the access segment of the network. Enterprise Network Support maintained select Agency Access devices, while Field Operations maintained the remaining Agency Access Devices and non-State Agency access devices. See the Network Services control for additional information.

Access devices connected each of the respective agencies’ and non-state agencies’ networks to the ICN Backbone Network via distribution routers. We reviewed the current electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. We reviewed the full configurations for a selection of devices as follows:

- 25 State Agency Access Routers
- 17 Non-State Agency Access Routers.

Upon review it appeared the configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

Authentications servers were utilized to provide authorized access to devices maintained by Network Operations, Enterprise Network Support and Field Operations. Per review of the vendor website, authentication software utilized appeared to be the current vendor recommended release. Upon review, accounts with powerful access rights appeared to be appropriately assigned and utilized appropriate access restrictions. See the Network Services control for additional information.

We also reviewed device configurations for the IP addresses of defined external authentication servers and compared these IP addresses to the IP addresses of the external authentication servers in production. Upon review of configuration files we noted a small number of devices that did not utilize any authentication servers.

The same backup server utilized by Network Services, was also utilized to routinely backup Agency Access device configurations maintained by Field Operations. Upon review, we noted all 25 Field Operations Agency Access devices permitted the backup server access to the devices for configuration backups. See the Network Services control for additional information.

Additionally, backup servers located at the various RTCs were utilized to routinely backup non-Agency Access device configurations maintained by Field Operations. Upon review, we noted all 17 non-Agency Access devices permitted the devices respective RTC backup server access to the device for configuration backups.

Additionally, devices connected to SolarWinds for monitoring purposes, were also connected to the SolarWinds Network Configuration Module (NCM). NCM inspects the configuration files daily for changes, making new backup copies when changes were identified. All of 42 Field Operations devices, selected for review to ensure SolarWinds connectivity, were connected to SolarWinds. See the Network Services control for additional information.

No significant exception noted; however, we noted some parameters which should be reviewed to ensure security issues were appropriately addressed and all devices were not connected to an authentication server.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. However, the complexity of the statewide network necessitates continual review and analysis to ensure security controls meet the Department’s standards. To enhance the controls, Field Operations should continually review security parameters to ensure security issues are adequately addressed.

NETWORK SERVICES - LAN SERVICES

EXISTING ENVIRONMENT

Background Provided by the Department: LAN Services is responsible for the installation, configuration, and support of the Department's LAN networking infrastructure, including: switches, routers, hubs, firewalls, wireless switches and inside cabling.

Department's Description of Control: The Department's LAN Standards document outlines the standard/template setting for the LAN network.

Tests Performed: Reviewed network diagrams, device configurations, hardware and software vendor websites, configuration standards, and interviewed staff.

Test Results: The Department maintained the State of Illinois Statewide Network. LAN Services was responsible for maintaining the State Agency Network (agency specific firewalls, routers, and switches).

LAN Services provided the LAN network architecture (including firewalls, routers, and switches) for the Department and consolidated agencies.

To assist in the configuration of Agency LAN infrastructure devices, LAN Services maintained the CMS/BCCS LAN Services Standards for Hardware Configuration and Development document. Upon review of the standards we noted they, for the most part, provided for appropriate baseline settings; however, we did note instance where configurations established within the standards could be enhanced. Additionally, upon review of configurations, we noted instances where the configurations deviated from the standards.

We reviewed the current electronic configurations of the devices, which contained software revision levels and fully documented high-level rule base descriptions. We reviewed the full configurations for a selection of devices as follows:

- 26 Firewalls.
- 25 Routers.
- 3 Switches.

Upon review it appeared the configurations were, for the most part, appropriately configured; however, we did note instances where configurations could be enhanced.

No significant exception noted; however, we did note some parameters which should be reviewed to ensure security issues are appropriately addressed.

Department's Description of Control: The Department maintained individual network topology maps for each network segment.

Tests Performed: Reviewed network topologies, device configurations, and interviewed staff.

Test Results: To document its network architecture, LAN Services maintained individual network topology maps for each of the agency network segments it maintained. Upon review and discussion with staff, network topology maps provided appeared to be, for the most part, accurate and complete. Additionally, during our review of topologies and configurations we determined devices were placed in suitable logical positions.

No significant exception noted.

Department's Description of Control: The Department utilizes SolarWinds Orion to monitor the network and ensure configurations are appropriately backed up.

- Reports of incidents are generated daily and distributed for appropriate review.

Tests Performed: Viewed SolarWinds output and interviewed staff.

Test Results: SolarWinds Orion was utilized to agency network segments maintained by LAN Services. SolarWinds Orion primarily monitored up/down status of devices. However, information was also collected regarding CPU utilization, memory, last reboot, packet loss, bandwidth, etc. for reference and reporting purposes as necessary.

SolarWinds also sent alerts and log information to the LAN Services logging server which was reviewed daily.

Additionally, all devices were connected to SolarWinds for monitoring purposes and were routinely backed-up.

No significant exception noted.

Department's Description of Control: TACACS is utilized to ensure only authorized individuals have appropriate access.

Tests Performed: Reviewed access rights, account parameters, device configurations, vendor website, and interviewed staff.

Test Results: Authentications servers were utilized to provide authorized access to the firewalls, routers, and switches maintained by LAN Services. Per review of the vendor website, the servers appeared to be using the current vendor recommended release.

We reviewed accounts with administrative privileges to ensure appropriate access restrictions and appropriate user assignment for the State Agency networking firewalls, routers and switches maintained by LAN Services. Upon review, accounts with powerful access rights generally appeared to be appropriately assigned and utilized appropriate access restrictions.

We also reviewed firewall, router, and switch configurations for the IP addresses of defined external authentication servers and compared these IP addresses to the IP addresses of the external authentication servers in production. Upon review of the configuration files we noted all devices reviewed utilized these servers.

No significant exception noted.

Department’s Description of Control: The Change Management process is utilized for tracking and authorizing changes.

Tests Performed: Interviewed staff.

Test Results: Agency network infrastructure changes followed the CMS Change Management process to ensure changes were tracked and appropriately authorized. See Change Control review for additional information.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. However, the complexity of the agency networks necessitates continual review and analysis to ensure security controls meet the Department’s standards. To enhance the controls, the Department should continually review security parameters to ensure security issues are adequately addressed and ensure established configuration standards (and associated templates) are consistently applied (when possible) to all devices.

LAN APPLICATION DEVELOPMENT

EXISTING ENVIRONMENT

Background Provided by the Department: The LAN Application Development section is responsible for the development of custom and packaged Local Area Network (LAN) based application software.

Department Description of Control: This process is governed by IT Governance; therefore we follow the pertinent IT Governance process and associated policy.

Tests Performed: Reviewed IT Governance process, IT Governance Policy, and interviewed staff.

Test Results: LAN Application Development utilized the IT Governance process and the IT Governance Policy for projects that were required to complete the process. See the IT Governance control for detailed testing.

There were no projects that went through IT Governance during the audit period.

No significant exception noted.

Department Description of Control: For changes made to LAN Applications, we follow the applicable sections of the EAA Systems Development Methodology, which includes the Rapid Application Development (RAD) Development Standards.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology, Service Requests, and interviewed staff.

Test Results: The LAN Application Development Unit utilized the Application Systems Development Methodology (also known as the EAA Systems Development Methodology), dated August 2005, for changes and new developments.

For new developments, the Department utilized the Rapid Application Development (RAD) process in the ASD Methodology. The RAD process allowed exceptions to the sequential processes of the Methodology to utilize iterative and prototyping development technologies.

The RAD Methodology provided the same information as the sequential Methodology process, except the deliverables were grouped differently.

There were no new developments during the audit period.

For changes (maintenance and ad hoc), the Methodology only required a service request to be completed.

There was one completed SR which was classified as ad hoc during the audit period.

No significant exception noted.

Department Description of Control: Changes or enhancements to existing LAN Applications are tracked and authorized via Service Requests submitted through the Service Request Registration System (SRRS) or via an Enterprise Service Request (ESR) submitted through Remedy Change Management.

Tests Performed: Reviewed changes, SRRS system, Remedy Change Management processes, and interviewed staff.

Test Results: The Department was in the process of phasing out the service request process through the SSRS System and utilizing the ESR process through the Remedy Change Management System to track and authorize changes.

For changes that were documented in the SRRS system, the Application Systems Development Methodology was utilized. We reviewed the one closed service request noting that it was properly authorized but not properly approved.

