STATE OF ILLINOIS

OFFICE OF THE AUDITOR GENERAL

SERVICE ORGANIZATION CONTROL REPORT

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES BUREAU OF COMMUNICATIONS & COMPUTER SERVICES

JULY 2013

WILLIAM G. HOLLAND

AUDITOR GENERAL

SERVICE ORGANIZATION CONTROL REPORT

Department of Central Management Services
Bureau of Communications and Computer Services

July 2013

TABLE OF CONTENTS

Management of the Department of Central Management Services' Assertion Regarding the State of Illinois Information Technology Environment 'System' 1

Independent Service Auditor's Report 5

Description of the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Information Technology Environment 'System' 11

- Background 11
- Components of the System 11
- Infrastructure 11
- Software 12
- People 14
- Procedures 17
- Data 18

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring of Controls 19

- Control Environment 19
- Security Policies 20
- Risk Assessment Process 23
- Information and Communication Systems 24
- Monitoring Controls 24

Boundaries of the System 25

Trust Services Criteria and Related Controls 26

Complementary User-Entity Controls 27

Description of Test of Controls and Results Thereof 29

- Trust Services - Security Principle, Criteria, Related Controls and Test of Controls 30
- Trust Services - Availability Principle, Criteria, Related Controls and Test of Controls 47
- Trust Services - Processing Integrity Principle, Criteria, Related Controls and Test of Controls 67

Other Information Provided by the Department that is Not Covered by the Service Auditor's Report 93

- Department's Corrective Action Plan 94
- Department's Analysis of Staffing Trends 100
- Listing of User Agencies of the State of Illinois Information Technology Environment 101
- Listing of User Agencies of the Accounting Information System 103
- Listing of User Agencies of the Central Inventory System 105
- Listing of User Agencies of the Central Payroll System 106
- Listing of User Agencies of the Central Time and Attendance System 107
- Listing of User Agencies of the eTime System 108
- Listing of Security Software Proxy Agencies 109

Acronym Glossary 111

CMS

ILLINOIS Pat Quinn, Governor
DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
Malcolm Weems, Director

July 2, 2013

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

RE: Management of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Information Technology Environment 'System' for the Period July 1, 2012 to June 30, 2013

Dear Mr. Holland:

We have prepared the attached description titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services, State of Illinois Information Technology Environment 'System' Throughout the Period July 1, 2012 to June 30, 2013" (the description), based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.34–.35 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the State of Illinois Information Technology Environment, particularly system controls intended to meet the criteria for the security, availability, and processing integrity principles set forth in TSP section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the State of Illinois Information Technology Environment 'System' throughout the period July 1, 2012 to June 30, 2013 based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided

(2) The components of the system used to provide the services, which are the following:

- *Infrastructure.* The physical and hardware components of a system (facilities, equipment, and networks).
- *Software.* The programs and operating software of a system (systems, applications, and utilities).
- *People.* The personnel involved in the operation and use of a system (developers, operators, users, and managers).
- *Procedures.* The automated and manual procedures involved in the operation of a system.
- *Data.* The information used and supported by a system (transaction streams, files, databases, and tables).

(3) The boundaries or aspects of the system covered by the description

(4) How the system captures and addresses significant events and conditions

(5) The process used to prepare and deliver reports and other information to user entities and other parties

(6) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system

(7) Any applicable trust services criteria that are not addressed by a control at the Department of Central Management Services, Bureau of Communications and Computer Services and the reasons therefore

(8) Other aspects of the Department of Central Management Services, Bureau of Communications and Computer Services control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria

(9) Relevant details of changes to the Department of Central Management Services, Bureau of Communications and Computer Services, State of Illinois Information Technology Environment during the period covered by the description

ii. The description does not omit or distort information relevant to the State of Illinois Information Technology Environment 'System' while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. the controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

Sincerely,

Rich Fetter

Rich Fetter, Deputy Director
Illinois Department of Central Management Services
Bureau of Communication and Computer Services

This page intentionally left blank

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

INDEPENDENT SERVICE AUDITOR'S REPORT

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

Scope
We have examined the attached Description titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' State of Illinois Information Technology Environment 'System'" for the period July 1, 2012 to June 30, 2013 (the Description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the security, availability, and processing integrity principles set forth in <u>TSP Section 100,</u> *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period July 1, 2012 to June 30, 2013. The Description indicates that certain applicable trust services criteria specified in the Description can be achieved only if complementary user-entity controls contemplated in the design of the Department of Central Management Services, Bureau of Communications and Computer Services' controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

Service organization's responsibilities
The Department of Central Management Services, Bureau of Communications and Computer Services has provided the attached assertion titled "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Information Technology Environment 'System'" for the period July 1, 2012 to June 30, 2013, which is based on the criteria identified in management's assertion. The Department of Central Management Services, Bureau of Communications and Computer Services is responsible for (1) preparing the Description and assertion; (2) the completeness, accuracy, and method of presentation of both the Description and assertion; (3) providing the services covered by the Description; (4) specifying the controls that meet the applicable trust

services criteria and stating them in the Description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the Description based on the Description criteria set forth in the Department of Central Management Services, Bureau of Communications and Computer Services' assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in Government Auditing Standards issued by the Comptroller General. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is fairly presented based on the Description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period July 1, 2012 to June 30, 2013.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the Description based on the Description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the Description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations
Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion
The Department of Central Management Services, Bureau of Communications and Computer Services states in the Description of System the processes outlined in the Application Lifecycle Management Manual are used to control changes related to the applications maintained by the Department (page 13). However, as noted on pages 49, 69, 85 and 86 of the Description of Test of Controls and Results Thereof, a suitable change management process was not in place from July 1, 2012 to November 30, 2012. In addition, for changes after November 30, 2012: 10 out of 10 change tickets did not comply with the Application Lifecycle Management Manual, and 55 out of 77 change tasks did not have appropriate documentation to support the move to production. Thus, controls over changes to applications were not operating effectively

throughout the period July 1, 2012 to June 30, 2013. This control deficiency resulted in not meeting the criterion "Testing, evaluating, and authorizing system components before implementation", "Procedures exist to maintain system components, including configurations consistent with the defined system processing integrity and related security policies", and "Procedures exist to provide that only authorized, tested and documented changes are made to the system."

Additionally, the Department of Central Management Services, Bureau of Communications and Computer Services states in the Description of System, in order for password resets to Department and proxy agency user profiles to be completed, an email request to the Help Desk is to be submitted or by accessing the Department's Identity Management website. However, as noted on pages 37, 58, and 77 of the Description of Tests of Controls and Results Thereof, the password resets were completed via direct phone call or email to the Department's Coordinator, at which time the Department's Coordinator would reset the password. Thus, the control over the reset of mainframe passwords was not operating effectively throughout the period July 1, 2012 to June 30, 2013. This control deficiency resulted in not meeting the criterion "The process to make changes and updates to user profiles."

In addition, the Department of Central Management Services, Bureau of Communications and Computer Services states in the Description of System, Department staff have been assigned responsibility for monitoring and ensuring compliance with security policies. According to the security policies, the Department and security personnel were responsible for the monitoring, auditing, tracking, and for the validation of compliance with the policies and procedures. Additionally, they were responsible for investigating violations of laws, policies, and procedures. However, as noted on pages 43, 63, and 82 of the Description of Tests of Controls and Results Thereof, the security policies did not define who security personnel were and we were unable to determine who within the Department was responsible. Thus, the control over the monitoring of noncompliance with security policies was not operating effectively throughout the period July 1, 2012 to June 30, 2013. This control deficiency resulted in not meeting the criterion "Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis."