For changes that were documented in the Remedy Change Management system, the changes were either categorized as "changes" or "service requests". If the request was categorized as a change, then the Remedy Change Management Guide was utilized. If the request was categorized as a service request, then the Remedy User Guide was utilized.

Department management stated if the request was a problem/issue it was categorized as a "service request" and if the request was a change to an application or an enhancement it was categorized as a "change"

Unlike the SRRS systems process, the Department did not have specific references to a systems development process when utilizing ESR process through the Remedy Change System. In addition, a formal criteria for the determination of a change or service request was not incorporated in the ESR process.

We reviewed five "change" requests, noting none had an ESR attached as indicated in the Description of Control. However, the five change requests followed the Remedy Change Management Guide.

We reviewed seven "service requests", noting each had an ESR. However, we noted three service requests were not properly completed per requirements of the Remedy User Guide.

No significant exception noted due to the lack of new developments or major changes during the audit period. However, the formal process to track and authorize changes was not consistently applied. Additionally, the Department's procedures for changes controlled via Remedy did not address system development requirements.

Department Description of Control: The development security is controlled by Access Security Groups which, along with Drive Mapping, ensures that the individual developing the application does not move the change into the production environment.

Tests Performed: Interviewed staff.

Test Results: Development security was controlled via Access Security Groups. Access Groups were assigned to allow individuals access to specific folders.

No significant exception noted.

Department Description of Control: Management oversight, including authorization to move new or modified LAN Applications into production are controlled via the Service Request Registration System (SRRS) and Remedy Change Management.

Tests Performed: Reviewed service requests, Remedy change tickets, and interviewed staff.

Test Results: To ensure adequate authorization of moves to production, the Department utilized the authorization processes of the SRRS system or the Remedy Change Management process.

We reviewed the one closed service request (classified as maintenance) to ensure adequate authorization was obtained prior to moving the change into production, noting it was properly authorized but not properly approved. In addition, due to staffing limitations, the individual making the changes sometimes moved the change to production.

We also reviewed the five change tickets that followed the Remedy Change Management process to ensure adequate authorization was obtained prior to moving the change into production, noting no exceptions.

Although the Department had a process in place to ensure authorization and approval of changes it was not always followed. In addition, moves to the production environment were not always performed by an independent person.

OVERALL CONCLUSION

Based on the test results described above and the lack of any new developments or major changes during the audit period, the controls were operating with sufficient effectiveness to achieve the control objectives. However, to enhance the controls, the Department should ensure an appropriate segregation of duties exists and have an independent person perform moves to production. In addition, the Department should ensure all requests are properly approved and incorporate specific references to a systems development process for changes which utilize the Remedy Change System.

INTERACTIVE SYSTEMS (WEB SERVICES)

EXISTING ENVIRONMENT

Background Provided by the Department: The Department provides a variety of internal and external web sites/applications in order for agencies to communicate their information to both the public and private sectors.

Department Description of Control: Developers test for web accessibility in accordance with IITAA requirements using evaluation tools provided by DHS.

Tests Performed: Reviewed IITAA Website, emails, and interviewed staff.

Test Results: The Department of Human Services' website documented the Illinois Information Technology Accessibility Act (IITAA) guidelines utilized by the Department's Illinois Office of Information and Communications (IOIC) to determine website compliance with the IITAA guidelines.

The Department stated that Web Services did not have a formal procedure for Web Accessibility.

We reviewed the one service request that was closed during the audit period, noting an email indicated IITAA web accessibility testing had been conducted.

No significant exception noted.

Department Description of Control: Domain Name Service (DNS) Request Form with signatures for Requester and Server Admin ensure requests are properly authorized, documented and tracked.

Tests Performed: Reviewed DNS Request Forms and interviewed staff.

Test Results: Any State of Illinois agency, board, commission, city, county, etc. could request an Illinois.gov domain name.

Although, Web Services did not have a formal procedure to approve the Domain Name Requests; they did have an informal process which was to be followed.

We reviewed 20 Domain Name Request Forms noting they contained appropriate information and approvals.

No significant exception noted.

Content Management

Department Description of Control: New web site developments utilize the Web Services Content Change Procedures in conjunction with the New Website Checklist.

Tests Performed: Reviewed the Web Services Content Change Procedures, Website Checklist, and interviewed staff.

Test Results: The Department developed the Web Services Content Change Procedures, revised January 30, 2008 and the Website Checklist, not dated, to manage web content changes for websites managed by the Department.

However, upon review we noted the Procedures did not reflect the current process utilized by Web Service. Per Department management, the Web Services Manager had no involvement with the request, except when problems arose.

The Website Checklist was to be completed by the requesting agency, in order to provide information to Web Services on the design of the new website.

No significant exception noted; however, the Web Services Content Change Procedure did not reflect the current process.

Department Description of Control: Web Services Application (Access) is used to authorize web content changes.

Tests Performed: Reviewed the Web Content Change Procedures, Web Service Application (Access database), and interviewed staff.

Test Results: The Web Services Application was utilized to log information regarding the date in which the authorization email (from the user agency) was received by Web Services. The actual authorization email was maintained in a separate electronic file.

We reviewed 18 web content changes for the authorization email from the user agency, noting one of 18 did not have the email authorizing the change.

No significant exception noted; however, documentation supporting one change was not provided.

Department Description of Control: Changes or enhancements are tested in accordance with Web Services Content Change Procedures and a business owner or Illinois Office of Information and Communication review ensure content changes are correct.

Tests Performed: Reviewed the Web Content Change Procedures, emails, and the Web Service Application.

Test Results: According to the Web Services' Manager, it was the responsibility of the requesting agency or the Illinois Office of Information and Communication to conduct testing of the change/enhancement. Once testing was completed, an email was required to be sent to Web Service stating approval.

We reviewed 18 web content changes for approvals, noting that one of 18 did not have the email from the user agency or Illinois Office of Information and Communication accepting the changes.

No significant exception noted; however, documentation supporting approval of one change was not provided.

Department Description of Control: Access to the production environment is controlled by:

- Security access rights manage who can move the change.
- Web Services Content Change Procedures in conjunction with Web Services application defines the process and records the name of the person that moved the change to production.

Tests Performed: Reviewed web content changes for moves to production and interview staff.

Test Results: Access to the production environment was controlled by the employee's access rights.

According to the Web Services Change Procedures, the Production Manager was responsible for moving the change into the production environment. Additionally, the Web Services Application (Access database) recorded who completed the change and who moved the change to production.

We reviewed 18 moves to production for Web content changes noting one developer completed the change and move to production for 16 of the moves to production. The Department was unable to provide documentation on the move to production for the remaining two changes.

No significant exception noted, however documentation was not provided for two changes. In addition, moves to the production environment were not always performed by an independent person.

Internet Applications

Department Description of Control: This process is governed by IT Governance; therefore we follow the pertinent IT Governance process and associated policy.

Tests Performed: Reviewed IT Governance process, IT Governance Policy, IT Governance Charters and interviewed staff.

Test Results: Web Services utilized the IT Governance process and the IT Governance Policy for projects that were required to complete the process. See the IT Governance control for detailed testing.

No significant exception noted.

Department Description of Control: For changes made to Web Sites/Applications, we follow the applicable sections of the EAA Systems Development Methodology, which includes the Rapid Application Development (RAD) Development Standards.

Tests Performed: Reviewed Application Systems Development Methodology, service requests, and interviewed staff.

Test Results: Web Services utilized the Application Systems Development Methodology (also known as the EAA Systems Development Methodology), dated August 2005, for changes and new developments.

For new developments, the Department utilized the Rapid Application Development (RAD) process in the ASD Methodology. The RAD process allowed exceptions to the sequential processes of the Methodology to utilize iterative and prototyping development technologies.

The RAD Methodology provided the same information as the sequential Methodology process, except the deliverables were grouped differently.

For changes (maintenance and ad hoc), the Methodology only required a service request to be completed.

There was one completed service request which was classified as maintenance during the audit period.

No significant exception noted.

Department Description of Control: Changes or enhancements to existing Web Applications are tracked and authorized via Service Requests submitted through the Service Request Registration System (SRRS) or via an Enterprise Service Request (ESR) submitted through Remedy Change Management.

Tests Performed: Reviewed service requests, Remedy change tickets, and interviewed staff.

Test Results: The Department utilized the service requests process via the SRRS system and the ESR process via the Remedy Change Management system to document changes or enhancements to web applications.