The Department of Central Management Services, Bureau of Communications and Computer Services also states in the Description of System, risk assessments are to be preformed periodically and, as security threats are identified, they are to be assessed. However, as noted on pages 35, 53, and 73 of the Description of Tests of Controls and Results Thereof, formal risk assessments, threat analysis, and treatment plans based on the IT Risk Assessment Framework had not been performed. Thus, the control over risk assessments was not operating effectively throughout the period July 1, 2012 to June 30, 2013. This control deficiency resulted in not meeting the criterion "Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats."

In our opinion, except for the matters referred to in the four preceding paragraphs, based on the Description criteria identified in the Department of Central Management Services, Bureau of

Communications and Computer Services' assertion and the applicable trust services criteria, in all material respects

> *a.* the Description fairly presents the system that was designed and implemented throughout the period July 1, 2012 to June 30, 2013.
>
> *b.* the controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period July 1, 2012 to June 30, 2013, and user entities applied the complementary user-entity controls contemplated in the design of the Department of Central Management Services, Bureau of Communications and Computer Services' controls throughout the period July 1, 2012 to June 30, 2013.
>
> *c.* the controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period July 1, 2012 to June 30, 2013.

Description of tests of controls
The specific controls we tested and the nature, timing, and results of our tests are presented in the section of our report titled "Description of Test of Controls and Results Thereof."

Supplementary information
The information attached to the Description titled "Other Information Provided by the Department of Central Management Services, Bureau of Communications and Computer Services That Is Not Covered by the Service Auditor's Report" describes staffing trends, user agency listings, and the Department's Corrective Action Plan. It is presented by the management of the Department of Central Management Services, Bureau of Communications and Computer Services to provide additional information and is not a part of the Department of Central Management Services, Bureau of Communications and Computer Services' Description of the State of Illinois Information Technology Environment made available to user entities during the period from July 1, 2012 to June 30, 2013. Information about the Department of Central Management Services, Bureau of Communications and Computer Services' staffing issues, user listings, and Department's Corrective Action Plan have not been subjected to the procedures applied in the examination of the Description of the State of Illinois Information Technology Environment and the suitability of the design and operating effectiveness of controls to meet the related criteria stated in the Description of the State of Illinois Information Technology Environment, and, accordingly, we express no opinion on it.

Intended use
This report and the Description of Tests of Controls and Results Thereof are intended solely for the information and use of the Department of Central Management Services, Bureau of Communications and Computer Services' user entities of the "Description of the Department of Central Management Services, Bureau of Communications and Computer Services' Assertion Regarding the State of Illinois Information Technology Environment" during some or all of the period July 1, 2012 to June 30, 2013, the Auditor General, the General Assembly, the Legislative

Audit Commission, the Governor, and independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

However, this report is a matter of public record and the distribution is not limited.

William J. Sampias, CISA
Director, Information Systems Audits

Mary Kathryn Lovejoy, CPA, CISA
Information Systems Audit Manager

July 2, 2013
Springfield, Illinois

This page intentionally left blank

DESCRIPTION OF THE DEPARTMENT OF CENTRAL MANAGEMENT SERVICES BUREAU OF COMMUNICATIONS AND COMPUTER SERVICES' STATE OF ILLINOIS INFORMATION TECHNOLOGY ENVIRONMENT 'SYSTEM' THROUGHOUT THE PERIOD JULY 1, 2012 TO JUNE 30, 2013

Background

The Department of Central Management Services Bureau of Communications 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).

The Bureau of Communications and Computer Services:

- Manages the planning, procurement, maintenance, and delivery of voice, data, wireless, video, Internet, and telecommunications services to all state government agencies, boards, commissions, and state supported institutions of higher education in Illinois, as well as other governmental and some non-governmental entities.
- Operates the Central Computer Facility, as well as other facilities, which provides mainframe processing systems and support for most state agencies.
- Maintains applications that state government agencies, boards, and commissions may utilize to meet their financial requirements.

Components of the System

The System is comprised of the following components:

- Infrastructure (facilities, equipment, and networks),
- Software (systems, applications, and utilities),
- Data (transaction streams, files, databases, and tables).
- People (developers, operators, users, and mangers), and
- Procedures (automated and manual),

The following sections of this description define each of these five components comprising the System.

Infrastructure

The State of Illinois Information Technology Environment is housed at the Central Computer Facility (CCF), Communications Building and additional facilities throughout the State. Residing at the CCF are the supporting mainframe operating system platforms, networking components (firewalls, routers, switches), and data storage devices.

The Department is responsible for supporting and maintaining three mainframe units, which are configured into 12 production systems and 9 test systems. In addition, the Department is responsible for installing, maintaining and managing the Illinois Century Network, including approximately 3,800 circuits, egress circuits, routers, firewall, switches, fifteen Point-of-

Presence sites, and various monitoring tools. The Department also maintains the Enterprise Virtual Private Network solution which allows the Department and user agencies to connect remotely to resources. The Department has configured the network in a redundant manner.

The Department maintains Direct Access Storage Devices (DASD), Disk Library for Mainframe (DLM), and tape drives for reading and writing tapes in order to provide backup and storage services.

The Department makes available encryption technologies and access gateways for the transmission of sensitive or confidential information.

Software

The Department provides a mainframe hosting environment for user agencies. The mainframe hosting services include development, testing and acceptance environments. The mainframe operating system software includes:

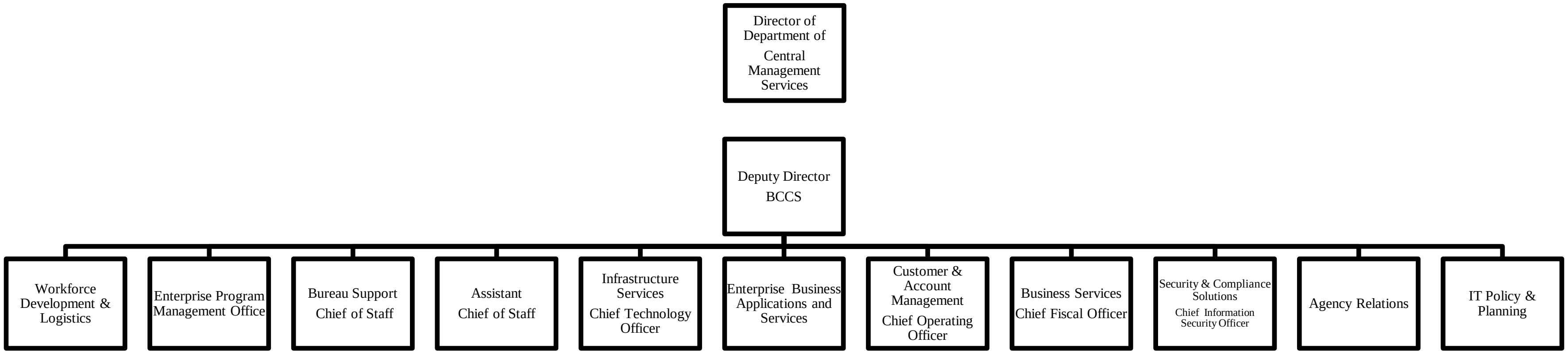
- The primary operating system is Zero Downtime Operating System (z/OS). z/OS is a complex operating system used on mainframes and functions as the system software that controls the initiation and processing of work within the computer. The System Management Facility (SMF) records the activity within the operating system.
- z/Virtual Machine (z/VM) is a time-sharing, interactive, multi-programming operating system for mainframes. The major subsystem supported in z/VM is NOMAD, which is business intelligence software for enterprise reporting and rapid application development.
- The Customer Information Control System (CICS) is a software product that enables online transaction processing. CICS allows numerous transaction types, entered from multiple terminals, to be processed concurrently by user written application programs. CICS acts as an interface between the operating system and application programs.
- DataBase 2 (DB2) is a relational database management system for z/OS environments, which the Department makes available. The Department has established more than 10 subsystems.
- Information Management System (IMS), which is an online database software subsystem, is used as the control architecture under which online database system applications process. An IMS system is capable of running many different applications within a single definition of one or more “Message Processing Region” and one “Control Region”. The IMS applications can access IMS, DB2 and CICS data files. Users control their own TIMS and GIMS RACF definitions.