We inquired with the Department regarding the criteria for determining if a change or enhancement would follow the Service Request process or the ESR process. The criteria had to do with the complexity, and the involvement of other divisions within the Department. If the change or enhancement required coordination between other divisions the ESR process was used. If the change or enhancement involved the servers that were managed by Web Services then the SRRS process was to be followed.

For changes that were documented in the SRRS system, the Application Systems Development Methodology was utilized. We reviewed the one closed Service Request during the audit period and noted it contained adequate approvals as defined by the Methodology.

We reviewed six “service requests”, noting each had an ESR; however, the service requests were not properly completed per requirements of the Remedy User Guide. Although, we did note the ESRs had been properly approved.

Unlike the SRRS systems process, the Department did not have specific references to a systems development process when utilizing ESR process through the Remedy Change System.

No significant exception noted; however, the Department’s procedures for changes controlled via Remedy did not address system development requirements.

Department Description of Control: Access to the production environment is controlled by:

- Security access rights manage who can move the change.
- An Enterprise Service Request (ESR) is submitted to move changes to Production.

Tests Performed: Reviewed moves to production and interviewed staff.

Test Results: Access to the production environment was controlled by the employee’s access rights.

The Internet Applications staff had access to applications in which they were the lead developer. In the event the Internet Application staff required additional access the user agency was required to give approval, via email to Web Services management.

The Department did not have formal procedures regarding the move to production; however, they had an informal process. After the developer made the change an ESR would be submitted requesting that the Midrange Group make the move. The ESRs were to be completed in accordance with the Remedy User Guide.

We reviewed 16 changes which were moved to production during the audit period, noting no exceptions.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objectives. However, to enhance their controls the Department should:

- Ensure all requests are properly completed.
- Ensure appropriate documentation is maintained.
- Update the Web Content Change Procedures to reflect the current process.
- Incorporate specific references to a systems development process for changes which utilize the Remedy Change System.
- Ensure appropriate segregation of duties exists and have an independent person perform moves to production.

This Page Intentionally Left Blank

APPLICATION CONTROLS
Control Objectives

Application controls are the methods, policies, and procedures adopted by an organization to ensure all transactions are entered, processed, and reported correctly. Application controls ensure data being entered, processed, and stored are complete and accurate. They ensure the output from the computer application is timely and accurate.

Application controls can be grouped into three areas: input; processing; and output. Input controls ensure the data entered into the system are authorized and accurate. These controls include both manual and computerized techniques. Processing controls are those that are coded into the software program. Manual procedures often supplement the programmed controls to verify that all processing has taken place as intended. Output controls govern the printing and distribution of reports. Specific control objectives are imbedded in the Department's Description of Control.

The Department has developed several applications for use by State agencies. As part of the Third Party Review, we reviewed four of the applications used by multiple State agencies.

The applications reviewed were:

- Accounting Information System;
- Central Payroll System;
- Central Inventory System; and
- Central Time and Attendance System.

This Page Intentionally Left Blank

ACCOUNTING INFORMATION SYSTEM (AIS)

EXISTING ENVIRONMENT

The Accounting Information System (AIS) was implemented in 1995. AIS was utilized by 55 entities. (See page 169 for a list of user agencies).

Background Provided by the Department: AIS functions as an automated expenditure control and invoice/voucher processing system. AIS, in processing invoices, allocates invoice amounts into sub accounts; groups invoices, according to the Comptroller's Statewide Accounting Management System (SAMS) procedures, for the preparation of vouchers; and allows users to track cost centers.

Department's Description of Control: AIS interfaces with the Illinois Governmental Purchasing System (IGPS), the Accounts Receivable Posting System (ARPS), the Central Inventory System (CIS) and the Central Payroll System (CPS).

Tests Performed: Reviewed interface listing and interviewed staff.

Test Results: AIS interfaced with the Illinois Governmental Purchasing System (IGPS), the Accounts Receivable Posting System (ARPS) and the Central Payroll System (CPS).

Department staff stated the Central Inventory System did not interface with AIS.

No significant exception noted.

Department's Description of Control: AIS is secured using security software, in addition to internal security requirements.

- Users must have an authorized ID and password to gain access.
- Assignment and authorization of access rights is the responsibility of the user agency.
- Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

Tests Performed: Reviewed the Mainframe Security Procedures, AIS User Manual, appropriateness of individuals with access to AIS, and interviewed staff.

Test Results: Access to AIS was controlled through security software (Resource Access Control Facility (RACF)), in addition to AIS' internal security. Users must have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment was obtained, users must use a separate application user ID and password to gain access to AIS.

Assignment and authorization of access rights were the responsibility of each agency's security administrator.

The Department required Departmental employees to complete a RACF Mainframe Request, obtain approval and forward to the Technical Support staff for completion of access rights. We reviewed access rights of 20 Department staff members to AIS, noting two of the individuals indicated as having access, were no longer employed by the Department. The Department indicated the access rights had been revoked.

No significant exception noted; however, access rights were not periodically reviewed to ensure appropriateness.

Department's Description of Control: Changes to AIS are controlled through the Enterprise Business Applications Methodology.

- Changes are initiated through the use of a Service Request Form.
- Changes are approved and tested before implementation into the production environment.
- Changes are moved into production by the Library Control Group.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology Manual (Methodology), Service Requests (SR's), Program Library Procedures, Move Production Forms, and interviewed staff.

Test Results: The Methodology, revised August 2005, was "created to provide a structured process for the design, development and implementation of new systems, enhancements and maintenance to existing systems and for development of ad hoc requests."

The Program Library Procedures outlined the requirements utilized for new programs and modifications to existing programs.

We tested five service requests and no significant issues were identified. However, we did note that three of the service requests had been classified as enhancements, when in fact they were maintenance requests.

Additionally, we noted there were no major changes to AIS in the past year.

No significant exception noted; however, three service requests were not properly classified.

Department's Description of Control: Quality assurance procedures apply to significant developments and enhancements.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures and service requests.

Test Results: The QA procedures were included in Appendix D of the Application System Development Methodology. The procedures outlined the monitoring process for the design, development, and implementation of new developments and enhancements.

No changes during the audit period were required to follow the QA procedures.

No significant exception noted.

Department’s Description of Control: The AIS User Manual, located on the State’s Enterprise Web Server (Intranet), provides guidance on the use of the Accounting Information System.

Tests Performed: Reviewed the AIS Online User Manual.

Test Results: The Department had an online User Manual, which provided users with guidance on logging into AIS, security screen functions, producing and processing invoices, edit checks, and producing reports.

No significant exception noted.

Department’s Description of Control: AIS transactions are entered online in a real-time environment, with the ability to batch transactions for processing at a later date. AIS was developed with edits that force correction of errors and completion of critical fields before a transaction is accepted. All data entry is performed by user agencies and is the responsibility of user agencies.

Tests Performed: Reviewed AIS Online User Manual and agency data.

Test Results: The AIS transactions were entered online in real time environment with the ability to batch transactions for processing at a later date. Additionally, the AIS Online User Manual provided information regarding AIS built in edit checks which required specific fields to be completed before AIS transactions could be completed.

The accuracy and reconciliation of data was the responsibility of the user agency.

During our review, we selected two agencies' AIS data and tested the accounting records for proper input, edits, and compliance with date standards. We determined that the 79,707 data records tested were properly entered within the established parameters and complied with date composition standards. During our testing of AIS data, we did not identify any significant weaknesses.

No significant exception noted.

Department’s Description of Control: AIS provides various online and batch reports to assist in the balance of transactions. A complete listing of the various reports is maintained in the AIS Users Manual. Retention of the various reports is the responsibility of the user agency.

Tests Performed: Reviewed AIS User Manual and interviewed staff.

Test Results: The AIS User Manual provided a complete listing of various online and batch reports used for the balancing of transaction. Also, the retention of the various reports was the responsibility of the user agency.

No significant exception noted.

Department's Description of Control: AIS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Tests Performed: Reviewed AIS backup schedule and backups maintained at the CCF or at the off-site storage location and interviewed staff.

Test Results: Department staff stated backups of AIS were performed daily, weekly and monthly. The weekly backups were copied and sent to the off-site storage for disaster recovery purposes.

We reviewed a sample of 25 AIS backup tapes which were to be located at the off-site storage facility. However, we noted six backup tapes were located at the CCF. Department management stated the backup tapes were in-transit.

No significant exception noted.

Department's Description of Control: A disaster recovery plan for AIS provides guidelines for restoration.

Tests Performed: Reviewed AIS disaster recovery plan and testing documentation.

Test Results: The Financial Applications Disaster Recovery Plan provided for disaster recovery of financial systems in accordance with the Department's overall recovery plan. The Plan was last updated and tested in December 2009.

This Financial Applications Disaster Recovery Plan was comprised of two parts: Financial Systems Disaster Testing and Financial Systems Disaster Plan.

The Plan stated testing was to be conducted annually to ensure that backup and restore components were still current and functional. The Plan provided detailed step-by-step instructions for the restoration of the application and user data.

In December 2009, the Department conducted testing of AIS; testing documentation indicated all tasks had been "met."

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should periodically review access rights to AIS and ensure access is appropriate and ensure all service requests are properly classified.

Department records listed the following entities as users of the Accounting Information System.

1. Board of Higher Education
2. Capital Development Board
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Corrections
6. Department of Financial and Professional Regulation
7. Department of Human Rights
8. Department of Insurance
9. Department of Labor
10. Department of Juvenile Justice
11. Department of Military Affairs
12. Department of Natural Resources
13. Department of Public Health
14. Department of Revenue
15. Department of Veterans' Affairs
16. Department on Aging
17. Environmental Protection Agency
18. General Assembly Retirement System
19. Guardianship and Advocacy Commission
20. Human Rights Commission
21. Illinois Arts Council
22. Illinois Civil Service Commission
23. Illinois Commerce Commission
24. Illinois Community College Board
25. Illinois Council on Developmental Disabilities
26. Illinois Criminal Justice Information Authority
27. Illinois Deaf and Hard of Hearing Commission
28. Illinois Educational Labor Relations Board
29. Illinois Emergency Management Agency
30. Illinois Gaming Board
31. Illinois Labor Relations Board
32. Illinois Law Enforcement Training and Standards Board
33. Illinois Office of the State's Attorneys Appellate Prosecutor
34. Illinois Prisoner Review Board
35. Illinois Procurement Policy Board
36. Illinois Racing Board
37. Illinois Student Assistance Commission
38. Illinois Violence Prevention Authority
39. Illinois Workers' Compensation Commission
40. Judges' Retirement System
41. Judicial Inquiry Board
42. Office of Management and Budget
43. Office of the Attorney General
44. Office of the Auditor General
45. Office of the Executive Inspector General
46. Office of the Governor
47. Office of the Lieutenant Governor
48. Office of the State Appellate Defender
49. Office of the State Fire Marshal
50. Property Tax Appeal Board
51. State Board of Elections
52. State Employees' Retirement System
53. State Police Merit Board
54. State Universities Civil Service System
55. Supreme Court of Illinois

CENTRAL PAYROLL SYSTEM (CPS)

EXISTING ENVIROMENT

The Central Payroll System (CPS) was implemented in 1972. CPS was utilized by 76 entities. (See page 175 for a list of user agencies).

Department Description of Control: CPS was designed to provide assistance in preparing payrolls for state agencies. The system will accommodate agencies which are governed by the Rules of the Personnel Code and agencies that are exempt from the Personnel Code (Non-Code Agencies). The payroll system is a tool to be used by qualified personnel with SAMS and payroll procedure knowledge. CPS enables state agencies to maintain automated pay records and provide a file that is submitted to the Comptroller's Office for the production of payroll warrants. CPS has an interface with Central Time and Attendance System (CTAS) and Accounting Information System (AIS).

Tests Performed: Reviewed CPS User Manual and interviewed staff.

Test Results: According to the User Manual, the system was designed to provide assistance in preparing payrolls for agencies within the State of Illinois. The system would accommodate agencies which were governed by the Rules of the Personnel Code and agencies that were exempt from the Personnel Code, (Non-Code Agencies). Guidelines for payrolls were set forth in the current version of the Statewide Accounting Management System (SAMS), and the Illinois Compiled Statues.

CPS interfaced with Central Time and Attendance System and the Accounting Information System.

No significant exception noted.

Department's Description of Control: CPS is secured using security software, in addition to internal security requirements.

- Users must have an authorized ID and password to gain access.
- Assignment and authorization of access rights is the responsibility of the user agency.
- Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

Tests Performed: Reviewed the Mainframe Security Procedures, CPS User Manual, appropriateness of individuals with access to CPS, and interviewed staff.

Test Results: Access to CPS was controlled through security software (Resource Access Control Facility (RACF)), in addition to CPS' internal security. Users must have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment was obtained, users must use a separate application user ID and password to gain access to CPS.

Assignment and authorization of access rights were the responsibility of each agency's security administrator.

The Department required Departmental employees to complete a RACF Mainframe Request, obtain approval and forward to the Technical Support staff for completion of access rights. We reviewed access rights of Department staff members to CPS, noting three individuals should not have had access to the system. Upon notification, the Department removed their access.

No significant exception noted; however, access rights were not periodically reviewed to ensure appropriateness.

Department's Description of Control: Changes to CPS are controlled through the Enterprise Business Applications Methodology.

- Changes are initiated through the use of a Service Request Form.
- Changes are approved and tested before implementation into the production environment.
- Changes are moved into production by the Library Control Group.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology Manual (Methodology), Service Requests (SR's), Program Library Procedures, Move Production Forms, and interviewed staff.

Test Results: The Methodology, revised August 2005, was "created to provide a structured process for the design, development and implementation of new systems, enhancements and maintenance to existing systems and for development of ad hoc requests."

The Program Library Procedures outlined the requirements utilized for new programs, and modifications to existing programs.

We tested five service requests for compliance with the Methodology, noting two service requests (classified as maintenance) were not properly approved.

Additionally, we noted there were no major changes to CPS in the past year.

We tested five service requests noting they required a move to production form to be completed. Our review indicated no exceptions.

No significant exception noted; however, two service requests (classified as maintenance) were not properly approved.

Department's Description of Control: Quality assurance procedures apply to significant developments and enhancements.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures and service requests.

Test Results: The QA procedures were included in Appendix D of the Application System Development Methodology. The procedures outlined the monitoring process for the design, development, and implementation of new developments and enhancements.

No changes during the audit period were required to follow the QA procedures.

No significant exception noted.

Department Description of Control: The CPS User Manual provides guidance on the use of the Central Payroll System.

Tests Performed: Reviewed CPS User Manual.

Test Results: The Department had a User Manual, dated April 2009, which provided users with guidance on logging into the application, recovery in the event of a disaster, backup cycle, adding/deleting employees, and the processing and completion of payroll.

No significant exception noted.

Department Description of Control: CPS has an edit feature designed to reject invalid information entered into the system. When invalid data has been entered into the system, an error message will appear at the top of the screen and the field that is in error will be highlighted. The system will not accept the entry until the error has been corrected or deleted. The Department has procedures in place to handle errors that occur during processing.

Tests Performed: Reviewed CPS User Manual, agency data, and interviewed staff.

Test Results: Data entered into the system was the responsibility of the user agency. The CPS contained online edit checks to help prevent a user from entering a transaction with invalid data. If an error occurred during data entry, users were not allowed to continue until the error had been corrected.

The online data entry function had error codes and corresponding messages, which were displayed online when an error occurred, and the field that had the error in it was highlighted. Although the error messages were not discussed directly in the CPS Manual, the messages were understandable, and the CPS Manual identified acceptable values for the field.

After the data was entered successfully, the CPS staff executed a Gross-to-Net program, which processed the batch transactions for any errors and generated a Tentative Vouchers Report. If no errors occurred, a copy of the Tentative Vouchers Report was forwarded to the agencies for approval prior to being submitted to the Comptroller’s Office for warrant generation. If an error occurred, it would be identified on the report, which also contained payroll totals and statistics. The totals and statistics were used by CPS staff to ensure that all payrolls had been processed.

If an error occurred and could be fixed, the CPS staff would fix the error, reschedule another voucher and complete a Payroll Adjustment form. The Payroll Adjustment forms were used to notify the agency of the error/correction.

During our review, we selected two agencies' CPS data and tested employee identification numbers, voucher numbers, warrant amounts and date fields for proper input, edits, and compliance with date standards. We determined that the 33,474 data records tested were entered properly and complied with date composition standards. During our testing of CPS data, we did not identify any significant weaknesses.

No significant exception noted.

Department Description of Control: The payroll vouchers/reports that are produced from the batch process are printed by the Department's Production Operations Services and delivered to Central Payroll.

- Central Payroll separates the vouchers/reports for each agency to pickup or to be delivered by Mail Messenger, UPS, or Fed Ex.
- Each agency must submit a list of individuals that are approved to pick up payroll related materials. This list is reviewed periodically by the user agencies.
- The retention of these payroll vouchers/reports is the responsibility of the user agency.