In addition, the Department maintains applications, which all State agencies, boards, and commissions may utilize:

- The Accounting Information System (AIS) is an automated expenditure control and invoice voucher processing system. Appropriation, obligation, cash and vendor processing functions support the invoice processing. AIS allocates invoice amounts into sub accounts and allows users to track cost centers. Vouchers are created in AIS according to the Comptroller's Statewide Accounting Management System (SAMS) procedures.
- The Central Inventory System (CIS) is an automated asset inventory control system, which also allows the user agency to track depreciation. 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.
- The Central Payroll System (CPS) provides assistance in preparing payrolls for state agencies. CPS enables State agencies to maintain automated pay records and generates a file that is submitted to the Comptroller's Office for the production of payroll warrants.
- The Central Time and Attendance System (CTAS) is an online system used to maintain "available benefit time". CTAS provides for attendance information to be recorded using either the positive or exception method.
- eTime is a web-based application used to maintain employee timekeeping records; leave and overtime requests, daily time reports, and time balances. The eTime nightly batch process updates CTAS.

People

The Department of Central Management Services, Bureau of Communications and Computer Services is divided into several divisions in order to provide services to its users.


Director of Department of Central Management Services
Deputy Director BCCS
Workforce Development & Logistics
Enterprise Program Management Office
Bureau Support Chief of Staff
Assistant Chief of Staff
Infrastructure Services Chief Technology Officer
Enterprise Business Applications and Services
Customer & Account Management Chief Operating Officer
Business Services Chief Fiscal Officer
Security & Compliance Solutions Chief Information Security Officer
Agency Relations
IT Policy & Planning

Deputy Director

The Deputy Director of the Bureau of Communications and Computer services is responsible for the overall management of all Information Technology and Telecommunication functions, which includes services provided to all state agencies as well as other Illinois government entities. The Deputy Director works with Department senior management, the Governor's Office and the State Chief Information Officer to develop policies, priorities and plans for statewide Information Technology and Telecommunication programs. The Deputy Director is responsible for the follow teams:

Chief Operating Officer

The Chief Operating Officer serves as a policy formulating administrator in planning, directing, implementing and administering the Customer and Account Management group. The Customer and Account Management is the single point of contact for user service requests, service provisioning, and incident management.

- Customer Service Center (CSC)
  The CSC serves as the central point of contact for telecommunications and information technology users. The CSC serves as a Help Desk to handle process and manage incidents and requests for services.

- Communications Management Center (CMC)
  The CMC is responsible for all network trouble resolutions, surveillance and ongoing technical support. The CMC is operational 24x7, and handles after hours calls of the Customer Service Center (CSC).

- Field Operations / Regional Technology Centers (RTC)
  Field Operations is responsible for maintaining nine Regional Technology Centers located throughout the State and assisting Network Services in maintaining Illinois Century Network Point-of-Presence (POP) sites throughout the State.

- Network Services
  Network Services is responsible for management and oversight of the Illinois Century Network (ICN), the Illinois Wireless Information Network, and all engineering responsibilities related to State of Illinois telecommunications services.

  - Network Operations is responsible for installing, maintaining and managing the ICN Backbone including backbone circuits, egress circuits, routers, firewalls, switches, fifteen Point-of-Presence (POP) sites, WAN monitoring tools and WAN services. Additionally, Network Operations provides tier III network support to other staff within Network Services.

  - Enterprise Network Support is responsible for design and support of State agencies network access. Responsibilities include installation and support of access routers, WAN switches, VOIP, video conferencing, fiber, DNS, and Internet. Network Integration also performs tier III technical support for the CMC and directly to state agencies.

Chief of Staff

The Chief of Staff serves as advisor to the Deputy Director on strategic, operational and problem resolution issues, serves as primary resource between the Deputy Director and senior management, and performs special projects related to Bureau operations.

Workforce Development and Logistics

The Workforce Development and Logistics coordinates and facilitates internal personnel paperwork, workforce training, development and implementation, and workforce logistics for the Bureau.

Enterprise Program Management Office

The Enterprise Program Management Office (EPMO) develops and implements enterprise project management policies, processes, and services as well as other related project management support activities. The EPMO directly manages large, complex (Tier 3) projects, and oversees all other projects that meet the criteria for IT Governance (Tier 2).

Chief Technology Officer

The Chief Technology Officer oversees the Infrastructure Services Division in order to provide continuous oversight, operation, and support of the State’s Information Technology infrastructure. The Infrastructure Services Division is divided into several teams:

- Data Center Operations

  Mainframe Services is responsible for the mainframe operating systems, database systems, and software installation, maintenance, and support function/services.

  Enterprise Storage and Backup is responsible for the oversight and management of the storage and backup systems across all platforms.

- Enterprise Production/Operations

  Library Services is responsible for media initiation, inventory, tracking, lifecycle management, and business continuity media management.

  Production Control is responsible for computer job scheduling and monitoring.

  Command Center Operations is responsible for providing continuous monitoring and operation of the Department's computing resources to ensure availability, performance, and support response necessary to sustain user business demands.

- LAN Services

  LAN Services is responsible for entering rules into the firewalls and monitoring security violations. Additionally, this group is responsible for consolidated and managed agencies LAN networks, which includes: firewalls, routers, switches, hubs, IDS and wireless switches.

Enterprise Business Applications and Services

The Enterprise Business Applications and Services (EBAS) Division is responsible for the development and maintenance of the applications, which are available for use by user agencies.

The Division is responsible for the maintenance and support of the applications used by agencies, Accounting Information System (AIS), Central Payroll System (CPS), Central Inventory System (CIS), Central Time and Attendance System (CTAS), and eTime.

Agency Relations

Agency Relations Liaisons (ARL) establishes and maintains user relationships, and serves as an advocate and facilitator. Agency Relations primary focus is user relationship management, event coordination and marketing and communications.

Chief Fiscal Officer

The Chief Fiscal Officer oversees the management of the fiscal operations for the Bureau. This position administers the Communications Revolving Fund (CRF) the Statistical Services Revolving Fund (SSRF), and the General Revenue Fund (GRF) for educational technology (Illinois Century Network).

IT Policy and Planning

The IT Policy and Planning Division performs senior-level project management and serves as a policy and planning advisor to the Deputy Director.