Tests Performed: Reviewed the Payroll Release Log, CPS Authorization Listing, CPS User Manual, and interviewed staff.

Test Results: Each pay period, the following standard payroll reports were provided to agencies:

- Personal Services Expenditure,
- Personal Services Expenditure/With Insurance,
- Employer Retirement Pick-Up,
- University Retirement Report,
- Group Insurance Salary Refund Report,
- Payroll/Group Insurance Discrepancy Report, and
- Position Occupied Report.

Reports were printed by I/O Control and then delivered to the CPS staff for distribution. Security guards were provided with the both the Payroll Pickup Procedures and a list of individuals authorized to pick up payroll reports. User agency staff obtained payroll reports from the lobby of the Communications Building after providing security guards with a valid ID for comparison to the authorization list and signing the Payroll Release Log.

We reviewed the Payroll Release Log for the month of February 2010, noting the individuals who picked up payroll were appropriately authorized.

No significant exception noted.

Department Description of Control: CPS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Tests Performed: Reviewed backup schedules, backups maintained at the CCF and at the off-site storage location, and interviewed staff.

Test Results: According to Department staff, CPS backups were performed twice daily, once before batch processing and once after the batch process. In addition, every week a backup was performed, which was rotated to the off-site location. Specific monthly backups were not performed.

We reviewed a sample of four CPS backup tapes and located all the tapes at the CCF or the off-site storage location.

In addition, we noted the CPS backup tapes were not encrypted to protect personal or confidential data.

No significant exception noted; however, CPS backup tapes were not encrypted to protect personal or confidential data.

Department Description of Control: Disaster Recovery guidance is included in the CPS User Manual.

Tests Performed: Reviewed CPS User Manual.

Test Results: Disaster recovery guidance was communicated to user agencies through the CPS User Manual. In the event of an emergency, Central Payroll would submit to the Comptroller’s Office the last correct version of the payroll file for payment. User agencies were responsible for supplying the last correct version of the hardcopy voucher to allow the Comptroller’s Office to produce a warrant for that agency. User agencies were responsible for retaining the hardcopy payroll voucher for the three most current pay periods.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should periodically review access rights to CPS and ensure access is appropriate and ensure all service requests are properly approved. In addition, the Department should ensure personal or confidential on backup tapes is adequately protected from unauthorized or accidental disclosure.

Department records listed the following entities as users of the Central Payroll System.

1. Board of Higher Education
2. Capital Development Board
3. Commission on Government Forecasting and Accountability
4. Court of Claims
5. Department of Agriculture
6. Department of Central Management Services
7. Department of Children and Family Services
8. Department of Commerce and Economic Opportunity
9. Department of Corrections
10. Department of Financial and Professional Regulation
11. Department of Human Rights
12. Department of Insurance
13. Department of Juvenile Justice
14. Department of Labor
15. Department of Military Affairs
16. Department of Natural Resources
17. Department of Public Health
18. Department of Revenue
19. Department of Veterans' Affairs
20. Department on Aging
21. East St. Louis Financial Advisory Authority*
22. Emergency Management Agency
23. Environmental Protection Agency
24. Executive Ethics Commission
25. Guardianship and Advocacy Commission
26. House of Representatives
27. Human Rights Commission
28. Illinois Arts Council
29. Illinois Civil Service Commission
30. Illinois Commerce Commission
31. Illinois Community College Board
32. Illinois Council on Developmental Disabilities
33. Illinois Criminal Justice Information Authority
34. Illinois Deaf and Hard of Hearing Commission
35. Illinois Educational Labor Relations Board
36. Illinois Gaming Board
37. Illinois Labor Relations Board
38. Illinois Law Enforcement Training and Standards Board
39. Illinois Math and Science Academy
40. Illinois Office of the State's Attorneys Appellate Prosecutor
41.. Illinois Prisoner Review Board
42. Illinois Procurement Policy Board
43. Illinois Racing Board
44. Illinois State Board of Investment *
45. Illinois State Police
46. Illinois Student Assistance Commission
47. Illinois Violence Prevention Authority
48. Illinois Workers' Compensation Commission
49. Joint Committee on Administrative Rules
50. Judges' Retirement System
51. Judicial Inquiry Board
52. Legislative Audit Commission
53. Legislative Ethics Commission
54. Legislative Information System
55. Legislative Printing Unit
56. Legislative Reference Bureau
57. Legislative Research Unit
58. Office of Management and Budget
59. Office of the Architect of the Capitol
60. Office of the Attorney General
61. Office of the Auditor General
62. Office of the Executive Inspector General
63. Office of the Governor
64. Office of the Lieutenant Governor
65. Office of the Secretary of State
66. Office of the State Appellate Defender
67. Office of the State Fire Marshal
68. Office of the Treasurer
69. Property Tax Appeal Board
70. State Board of Education
71. State Board of Elections
72. State Employees' Retirement System
73. State of Illinois Comprehensive Health Insurance Board
74. State Police Merit Board
75. State Universities Civil Service System
76. Teachers' Retirement System of the State of Illinois

* Agency Payroll information was entered into the system by CPS staff.

CENTRAL INVENTORY SYSTEM (CIS)

EXISTING ENVIRONMENT

The Central Inventory System (CIS) was implemented in 1998. CIS was utilized by 22 entities. (See page 180 for a list of user agencies).

Department Description of Control: CIS is an automated inventory control system. CIS has the ability to utilize an optical scanner to read bar code labels during a physical inventory by using additional external software. CIS allows user agencies to maintain records of inventory and to comply with the Department's Property Control Division's rules of reporting and processing. CIS meets all the GASB-34 rules; it allows the user agencies the ability to accurately track depreciation on items that they specify.

Tests Performed: Reviewed the Department's Property Control Division's rules, CIS User Manual, and interviewed staff.

Test Results: CIS was an automated system that allowed agencies to maintain records of inventory to comply with the Department's Property Control Division's rules of reporting and processing (44 Ill. Adm. Code 5010).

The rules of reporting and processing were divided into 12 subparts: General, Marking and Inventory of State Property, Property Reporting System, Inventory Requirements, Transferable Equipment, Scrap Sales and Procedures, Disposition of Vehicles, Disposition of Electronic Data Processing Equipment, Antique, Historical and Special Interest Property, Exemptions, Disposition of Laboratory Equipment, and Disposition of Hazardous Material.

Each subpart contained sections outlining documented procedures or rules for reporting and processing pertaining to property management.

CIS had the ability to read bar code labels for physical inventory.

The CIS application followed GASB-34 rules mandated by the Office of the Comptroller.

No significant exception noted.

Department's Description of Control: CIS is secured using security software, in addition to internal security requirements.

- Users must have an authorized ID and password to gain access.
- Assignment and authorization of access rights is the responsibility of the user agency.
- Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

Tests Performed: Reviewed the Mainframe Security Procedures, CIS User Manual, appropriateness of individuals with access to CIS, and interviewed staff.

Test Results: Access to CIS was controlled through security software (Resource Access Control Facility (RACF)), in addition to CIS' internal security. Users must have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment was obtained, users must use a separate application user ID and password to gain access to CIS.

Assignment and authorization of access rights were the responsibility of each agency's security administrator.

The Department required Departmental employees to complete a RACF Mainframe Request, obtain approval and forward to the Technical Support staff for completion of access rights. We reviewed access rights of six Department staff members to CIS, noting all staff appeared to have appropriate rights

No significant exception noted.

Department's Description of Control: Changes to CIS are controlled through the Enterprise Business Applications Methodology.

- Changes are initiated through the use of a Service Request Form.
- Changes are approved and tested before implementation into the production environment.
- Changes are moved into production by the Library Control Group.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology Manual (Methodology), Service Requests (SR's), Program Library Procedures, Move Production Forms and interviewed staff.

Test Results: The Methodology, revised August 2005, was "created to provide a structured process for the design, development and implementation of new systems, enhancements and maintenance to existing systems and for development of ad hoc requests."

During the audit period, CIS had one service request. We reviewed the service request, noting it complied with the Methodology.

Additionally, we noted there were no major changes to CIS in the past year.

The Program Library Procedures outlined the requirements utilized for new programs, and modifications to existing programs.

No significant exception noted.

Department's Description of Control: Quality assurance procedures apply to significant developments and enhancements.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures and service requests.

Test Results: The QA procedures were included in Appendix D of the Application System Development Methodology. The procedures outlined the monitoring process for the design, development, and implementation of new developments and enhancements.

No changes during the audit period were required to follow the QA procedures.