Chief Information Security Officer

The Chief Information Security Officer serves as a policy making official responsible for the policy development, planning, implementation, and administration of the Security and Compliance Solutions division. The Chief Information Security Officer is responsible for overseeing and implementing the sensitive and confidential Information Technology security program for agencies, boards and commissions under the jurisdiction of the Governor.

- Security and Compliance Solutions

  Security and Compliance Solutions has the following responsibilities:
  - Providing the IT security program statewide to agencies
  - Communicating security principles through issuance of policy and hosting education opportunities,
  - Alerting users to known occurrences or potential imminent threats that could cause risk to cyber resources,
  - Notifying the applicable management of non-compliance/violations of the systems security,
  - Developing and assessing risk associated with specific business information systems and developing appropriate remediation plans,
  - Conducting security testing of the infrastructure, and
  - Developing and maintaining the statewide disaster recovery services for the State's Information Technology infrastructure.

Procedures

The Department has developed and communicated to Department staff security procedures over the following areas:

- Data classification,
- Authorization, changes and termination of information system access,

- System security administration,
- Network operations,
- Maintenance and support of systems and necessary backups and off site storage,
- Maintenance of restricted access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices, and
- Incident response (physical and logical).

Data

The Department provides applications (AIS, CIS, CPS, CTAS, and eTime) which user agencies may utilize. The origination, input, accuracy and output of information is the responsibility of the user agencies. Each transaction entered is assigned an identifying number.

User manuals and reference documents provide guidance to users on data entry, edits, and error correction procedures. Additionally, the manuals and reference documents outline various reports which the user agency may produce.

Distribution of digital output is restricted to authorized users through the management of system software tools or online viewing software. Distribution of hardcopy output is restricted through physical and manual controls. Hardcopy output is printed at a secure facility with security guards. Upon request for pick up, the individual must identify themselves and be verified against an authorization listing.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING OF CONTROLS

Control Environment

Management Philosophy

The Department of Central Management Services, Bureau of Communications and Computer Services' control environment reflects the values of the Department regarding the importance of security over the infrastructure and user's data and information. The Bureau of Communications and Computer Services' management meets weekly to ensure the importance of security is passably communicated to all levels within the Department. The Department has established security policies and procedures, which have been communicated to staff and users, via the website. In designing its controls, the Department has taken into consideration the relevance of the control in order to meet the relevant trust criteria.

Security Management

The Chief Information Security Officer, along with Department staff is responsible for the development and management of security over the State of Illinois Information Technology Environment. The Chief Information Security Officer is responsible for the policy development, planning, implementation, and administration. The security policies are reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel and the Chief Information Security Officer.

The application managers are responsible for the development and management of the applicable user manuals.

Department staff is assigned the responsibility for the monitoring and ensuring compliance with the security policies.

New Department staff is required to sign a statement signifying that they will comply with the security policies. Additionally, Department staff reconfirms their compliance with the security policies through annual security awareness training. Contractors are required to take the annual security awareness training and certify they will comply with security policies.

The Department adheres to the State's hiring procedures for the hiring of staff. The Department's position descriptions, which define job requirements, are available upon request and are posted for open positions. Additionally, Department staff is notified when position descriptions are updated.

Annual performance evaluations are completed. Staff is provided training and cross training is conducted for key positions.

The Department's Security and Compliance Solutions Division participates in user groups and subscribes to services related to computer viruses.

Security Policies

The following policies and related processes identify and document the physical and logical security, availability, and processing requirements of Department staff and users:

Information Technology 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,
- Recovery Methodology,
- IT Resource Access Policy,
- Laptop Data Encryption Policy,
- Backup Retention Policy,
- Statewide CMS/BCCS Facility Access Policy, and
- IT (Information Technology) Risk Assessment Policy.

General Policies

- Change Management Policy,
- Data Breach Notification Policy,
- Action Plan for Notification of a Security Breach,
- Electronically Stored Information Retention Policy,
- IT Governance Policy,
- Mobile Device Security Policy, and
- Wireless Communication Device Policy.

User Manuals

- Accounting Information System User Manual,
- Central Inventory System User Manual,
- Central Payroll System User Manual,
- Central Time and Attendance System User Manual, and
- eTime Reference Documents.

Personnel Security

Background checks are performed on all Department staff requiring access to Department resources. Department employees are subject to the Department's procedures/process for accessing systems. Additionally, Department staff and users are instructed to report security incidents/issues to the Department's Help Desk or a supervisor.

Physical Security

The Central Computing Facility (CCF) and Communications Building, which house the State of Illinois Information Technology Infrastructure, provide the following features:

- The CCF and the Communications Building maintain high security standards for building access and perimeter monitoring. The interior and exterior of the facilities are monitored and access enforced by card key access. In order to obtain a card key, an ID Badge Request Form is to be completed and approved by the authorized manager. In addition, a valid ID must be presented.
- Visitors are required to be escorted, in addition to signing in and out.
- The facilities are guarded by security guards 24x7. Video surveillance is used to monitor the CCF and the Communications Building and is monitored by the security guards.
- The fire detection devices are monitored by the Command Center. The monitoring system informs the Command Center of the specific alarm. The CCF computer room fire suppression system is Underwriter Laboratory approved and utilizes an environmentally friendly agent; FM-200. Additionally, the CCF and the Communications Building have fire extinguishers installed throughout each facility.
- The CCF has sensors installed below the raised floor to detect water leakage.
- The CCF and the Communications Building are equipped with uninterruptible power supplies (UPS) in the event of a power failure. In the event of a power failure, the UPS would engage immediately, drawing power from the battery farm and generators.

The Department’s offsite storage facility has physical access controls in place. Additionally, only authorized Department staff are able to access the offsite storage facility.

The Department has preventive maintenance agreements in place and conducts scheduled maintenance for key system hardware components.

Change Management

The Department has implemented a formal change management process which requires tracking, approval, testing, and backout plans for system changes. The Remedy Change Control System is used to create, review, approve, and track change requests.

System change requests are reviewed by the Change Management Unit. System changes to be reviewed are made available to members of the Change Advisory Council (CAC) before the meeting. In addition, the results of the meeting are made available via the ECM SharePoint site. Users have access to the ECM SharePoint site.

Emergency changes follow the defined change management process, but at an accelerated timeline.

The Application Lifecycle Management Manual outlines the requirements to implement application changes. Emergency changes to applications are to follow the Application Lifecycle Management Manual. Production moves require an approved movesheet or an Enterprise Service Request.

Changes to the applications are communicated to users via email or phone. Planned changes to applications are conducted during the scheduled maintenance window.

Standards provide guidance on the configuration and deployment of network devices. Tools are in place to assist in the deployment of and reporting on configurations.

The IT Governance process governs the acquisition of systems and technology. As part of the IT Governance process, user agencies are to classify their data in accordance with the Data Classification Policy.

System Monitoring

The Operation Center continuously monitors the operation of the computing resources to ensure availability, performance, and response necessary to sustain user business demands. The Operation Center operates 24 hours a day, 7 days a week, 365 days a year. The Department utilizes various tools to review and assess the infrastructure and vulnerabilities.

Problem Management

Department staff and users are instructed to contact the Customer Service Center (Help Desk) or their supervisor to report any and all security, availability and processing issues. Staff and users may contact the Help Desk via phone or email to report an incident. When a report is received, the Help Desk staff open a ticket in Remedy and record the incident, as well as the user name, agency, contact information and a detailed incident description. The ticket is tracked through Remedy until resolution.

Backup and Recovery

The Department provides recovery services for the mainframe infrastructure in order to minimize the risk of disrupted services or loss of resources using vendor contracted services. The recovery of the user agency applications and data are the responsibility of the user agency.

The Department maintains information on State agencies critical applications, via the Business Reference Model. State agencies are required to categorize, prioritize and define critical information. This information informs the Department of the required recovery capacity needs.

The Department has developed policies and procedures, which are tested annually, to assist with the recovery of the infrastructure.

System data is replicated daily and weekly to the Alternate Data Center. In addition, weekly backups are backed up to tape and sent to the offsite storage facility. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized staff.

The Department maintains an inventory of the backups, along with their location. An annual verification is conducted.

System Account Management

Resource Access Control Facility (RACF) security software is utilized to restrict access to defined systems, subsystems, and mainframe applications. RACF enforces the individual's accountability over data and system resources by positively verifying the individual's authority to utilize the system resource or data.

A user ID is used to identify the user along with a password to verify the user's identity. The Department maintains a log of all access attempts, which is used to monitor unauthorized access attempts and identify areas of weakness. System options and parameters are implemented to protect data and resources.

Users are required to establish their identity and authenticate to systems and applications through the use of user IDs and passwords. It is the standard practice to assign each valid user a unique and individual ID. Password configurations have been established.

Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form and submit via a Remedy Enterprise Service Request. The Mainframe Application Access Request Form indicates the access required and proper approval. Password resets to Department and proxy agency user profiles are to be completed by submitting an email request to the Help Desk or by accessing the Department's Identity Management website.

Bi-monthly the Department's RACF Coordinator receives a separation report documenting separations. The Department's RACF Coordinator will review and revokes the user's ID. Bi-annually, the Department's RACF Coordinator will send all agencies a listing of their respective users, requesting the agency to review for accuracy, note any modifications, and return to the Department.

Network Services requires manager review and approval of new access rights. LAN Services utilized the LAN Services Access Authorization Form in order for staff to obtain access rights. Network Services is notified by Personnel of changes in an individual's employment status and makes changes to user's access rights accordingly. Changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization Form.

Operating system configuration defaults are restricted to authorized personnel through logical access controls. Master passwords are maintained in an encrypted database. Authentication servers are utilized to control access, log access attempts, and alert management.

Risk Assessment Process

The Security and Compliance Solutions Division assess security risk on an ongoing basis. As security threats are identified, the specific risk is assessed. Additionally, regular meetings with management and users are held to discuss security and risk issues.

Department management considers technological developments, and laws and regulations during the planning process. Additionally, management conducts meetings with user agencies to determine their future needs.

Information and Communication Systems

The Department's security policies, website, and user manuals assist in ensuring Department staff and users are aware of their individual roles and responsibilities concerning the security, availability, and processing integrity over the State of Illinois Information Technology Environment. Additionally, the Department communicates security events and issues to Department staff and users via email, phone, and postings on the Department's website.

The security policies outline the responsibilities of the Department and the users:

- It was the responsibility of the users to understand the applicable policy and to follow the corresponding procedures.
- The resource custodians were responsible for understanding and adhering to the policies and for granting, reviewing, and removing access to resources.
- The Department and security personnel were responsible for the monitoring, auditing, tracking, and for the validation of compliance with the policies and procedures. Additionally, they were responsible for investigating violations of laws, policies, and procedures.

The Department has published on their website the Service Catalog, which documents the services provided, in addition to the availability of specific systems. The Service Catalog documents the commitments and obligations of the Department and users.

Monitoring Controls

The Department utilizes various tools to review and assess the infrastructure and vulnerabilities. Logs are analyzed; either manually or by automated tools, to identify trends that may have the potential to impact the Department's ability to achieve system security objectives. Security issues are addressed with management at various meetings.

BOUNDARIES OF THE SYSTEM

The Department of Central Management Services provides all state government agencies, boards, and commissions an Information Technology infrastructure in which to host their applications. The system description herein only relates to the mainframe computing environment and excludes the midrange server computing environment. The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures and data necessary to provide such services. The boundaries of the Department's system include the mainframe environment, networking components (firewalls, routers, switches), and data storage devices. The Department maintains and provides applications which are utilized by multiple agencies; Accounting Information System, Central Inventory System, Central Time and Attendance System, Central Payroll System, and eTime; however, the input and integrity of the data is the responsibility of the user and, therefore, is not within the boundaries of the system.

TRUST SERVICES CRITERIA AND RELATED CONTROLS

Although the trust services criteria and related controls are presented in Trust Services Security Principle, Availability Principle, and Processing Integrity Principal Criteria's, along with the Related Controls, and Test of Controls, they are an integral part of the State of Illinois Information Technology Environment System's description.

COMPLEMENTARY USER-ENTITY CONTROLS

The Department of Central Management Services' services were designed with the assumption that certain controls would be implemented by the user agency. The user agency controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by the user agency.

User agencies of the Department of Central Management Services, Bureau of Communications and Computer Services, State of Illinois Information Technology Environment should maintain controls to provide reasonable assurance that:

- User agencies have reviewed and adhere to the security policies located on the Department's website.
- User agencies have communicated to the Department their specific security requirements.
- User agencies have informed the Department's Help Desk in a timely manner of any security, availability, or processing issues.
- User agencies have classified their applicable applications and data based on criticality and sensitivity.
- User agencies have reviewed, updated, approved, and returned to the Department on a bi-annual basis their applicable user listings.
- User agencies are effectively utilizing security software features and perform periodic reviews of existing profiles to ensure that access rights are appropriate.
- User agencies have reviewed the effectiveness of critical manual controls over the applications, including the retention and maintenance of source documents necessary to maintain an audit trail of transactions.
- User agencies enter only accurate and authorized data into the applications.
- User agencies regularly review the users and user groups with access to the applications to ensure access authorized is appropriate.
- User agencies regularly review those authorized to pick up payroll reports, and inform appropriate Department staff of changes timely.
- User agencies retain hardcopy payroll vouchers for at least the three most current pay periods, as specified by the CPS User Manual.
- User agencies develop and maintain appropriate and viable business continuity plans, application recovery scripts, designated application information updates to the Business Reference Model, recovery exercise procedures and schedules, and ongoing communications with the Department.

This page intentionally left blank

Description of Test of Controls and Results Thereof

TRUST SERVICES - SECURITY PRINCIPLE, CRITERIA, RELATED CONTROLS AND TEST OF CONTROLS

1.0 – Policies: The entity defines and documents its policies for the security of its system.

Criteria 1.1	The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The security policies addressing logical and physical security are reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel and the Chief Information Security Officer.	Reviewed the security policies addressing logical and physical security to determine if the policies had been reviewed and approved by the Department’s Director, Deputy Director, Deputy General Counsel, and the Chief Information Security Officer.	A formal process requiring periodic reviews of policies did not exist.
The Department has implemented security policies, which are posted on the Department's website.	Reviewed the Department’s website to ascertain whether the Department’s security policies are posted on the website.	No deviations noted.