No significant exception noted.

Department's Description of Control: The CIS User Manual provides guidance to the use of the Central Inventory System.

Tests Performed: Reviewed the CIS User Manual.

Test Results: The Department had a User Manual, which provided users with guidance on logging into application, adding/deleting transactions, and various reports which were available.

The Online User Manual provided users with guidance on logging into CIS, add/inquire/change/delete transactions, Barcode Inventory Process, obtaining various reports and contacting the Help Desk.

No significant exception noted.

Department's Description of Control: Data is entered online by user agencies. CIS has several edit checks to alert users of errors. Errors must be corrected before the transaction is accepted.

Tests Performed: Reviewed CIS User Manual and agency data.

Test Results: CIS contained online edit checks to help prevent a user from entering a transaction with invalid data. If an error occurred during data entry, the online edit would display a message and prompt the user for correct data. Data was entered online by user agencies and errors must be corrected before the transaction was accepted.

During our review, we selected two agencies' CIS data and tested the inventory records for proper input, edits, and compliance with date standards. We determined that the 79,599 data records tested were entered properly and complied with date composition standards. During our testing of CIS data, we did not identify any significant weaknesses.

No significant exception noted.

Department's Description of Control: A Location Balance Report is run nightly to determine whether the previous day's transactions processed correctly. Additional reports are available to users. The accuracy and reconciliation of data is the responsibility of the user agency.

Tests Performed: Reviewed Location Summary Report, Physical Inventory Report, CIS User Manual, and interviewed staff.

Test Results: The Location Summary Report provided information on inventory locations, number of items with value less than $100, number of items with value greater than $100, and determine of capitalizing the asset or not.

Additionally, the Report of Physical Inventory Reconciliation provided inventory items locations, and values.

We reviewed the Department's CIS Location Summary Report dated April 18, 2010 noting the report indicated no locations were out of balance. The Department utilized the Physical Inventory Report to ensure transactions posted properly.

Data entered into the system was the responsibility of the user agency. The CIS User Manual provided information on various reports available to user agencies to assist them in ensuring the accuracy and reconciliation of CIS data.

No significant exception noted.

Department's Description of Control: CIS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Tests Performed: Reviewed backup schedule, and backups maintained at the CCF or the off-site storage location, and interviewed staff.

Test Results: Department staff stated backups of CIS were performed daily, weekly and monthly. The weekly backups were sent to the off-site storage for disaster recovery purposes.

We reviewed a sample of 30 CIS backup tapes which were to be located at the off-site storage facility, noting none were located there. Per Department management, in November 2009 Library Control changed the process for identifying the backup tapes requiring off-site storage, which resulted in the vault listing being inaccurate. After notification, management stated the process had been updated and the CIS backup tapes would be included on the vault listing.

Backup tapes were not properly located at the off-site storage location.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should ensure CIS backups are properly located and accounted for.

Department records listed the following entities as users of the Central Inventory System.

1. Capital Development Board
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Employment Security
5. Department of Finance and Professional Regulations
6. Department of Human Rights
7. Department of Military Affairs
8. Department of Public Health
9. Department of Transportation
10. Department of Veterans' Affairs
11. Department on Aging
12. Environmental Protection Agency
13. Illinois Arts Council
14. Illinois Deaf and Hard of Hearing Commission
15. Illinois Educational Labor Relations Board
16. Illinois Law Enforcement Training and Standards Board
17. Illinois Office of the State's Attorneys Appellate Prosecutor
18. Illinois Violence Prevention Authority
19. Office of Management and Budget
20. Office of the Attorney General
21. Office of the Governor
22. Office of the Lieutenant Governor

CENTRAL TIME AND ATTENDANCE SYSTEM (CTAS)

EXISTING ENVIRONMENT

The Central Time and Attendance System (CTAS) was implemented in 1992. CTAS was utilized by 33 entities. (See page 185 for the list of user agencies).

Department Description of Control: CTAS is an online system used to maintain "available benefit time". Additionally, CTAS allows user agencies to monitor whether usage of time is in accordance with state rules. CTAS provides for attendance information to be recorded using either the positive or exception methods. CTAS interfaces with the Central Payroll System.

Tests Performed: Reviewed CTAS User Manual and interviewed staff.

Test Results: CTAS was an online system which maintained current available benefit time balances and monitored the usage of time. CTAS recorded information using the positive or exception methods.

CTAS interfaced with the Central Payroll System.

No significant exception noted.

Department Description of Control: CTAS is secured using security software, in addition to internal security requirements.

- Users must have an authorized ID and password to gain access.
- Assignment and authorization of access rights is the responsibility of the user agency.
- Once access has been gained to the operating system, users must have a separate application user ID and password to gain access.

Tests Performed: Reviewed the Mainframe Security Procedures, CTAS User Manual, appropriateness of individuals with access to CTAS, and interviewed staff.

Test Results: Access to CTAS was controlled through security software (Resource Access Control Facility (RACF)), in addition to CTAS' internal security. Users must have a properly authorized security software user ID and password to gain access to the operating environment. Once access to the operating environment was obtained, users must use a separate application user ID and password to gain access to CTAS.

Assignment and authorization of access rights were the responsibility of each agency's security administrator.

The Department required Departmental employees to complete a RACF Mainframe Request, obtain approval and forward to the Technical Support staff for completion of access rights. We reviewed access rights of 20 Department staff members to CTAS, noting two individuals should not have had access to the system. Upon notification, the Department removed their access.

No significant exception noted; however, access rights were not periodically reviewed to ensure appropriateness.

Department Description of Control: Changes to CTAS are controlled through the Enterprise Business Applications Methodology.

- Changes are initiated through the use of a Service Request Form.
- Changes are approved and tested before implementation into the production environment.
- Changes are moved into production by the Library Control Group.

Tests Performed: Reviewed the Application Systems Development (ASD) Methodology Manual (Methodology), Service Requests (SR's), Program Library Procedures, Move Production Forms, and interviewed staff.

Test Results: The Methodology, revised August 2005, was "created to provide a structured process for the design, development and implementation of new systems, enhancements and maintenance to existing systems and for development of ad hoc requests."

The Program Library Procedures outlined the requirements utilized for new programs and modifications to existing programs.

During the audit period, CTAS had two maintenance service requests. We reviewed the service requests, noting they complied with the Methodology.

Additionally, we noted there were no major changes to CTAS in the past year.

We tested two service requests noting only one required a move to production form to be completed. Our review of the form noted no exceptions.

No significant exception noted.

Department Description of Control: Quality assurance procedures apply to significant developments and enhancements.

Tests Performed: Reviewed EBAS Quality Assurance (QA) procedures and service requests.

Test Results: The QA procedures were included in Appendix D of the Application System Development Methodology. The procedures outlined the monitoring process for the design, development, and implementation of new developments and enhancements.

No changes during the audit period were required to follow the QA procedures.

No significant exception noted.

Department Description of Control: The CTAS User Manual provides guidance to the use of the Central Time and Attendance System.

Tests Performed: Reviewed CTAS User Manual and interviewed staff.

Test Results: The Department had a User Manual, which provided users with guidance on logging into the application, adding/deleting employees, and the processing and completion of transactions.

No significant exception noted.

Department Description of Control: Data is entered online by user agencies. CTAS has edit checks to alert users of errors. Transactions with errors will be rejected

Tests Performed: Reviewed CTAS User Manual and agency data.

Test Results: Data entered into the system was the responsibility of the user agency. CTAS contained edit checks built into the system to notify the user of any exceptions. The system performed an online edit check and would reject all transactions that did not meet the edit criteria.

During our review, we selected two agencies' CTAS data and tested date fields, vacation balances, and the employee identification numbers for proper input, edits, and compliance with date standards. We determined that the 3,815 data records tested were entered properly and complied with date composition standards. During our testing of CTAS data, we did not identify any significant weaknesses.

No significant exception noted.

Department Description of Control: CTAS provides online and batch reports that user agencies may use for reconciliation purposes. During the “close” process, CTAS generates error reports, reconciliation reports, and file maintenance activity reports. All transactions must be reconciled before the “close” process can be finalized. The accuracy and reconciliation of data is the responsibility of the user agency.

Tests Performed: Reviewed CTAS User Manual.

Test Results: During the “Close” process, CTAS generated an error report, a reconciliation report, and a file maintenance activity report. All errors were to be reconciled before the “Close” could be finalized.

The CTAS User Manual documented reports that could be requested by the user for reconciliation purposes.

No significant exception noted.

Department Description of Control: CTAS is backed up daily, weekly, and monthly. Backups are maintained at the Central Computer Facility and the regional off-site storage location.

Tests Performed: Reviewed backup schedule, backups maintained at the CCF or the off-site storage location, and interviewed staff.

Test Results: According to Department staff, CTAS backups were performed twice daily, once before and once after batch processing. In addition, every week a backup was performed. Specific monthly backups were not performed.

We reviewed a sample of 25 CTAS backup tapes which were to be located at the off-site storage facility, noting no exceptions.

In addition, we noted the CTAS backup tapes were not encrypted to protect personal or confidential data.

No significant exception noted; however, CTAS backup tapes were not encrypted to protect personal or confidential data.

Department Description of Control: CTAS Recovery procedures provide guidelines for restoration.

Tests Performed: Reviewed CTAS Production Data Base Recovery Instructions.

The Department had developed the CTAS Production Data Base Recovery Instructions, dated February, 2010. The Instructions provided steps for the recovery of the CTAS database in the event of an outage or disaster.

No significant exception noted.

OVERALL CONCLUSION

Based on the test results described above, the controls were operating with sufficient effectiveness to achieve the control objective. To enhance controls, the Department should periodically review access rights to CTAS and ensure access is appropriate and ensure personal or confidential on backup tapes is adequately protected from unauthorized or accidental disclosure.

Department records listed the following entities as users of the Central Time and Attendance System.

1. Capital Development Board
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Commerce and Economic Opportunity
5. Department of Financial and Professional Regulation
6. Department of Human Rights
7. Department of Insurane
8. Department of Labor
9. Department of Natural Resources
10. Department of Public Health
11. Department of Revenue
12. Department of Veterans' Affairs
13. Department on Aging
14. Environmental Protection Agency
15. Guardianship and Advocacy Commission
16. Human Rights Commission
17. Illinois Civil Service Commission
18. Illinois Comprehensive Health Insurance Plans
19. Illinois Deaf and Hard of Hearing Commission
20. Illinois Educational Labor Relations Board
21. Illinois Gaming Board
22. Illinois Law Enforcement Training and Standards Board
23. Illinois Planning Council on Developmental Disabilities
24. Illinois Procurement Policy Board
25. Illinois Racing Board
26. Illinois Workers’ Compensation Commission
27. Office of Management and Budget
28. Office of the Attorney General
29. Office of the Executive Inspector General
30. Office of the Governor
31. Office of the State Fire Marshal
32. Property Tax Appeal Board
33. State Board of Elections

This Page Intentionally Left Blank

APPENDIX A

COMPLEMENTARY USER ORGANIZATION CONTROLS

Users of the State's Central Computer Facility are responsible for complying with prescribed requirements and for using available security mechanisms to protect the security and integrity of their data. During the course of our review, we identified several areas of user agency responsibility that should be reviewed by user agencies and their internal and external auditors.

Disaster contingency plans are needed.
Due to the fact agencies rely on the Department for computing services, they should take steps to reduce the risks associated with disruption or loss. Agencies should:

- Submit a listing of critical applications with all pertinent information to the Department, at least annually.
- Submit detailed recovery requirements to the Department.
- Submit formal disaster recovery plans to the Department.
- Ensure all data is backed up and stored appropriately off-site.
- Ensure all critical applications are tested at least annually. Additionally, agencies should submit detailed goals and results of the test to the Department.

Available security mechanism should be utilized.
To ensure that controls are functional at the agency level, agencies should:

- Effectively utilize security software features and perform periodic reviews of existing profiles to ensure that access rights are appropriate.
- Formally encourage users to include both alphabetic and non-alphabetic characters in their passwords, to protect the security of their account.
- Examine revoked IDs and delete IDs that are no longer necessary.
- Utilize the Department's password reset utilities for users who are required to have the ability to reset passwords. Powerful attributes should only be assigned to users who need administrative capabilities.
- Provide timely notification to the Department's DB2 Application Support Administrator if the agency DB2 Coordinator changes and assign the DB2 Coordinator ID to a specific person to promote accountability for the use of the ID.
- Review the use of security permissions that permit multi-write capabilities on z/VM (which may cause data to be corrupted or lost) and have it eliminated from all minidisks where it is not absolutely essential.
- Coordinate with the Department to assure that automatic time-out settings for their CICS regions provide reasonable protection of the information resources for the agency, while considering their operational needs.
- Utilize available encryption technology to protect confidential data, including data on backup media.

Bills for computer services should be reviewed.
User agencies should monitor the monthly billing to ensure charges are correct. Additionally, all user agencies should submit payment in a timely manner.

Security and Controls over the Internet should be reviewed.
To enhance security, agencies should:

- Regulate and monitor Internet web-based content by utilizing resources such as Internet content filtering and access logging.
- Develop and implement policies and procedures regarding appropriate Internet usage.
- Utilize available encryption technology to secure transmission of confidential or sensitive information across the Internet.
- Ensure the Department is notified of IWIN accounts that need to be deactivated in a timely manner.

Accounting Information Systems (AIS) use should be reviewed.
We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using AIS should:

- Verify only accurate and authorized data are entered into AIS. It is the agency's responsibility to ensure only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to AIS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.

Central Payroll System (CPS) use should be reviewed.
We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using CPS should:

- Verify only accurate and authorized data are entered into CPS. It is the agency's responsibility to ensure only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to CPS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up payroll reports, and inform appropriate CPS personnel of changes timely.
- Retain hardcopy payroll vouchers for at least the three most current pay periods, as specified by the CPS User Manual.

Central Inventory System (CIS) use should be reviewed.
We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using CIS should:

- Verify only accurate and authorized data are entered into CIS. It is the agency's responsibility to ensure only properly authorized transactions are entered into the system.

- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to CIS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.

Central Time and Attendance System (CTAS) use should be reviewed.
We recommend user agencies review their bills to ensure they are billed properly for the systems they use. In addition, to ensure that controls are fully implemented and functional at the agency level, agencies using CTAS should:

- Verify only accurate and authorized data are entered into CTAS. It is the agency's responsibility to ensure only properly authorized transactions are entered into the system.
- Review the effectiveness of critical manual controls, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- Regularly review the users and user groups with access to CTAS to ensure access authorized is appropriate.
- Establish policies and procedures for the administration of user IDs.
- Regularly review those authorized to pick up timekeeping reports, and inform appropriate CTAS personnel of changes timely.

Note: Additional information is available to assist user agencies and their internal and external auditors in the review of these complementary controls or other pertinent controls. Please feel free to contact the Office at 217-782-6046 or auditor@mail.state.il.us.

This Page Intentionally Left Blank

APPENDIX B

LIST OF USER AGENCIES

1. Board of Higher Education
2. Capital Development Board
3. Chicago State University
4. Commission on Government Forecasting and Accountability
5. Court of Claims
6. Department of Agriculture
7. Department of Central Management Services
8. Department of Children and Family Services
9. Department of Commerce and Economic Opportunity
10. Department of Corrections
11. Department of Employment Security
12. Department of Financial and Professional Regulation
13. Department of Healthcare and Family Services
14. Department of Human Rights
15. Department of Human Services
16. Department of Insurance
17. Department of Juvenile Justice
18. Department of Labor
19. Department of Military Affairs
20. Department of Natural Resources
21. Department of Public Health
22. Department of Revenue
23. Department of Transportation
24. Department of Veterans' Affairs
25. Department on Aging
26. East St. Louis Financial Advisory Authority
27. Eastern Illinois University
28. Emergency Management Agency
29. Environmental Protection Agency
30. Executive Ethics Commission
31. General Assembly Retirement System
32. Governors State University
33. Guardianship and Advocacy Commission
34. Historic Preservation Agency
35. House of Representatives
36. Human Rights Commission
37. Illinois Arts Council
38. Illinois Civil Service Commission
39. Illinois Commerce Commission
40. Illinois Community College Board
41. Illinois Council on Developmental Disabilities
42. Illinois Criminal Justice Information Authority
43. Illinois Deaf and Hard of Hearing Commission
44. Illinois Educational Labor Relations Board
45. Illinois Finance Authority
46. Illinois Gaming Board
47. Illinois Housing Development Authority
48. Illinois Labor Relations Board
49. Illinois Law Enforcement Training and Standards Board
50. Illinois Math and Science Academy
51. Illinois Office of the State's Attorneys Appellate Prosecutor