Criteria 1.2	The entity's security policies include, but may not be limited to, the following matters:	
Criteria A	Identifying and documenting the security requirements of authorized users.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The security policies identify and document the general security requirements.	Interviewed staff and reviewed security policies to determine if they identify and document general security requirements.	No deviations noted.
Criteria B	Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Data Classification and Protection Policy documents the data classification schema used to value and classify information generated, accessed, transmitted or stored.	Interviewed staff and reviewed the Data Classification and Protection Policy to determine if it documents the data classification schema used to value and classify information generated, accessed, transmitted or stored.	No deviations noted.
The IT Resource Access Policy documents the requirements for obtaining access to resources.	Interviewed staff and reviewed the IT Resource Access Policy to determine if the Policy documents the process for obtaining access to resources.	No deviations noted.
The Electronically Stored Information Retention Policy documents the retention requirements for electronic information.	Interviewed staff and reviewed the Electronically Stored Information Retention Policy to determine if the Policy documents the retention requirements of electronic information.	No deviations noted.
The General Security For Statewide IT Resources Policy documents the destruction requirements.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy to determine if it documents destruction requirements.	No deviations noted.

Criteria C	Assessing risks on a periodic basis.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The IT Risk Assessment Policy documents the requirements for assessing risk.	Interviewed staff and reviewed the IT Risk Assessment Policy to determine if it documents the requirements for assessing risk.	No deviations noted.
Criteria D	Preventing unauthorized access.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The IT Resource Access Policy documents controls for preventing unauthorized access.	Interviewed staff and reviewed the IT Resource Access Policy to determine if the Policy documents the process for obtaining access to resources.	The Policy did not include specific requirements or procedures for requesting, modifying, approving, or periodically reviewing user access rights.
Criteria E	Adding new users, modifying the access levels of existing users, and removing users who no longer need access.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the Statewide CMS/BCCS Facility Access Policy documents the requirements for granting, assigning and revoking user access.	Interviewed staff and reviewed the IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the Statewide CMS/BCCS Facility Access Policy to determine if the policies document the requirements for granting, assigning and revoking user access.	The IT Resource Access Policy and the General Security For Statewide IT Resources Policy did not include specific requirements or procedures for requesting, modifying, approving, or revoking user access rights. The CMS/BCCS Facility Access Policy did not address requirements for modifying physical access rights.

Criteria F Assigning responsibility and accountability for system security.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the General Security For Statewide Network Resources Policy document the responsibilities and accountability of system security.	Interviewed staff and reviewed the IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the General Security For Statewide Network Resources Policy to determine if the policies document the responsibility and accountability of system security.	No deviations noted.
Criteria G Assigning responsibility and accountability for system changes and maintenance.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Change Management Policy documents the responsibility and accountability of Department staff for system changes and maintenance.	Interviewed staff and reviewed the Change Management Policy to determine if the Policy documents the responsibility and accountability of Department staff for system changes and maintenance.	No deviations noted.
Criteria H Testing, evaluating, and authorizing system components before implementation.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Change Management Policy documents the process in which infrastructure changes are to follow.	Interviewed staff and reviewed the Change Management Policy to determine if it documents the process in which infrastructure changes are to follow.	Testing requirements are not addressed in the Policy.
Criteria I Addressing how complaints and requests relating to security issues are resolved.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The General Security For Statewide IT Resources Policy states users are responsible for disclosing any actions or behaviors involving a State IT resource and report on actual or suspected breaches.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy to determine if the policy document the reporting and resolution of security breaches and other incidents.	The Policy did not address the entire process for reporting and resolving security issues.
Criteria J Identifying and mitigating security breaches and other incidents.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The General Security For Statewide IT Resources Policy and the Action Plan For Notification of a Security Breach documents the identification and notification of security breaches and other incidents.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy and the Action Plan For Notification of a Security Breach to determine if they document the identification, notification, and mitigation of security breaches and other incidents.	The Policy did not address the entire process for identifying, reporting, and mitigating security issues.
Criteria K Providing for training and other resources to support its system security policies.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The General Security For Statewide IT Resources Policy documents the security awareness training requirements for Department staff.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy to determine if the Policy documents the security awareness training requirements for Department staff.	No deviations noted.

Criteria L Providing for the handling of exceptions and situations not specifically addressed in its system security policies.

Department’s Control	Auditor’s Tests of Control	Test Results
The General Security For Statewide IT Resources Policy and the General Security For Statewide Network Resources Policy indicates it is the responsibility of the users to inform the Department, in writing of any exceptions or special use requirements.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy and the General Security For Statewide Network Resources Policy to determine if the policies indicate it is the responsibility of the users to inform the Department, in writing of any exceptions or special use requirements.	No deviations noted.

Criteria M Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.

Department’s Control	Auditor’s Tests of Control	Test Results
The IT Governance Policy documents the Department and the agencies responsibilities for identifying applicable laws, regulations, and other requirements as part of the new IT projects requirements.	Interviewed staff and reviewed the IT Governance Policy to determine if the Policy documents the Department and the agencies responsibilities for identifying applicable laws, regulations, and other requirements as part of the new IT projects requirements.	No deviations noted.

Criteria N Providing for sharing information with third parties.

Department’s Control	Auditor’s Tests of Control	Test Results
The Data Classification and Protection Policy and the General Security For Statewide IT Resources Policy document requirements for the sharing of information with third parties.	Interviewed staff and reviewed the Data Classification and Protection Policy and the General Security For Statewide IT Resources Policy to determine if the policies document requirements for the sharing of information with third parties.	No deviations noted.

Criteria 1.3 Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned.

Department’s Control	Auditor’s Tests of Control	Test Results
The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of the security policies.	Reviewed the position description for the Chief Information Security Officer to ascertain whether responsibilities for the development and maintenance of security policies are included. Reviewed security policies to determine if approval by the Chief Information Security Officer is documented.	No deviations noted.

2.0 – Communications: The entity communicates its defined system security policies to responsible parties and authorized users.

Criteria 2.1 The entity has prepared an objective description of system and its boundaries and communicated such description to authorized users.

Department’s Control	Auditor’s Tests of Control	Test Results
The Department has published the Service Catalog on its website, which documents the services provided by the Department.	Interviewed staff and reviewed the Service Catalog on the website to determine if it documents the services provided by the Department.	No deviations noted.

Criteria 2.2	The security obligations of users and the entity's security commitments to users are communicated to authorized users.	
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Department's security commitments and obligations are outlined in the Service Catalog, which is posted on the Department's website.	Reviewed Service Catalog on the website to determine if security commitments and obligations are outlined.	No deviations noted.
The security obligations of Department staff are communicated via the mandatory annual security awareness training, security policies, and periodic emails.	Interviewed staff, reviewed the General Security For Statewide IT Resources Policy, the CMS Security Fundamental web tutorial, and a sample of security communications to determine if security obligations are communicated to Department staff via the mandatory annual security awareness training, security policies, and periodic emails.	No deviations noted.
New Department staff is required to sign a statement signifying that they will comply with the security policies.	Reviewed the CMS Security Fundamentals web tutorial and the training certification list to determine if new Department staff is required to sign a statement signifying that they will comply with the security policies.	No deviations noted.
Department staff reconfirms their compliance with the security policies through the annual security training.	Reviewed the CMS Security Fundamental web tutorial and the listing of Department staff annual certifications to determine if staff reconfirms their compliance with the security policies through the annual security training.	No deviations noted.
Contractors are required to take the annual security awareness training and certify they will comply with security policies.	Interviewed staff and reviewed the CMS Security Fundamental web tutorial and the listing of contractor certifications to determine if contractors are required to take the annual security awareness training and certify they will comply with security policies.	No deviations noted.
The security obligations of users are communicated in several different fashions; policies published on the web, emails, and security notices on the website.	Reviewed a sample of emails and the Department's website to determine if security obligations of users are communicated via policies, security notices, and emails.	No deviations noted.