52. Illinois Power Agency
53. Illinois Prisoner Review Board
54. Illinois Procurement Policy Board
55. Illinois Racing Board
56. Illinois State Board of Investment
57. Illinois State Police
58. Illinois State Toll Highway Authority
59. Illinois State University
60. Illinois Student Assistance Commission
61. Illinois Violence Prevention Authority
62. Illinois Workers’ Compensation Commission
63. Joint Committee on Administrative Rules
64. Judges’ Retirement System
65. Judicial Inquiry Board
66. Legislative Audit Commission
67. Legislative Ethics Commission
68. Legislative Information System
69. Legislative Printing Unit
70. Legislative Reference Bureau
71. Legislative Research Unit
72. Northeastern Illinois University
73. Northern Illinois University
74. Office of Management and Budget
75. Office of the Architect of the Capitol
76. Office of the Attorney General
77. Office of the Auditor General
78. Office of the Comptroller
79. Office of the Executive Inspector General
80. Office of the Governor
81. Office of the Lieutenant Governor
82. Office of the Secretary of State
83. Office of the State Appellate Defender
84. Office of the State Fire Marshal
85. Office of the Treasurer
86. Property Tax Appeal Board
87. Senate Operations
88. Sex Offender Management Board
89. Southern Illinois University
90. State Board of Education
91. State Board of Elections
92. State Employees' Retirement System
93. State of Illinois Comprehensive Health Insurance Board
94. State Police Merit Board
95. State Universities Civil Service System
96. State Universities Retirement System
97. Supreme Court of Illinois
98. Teachers' Retirement System of the State of Illinois
99. University of Illinois
100. Western Illinois University

APPENDIX C

IDENTIFIED DESCRIPTION OF CONTROL DEFICIENCIES

The Department's Description of Control identified several controls that were not accurate based on test work performed.

The following table is a summary of specific deficiencies noted in the Department's Description of Controls (pages 5 to 33).

Department's Description of Control	Test Results	Report Page
Vendor Management		
The Department follows the Department's Fiscal Operating Policies and Procedures Guidelines established by BOSSAP.	Per Vendor Management staff, they did not utilize any specific sections of the Fiscal Operating Policies and Procedures Guidelines.	54
Service Reporting and Service Delivery and Implementation		
The BCCS Service Catalog is used to define the level of IT service a customer can expect for defined services.	The BCCS Service Catalog did not identify or define the level of IT service a user would expect for the defined services.	55
Security Administration		
RACF violations for BCCS staff are reviewed on an ongoing basis. Violation reports are provided to the individual responsible, requesting an explanation of the violation. These explanations are then reviewed for reasonableness.	We noted the Department had run the violation report for December 4,2009; however, there was no indication of the request, receipt, or review of violations expectations as outlined in the Description of Control.	97
Network Services		
To ensure the networks are appropriately configured, the Department: • Has established standards. • Created configuration templates for core and distribution routers. • Utilized Cisco Advanced Services quarterly reports.	The Department had not established standards.	143
LAN Application Development		
Changes or enhancements to existing LAN Applications are tracked and authorized via Service Requests submitted through the Service Request Registration System (SRRS) or via an Enterprise Service Request (ESR) submitted through Remedy Change Management.	We reviewed five "change" requests, noting none had an ESR attached as indicated in the Description of Control.	154
Accounting Information System		
AIS interfaces with the Illinois Governmental Purchasing System (IGPS), the Accounts Receivable Posting System (ARPS), the Central Inventory System (CIS) and the Central Payroll System (CPS).	Per Department staff, the Central Inventory System did not interface with AIS.	165

APPENDIX D

ACRONYM GLOSSARY

ACL – Access Control List

ACS – Automated Cartridge System

AGR – Department of Agriculture

AIM – Acquisition and Inventory Management

AIS – Accounting Information System

AOC – Automated Operations Control

AR – Agency Relations

ARB – Architecture Rationalization Board

ARPS – Accounts Receivable Posting System

ASD – Application System Development

BCCS – Bureau of Communication and Computer Services

BOPM – Bureau of Property Management

BOSSAP – Bureau of Strategic Sourcing and Procurement

BRM – Business Reference Model

Bureau – Bureau of Communication and Computer Services

CA – Computer Associates

CAC – Change Advisory Council

CCF – Central Computer Facility

CDMA – Code Division Multiple Access

CICS – Customer Information Control System

CIO – Chief Information Officer

CIS – Central Inventory System

CMC – Customer Management Center

CMS – Central Management Services

CPO – Chief Procurement Officer

CPU – Central Processing Unit

CPS – Central Payroll System

CRF – Communication Revolving Fund

CSC – Communications Solution Center

CSD – CICS System Definition File

CTAS – Central Time and Attendance System

CTI – Category, Type and Item

DASD – Direct Access Storage Device

DB2 – DataBase 2

DCEO – Department of Commerce and Economic Opportunity

DCMS – Department of Central Management Services

Department – Department of Central Management Services

DFPR – Department of Financial and Professional Regulation

DES – Department of Employment Security

DHS – Department of Human Services

DNR – Department of Natural Resources

DNS – Domain Name Service

DP – Data Processing

DPH – Department of Public Health

EA&S – Enterprise Architecture and Strategy

EBAS – Enterprise Business Application Services

EMS – Expense Management System

ENS – Enterprise Network Services

EPA – Illinois Environmental Protection Agency

EPM – Enterprise Program Management

EPMO – Enterprise Program Management Office

EPOS – Enterprise Production Operation Services

ESB – Enterprise Storage Backup

ESR – Enterprise Service Request

EUC – End User Computing

FCIAA – Fiscal Control and Internal Auditing Act

FIPS – Federal Information Processing Standards

FY – Fiscal Year

GIMS – Transaction Type for the Information Management System

GRF – General Revenue Fund

HFS – Department of Health and Family Services

HIPAA – Health Insurance Portability and Accountability Act

HMC – Hardware Management Console

HSM – Hierarchical Storage Management

H/V – Hirsch Velocity

IBM – International Business Machines

ICN – Illinois Century Network

ID – Identification

IDOT – Illinois Department of Transportation

IEMA – Illinois Emergency Management Agency

IFB – Invitation for Bid

IGPS – Illinois Governmental Purchasing System

ILCS – Illinois Compiled Statutes

IMS – Information Management System

INFOMAN – Information Management System

I/O – Input/Output

IOC – Illinois Office of the Comptroller

IOIA – Illinois Office of Internal Audit

IQAM – Infrastructure Quality Assurance & Methods

ISD – Information Services Division

ISP – Illinois State Police

IT – Information Technology

IITAA – Illinois Information Technology Accessibility Act

ITG – Information Technology Governance

IWIN – Illinois Wireless Information Network

JCL – Job Control Language

LAN – Local Area Network

LSM – Library Storage Manager

M&P – Methods and Procedures

MAC – Moves/Adds and Changes

MAS90 – Name of application utilized by Business Services

MPLS – MultiProtocol Label Switching

NOMAD – Name of application utilized on VM

PC – Personal Computer

PCF – Property Control Form

PIM – Program Information Management or Personal Information Management

PIR – Post-Implementation review

PKI – Public Key Infrastructure

POP – Point Of Presence

PSR – Paging Service Request or Product Standardization Request

QA – Quality Assurance

RACF – Resource Access Control Facility

RAD – Rapid Application Development

REV – Department of Revenue

RFI – Request for Information

RFP – Request for Proposal

RM – Risk Management

RMF – Resource Monitoring Facility

RTC – Regional Technology Center

RTO – Recovery Time Objective

SAMS – Statewide Accounting Management System

SMF – System Management Facility

SMS – System Management Storage

SNA – Systems Network Architecture

SPO – State Procurement Officer

SQL – Structured Query Language

SR – Service Request

SRRS – Service Request Registration System

SSL – Secure Socket Level

SSRF – Statistical Services Revolving Fund

SRRS – Service Request Registration System

SYSLOG – System Generated Log

TCP/IP – Transmission Control Protocol/Internet Protocol

TDR – Telecommunications Data/Intercity Service Request

TGR – Terminal Generation Request

TGS – Tape Generating System

TIMS – Transaction type for the Information Management System

TMS – Tape Management System

TRM – Technical Reference Model

TSO – Time Sharing Option

TSR – Telecommunications Service Request

TTS – Transient Tape System

UPS – Uninterruptible Power Supply

URL – Universal Resource Locator

VOIP – Voice Over Internet Protocol

VOTS – Voice Teleconferencing Services

WAN – Wide Area Network

WCS – Warehouse Control System

WSR – Wireless Service Request

z/OS – Zero Downtime Operating System

z/VM – Zero Downtime Virtual Machine