Criteria 2.3	Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of the security policies.	Reviewed the position description for the Chief Information Security Officer to ascertain whether responsibilities for the development and maintenance of security policies are included. Reviewed security policies to determine if approval by the Chief Information Security Officer is documented.	No deviations noted.
Position descriptions have been defined and communicated to employees.	Interviewed staff and reviewed a sample of position descriptions to ascertain whether position descriptions have been defined and communicated to employees.	No deviations noted.

Criteria 2.4 The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.

Department’s Control	Auditor’s Tests of Control	Test Results
The process for users to inform the Department of possible security issues and other incidents is posted on the Department's website.	Interviewed staff and reviewed the Department’s website to determine if the process for users to inform the Department of possible security issues and other incidents is posted on the website.	Procedures had not been developed to ensure security issues and incidents identified by users are communicated to management for review and resolution.
The General Security For Statewide IT Resources Access Policy documents the process for users to inform their supervisor of security incidents.	Reviewed the General Security For Statewide IT Resources Access Policy to determine if the Policy documents the process for users to inform their supervisor of security incidents.	The Policy does not address the process for supervisors to ensure security incidents identified by users are communicated to management for review and resolution.

Criteria 2.5 Changes that may affect system security are communicated to management and users who will be affected.

Department’s Control	Auditor’s Tests of Control	Test Results
Changes are communicated to users and management via the CAC meetings; which the meeting minutes are posted on the ECM SharePoint site.	Interviewed staff, reviewed a sample of communications, ECM Sharepoint site, a sample of reports, and sampled Requests For Changes (RFCs) to ascertain if changes are communicated to users and management via the CAC meeting minutes posted on the ECM Sharepoint site.	Four of 32 RFCs and 4 of 12 emergency RFCs were not included in CAC meeting minutes.
Agencies have access to the ECM SharePoint site.	Interviewed staff and utilized auditor access to determine if agencies have access to the ECM Sharepoint site.	No deviations noted.

3.0 – Procedure: The entity placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

Criteria 3.1 Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.

Department’s Control	Auditor’s Tests of Control	Test Results
A risk assessment is performed periodically.	Interviewed staff and reviewed the IT Risk Assessment Framework to determine if a risk assessment is performed periodically.	Formal risk assessments, based on the Framework, had not been periodically performed.
As security threats are identified, they are assessed.	Interviewed staff and reviewed the IT Risk Assessment Framework to ascertain whether, as security threats are identified, they are assessed.	Threat analysis and treatment plans based on the Framework had not been developed.

Criteria 3.2	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:	
Criteria A	Logical access security measures restrict access to information resources not deemed to be public.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
Logical access to information is protected through system security software and application security.	Interviewed staff and reviewed system options to determine if logical access is protected through system security software.	No deviations noted.
Access to resources is granted to authenticated users based on the user's identity.	Interviewed staff, reviewed security software manual, a sample of user profiles, and system options to determine that access to resources is granted to authenticated users based on the user’s identity.	No deviations noted.
System options have been configured to protect system resources.	Reviewed reports and system settings to determine that system options have been configured to protect system resources.	No deviations noted.
Criteria B	Identification and authentication of users.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
Users establish their identity and authentication to systems and applications through the use of user IDs and passwords.	Reviewed security software manual, user profiles, system options, and verified user sign-on process to determine that users establish their identity and authentication to systems and applications through the use of user IDs and passwords.	No deviations noted.
It is the standard practice to assign each valid user a unique and individual ID.	Interviewed staff and reviewed security reports and RACF procedures to ascertain whether it is the standard practice to assign each valid user a unique and individual ID.	No deviations noted.
Password configurations have been established.	Reviewed system options, password standards, and tested the use of the password standards to determine that password configurations have been established.	No deviations noted.
Users establish their identity and authentication to network services through the use of user IDs and passwords.	Interviewed staff and reviewed the architecture on a sample of authentication servers and a sample of user accounts to determine that users establish their identity and authentication to network services through the use of user IDs and passwords.	Four of 91 user accounts on authentication servers no longer required access.
Password configurations have been established on authentication servers.	Reviewed password configurations and a sample of user accounts determine that password configurations have been established.	Eleven out of 91 user accounts on authentication servers had not been configured to disable accounts after the defined number of unsuccessful login attempts.

Criteria C Registration and authorization of new users.

Department’s Control	Auditor’s Tests of Control	Test Results
Network Services required manager review and approval of new access rights. LAN Services utilized the LAN Services Access Authorization Form in order for staff to obtain access rights.	Interviewed staff, reviewed the LAN Services’ LAN Equipment Access Rights Standard, and a sample of LAN Services Access Authorization Forms to determine if Network Services required manager review and approval of new access rights and LAN Services utilized its Form for staff to obtain access rights.	Documentation of requests, reviews, and approvals was not maintained by all of Network Services.
Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form for new and modification requests and submit via a Remedy Enterprise Service Request.	Interviewed staff, reviewed the New RACF ID Procedures, ESR instructions, and a sample of new RACF IDs to determine if Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form for new and modification requests and submit via a Remedy Enterprise Service Request.	Six out of 19 new RACF ID requests did not utilize the Mainframe Security Request Form. Additionally, the Procedures did not address the methods for processing an ESR.
The Mainframe Application Access Request Form indicates the access required and proper approval.	Interviewed staff, reviewed the New RACF ID Procedures, ESR instructions, and a sample of new RACF IDs to determine if the Mainframe Application Access Request Form indicates the access required and proper approval.	Eleven out of 19 new RACF ID requests were not properly completed or approved.

Criteria D The process to make changes and updates to user profiles.

Department’s Control	Auditor’s Tests of Control	Test Results
Network Services is notified by Personnel of changes in an individual’s employment status and makes changes to user’s access rights accordingly. Changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization Form.	Interviewed staff, reviewed the LAN Services’ LAN Equipment Access Rights Standard, and a sample of LAN Services Access Authorization Forms to determine if Network Services is notified by Personnel of changes in an individual’s employment status and makes changes to user’s access rights accordingly and changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization Form.	Documentation of changes to user access rights was not maintained by all of Network Services. One of 2 Forms for departed employees had not been completed by LAN Services.
Password resets to Department and proxy agency user profiles are completed by submitting an email request to the Help Desk, or by accessing the Department’s Identity Management website.	Interviewed staff, observed the Help Desk reset process, reviewed the Identity Management website, RACF Password Reset Request Procedures, and a sample of RACF Password Resets to determine if password resets to Department and proxy agency user profiles are completed by submitting an email request to the Help Desk, or by accessing the Department’s Identity Management website.	23 out of 23 RACF Password Resets did not follow the Procedures. (See page 105 for a listing of affected agencies.) In addition, Help Desk staff did not have adequate rights to reset passwords for all agencies.

Bi-monthly the Department’s RACF Coordinator receives a separation report documenting separations from all agencies. The Department’s RACF Coordinator will review and revokes the user’s ID.	Interviewed staff, reviewed a sample of separation reports, and a sample of IDs on the separation report to determine if the Department’s RACF Coordinator receives a bi-monthly separation report and revokes user ID’s.	Documentation was not maintained of the review of the separation report and 1 out of 3 separated individuals’ RACF ID had not been revoked.
Bi-annually, the Department’s RACF Coordinator will send all agencies a listing of their users on the security authorization listing, requesting the agency to review for accuracy, note any modifications, and return to the Department.	Interviewed staff and reviewed update requests in September 2012 and May 2013 to determine if the Department’s RACF Coordinator bi-annually sends all agencies a listing of their users on the security authorization listing, requesting the agency to review for accuracy, note any modifications, and return to the Department.	No deviations noted.
Criteria E Distribution of output restricted to authorized users.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The distribution of output is restricted to authorized users via logical and physical security barriers.	Interviewed staff, assessed physical security barriers, observed distribution process, and reviewed logical security controls to ascertain whether the distribution of output is restricted to authorized users via logical and physical security barriers.	No deviations noted.
Distribution of digital output is restricted to authorized users through the management of system software tools or the online viewing software.	Interviewed staff and reviewed logical security controls to ascertain whether the distribution of digital output is restricted to authorized users through the management of system software tools or the online viewing software.	No deviations noted.
Distribution of hardcopy output is restricted through physical and manual controls.	Interviewed staff, assessed physical security barriers, and observed the distribution process to ascertain whether the distribution of hardcopy output is restricted through physical and manual controls.	No deviations noted.
Hardcopy output is printed at a secure facility with security guards.	Interviewed staff and assessed the physical security barriers to ascertain whether hardcopy output is printed at a secure facility with security guards.	No deviations noted.
Upon request for pick up, the individual must identify themselves and be on the authorization listing.	Observed the distribution process and sampled individuals from the authorization list to determine whether individuals must identify themselves and be on the authorization listing for report pick-ups.	One out of 25 individuals was not on the authorization list.

<table>
<tr><td colspan="3">Criteria F Restriction of access to offline storage, backup data, systems, and media.</td></tr>
<tr><th>Department’s Control</th><th>Auditor’s Tests of Control</th><th>Test Results</th></tr>
<tr><td>Access to offline storage, backup data, system and media is limited via physical and logical access controls.</td><td>Observed and reviewed physical access controls at the CCF, Communications Building, Alternate Data Center, and Regional Vault to determine that access is restricted. Interviewed staff and reviewed group and individual security profiles to determine if logical access controls are in place to limit access to off-line storage, backup data, system and media.</td><td>Two out of 40 individuals on the authorization listing no longer required access to the Alternate Data Center. Two out of the 32 individuals on the authorization listing no longer required access to the Regional Vault. Five individuals had excessive or inappropriate logical access rights.</td></tr>
<tr><td colspan="3">Criteria G Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).</td></tr>
<tr><th>Department’s Control</th><th>Auditor’s Tests of Control</th><th>Test Results</th></tr>
<tr><td>Logical security controls are in place to restrict access to operating system configurations.</td><td>Interviewed staff and reviewed system options, security reports, security software, exits, and access rights to sensitive system functions to determine if logical security controls are in place to restrict access to operating system configurations.</td><td>Four active IDs with the capability to modify operating system configurations were either not specifically assigned or were assigned to departed staff. Two IDs had excessive access to operating system resources.</td></tr>
<tr><td>Physical access controls are in place to restrict access to system consoles.</td><td>Interviewed staff and observed and reviewed physical access controls at the CCF to determine if physical access controls are in place to restrict access to system consoles.</td><td>No deviations noted.</td></tr>
<tr><td>Records exist for monitoring and documenting operating system actions.</td><td>Interviewed staff and reviewed system files to determine if records exist for monitoring and documenting operating system actions.</td><td>No deviations noted.</td></tr>
<tr><td>Operating systems are configured and controlled to promote security and integrity.</td><td>Interviewed staff and reviewed system options, security reports, security software, exits, and libraries to determine if operating systems are configured and controlled to promote security and integrity.</td><td>No deviations noted.</td></tr>
<tr><td>Security software passwords are maintained in an encrypted database.</td><td>Reviewed security software manual and security reports to determine if security software passwords are maintained in an encrypted database.</td><td>No deviations noted.</td></tr>
</table>

Authentication servers are utilized to control access, log access attempts, and alert management.	Interviewed staff and reviewed authentication servers to determine if they are utilized to control access, log access attempts, and alert management.	Two out of 4 authentication servers were not configured to alert management of multiple failed access attempts.

Criteria 3.3	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
Physical access is restricted via card key systems.	Observed and reviewed physical access controls at the CCF and Communications Building to determine if physical access is restricted via card key systems.	No deviations noted.
Card keys are utilized to restrict access to authorized individuals to the CCF and Communications Building.	Reviewed card key system and sampled associated access rights to determine if card keys are utilized to restrict access to the CCF and Communications Building.	One out of the 40 individuals sampled was a former employee who no longer required access to the CCF.
In order to obtain a card key, an ID Badge Request Form is to be completed, approval must be obtained from an authorized manager, and presentation of a valid ID.	Interviewed staff, reviewed the ID Badge Request Form, and sampled ID Badge Request Forms to determine if the Forms were completed, properly approved, and a valid ID was presented prior to obtaining a card key.	Nine out of 9 Forms were properly approved and indicated a valid ID was presented; however, 5 out of 9 had fields that were not completed.
Visitors are required to sign in and out, in addition to being escorted.	Interviewed security guards, reviewed Security Procedure Manual and Post Orders, sampled building admittance registers, and tested for compliance at the CCF and Communications Building to determine if visitors are required to sign in and out, in addition to being escorted.	Four out of 24 individuals sampled had expired badges; however, they were permitted access without being verified and escorted.
The CCF and the Communications Building are guarded by security guards.	Interviewed security guards, reviewed security guard contract, and observed security guards to determine if the CCF and Communications Building are guarded by security guards.	No deviations noted.
Video surveillance is utilized to monitor the CCF and the Communications Building.	Observed surveillance cameras to determine if video surveillance is utilized to monitor the CCF and the Communications Building.	No deviations noted.
Procedures exist for the identification and escalation of physical security breaches.	Interviewed staff and security guards, reviewed Security Procedure Manual and Post Orders, and reviewed a sample of building incident reports to ascertain whether procedures for the identification and escalation of physical security breaches were included and followed.	No deviations noted.
Physical access controls are in place to restrict access to the offsite storage location.	Observed and reviewed physical access controls at the Alternate Data Center and Regional Vault to determine if physical access controls are in place to restrict access to offsite storage locations.	No deviations noted.

Access to the offsite media is limited to authorized Department personnel.	Interviewed staff and reviewed the authorization listings for the Alternate Data Center and Regional Vault to determine if access to offsite media is limited to authorized Department personnel.	Two out of the 40 individuals on the authorization listing no longer required access to the Alternate Data Center. Two out of 32 individuals on the authorization listing no longer required access to the Regional Vault.

Criteria 3.4 Procedures exist to protect against unauthorized access to system resources.

Department's Control	**Auditor's Tests of Control**	**Test Results**
Access to system resources is restricted to authorized personnel through security software.	Interviewed staff, reviewed security reports, and sampled access rights to determine that access to system resources is restricted to authorized personnel through security software.	No deviations noted.
Access to high-level access privileges is limited to security administration personnel.	Interviewed staff, reviewed security reports, and sampled access rights to determine that access to high-level access privileges is limited to security administration personnel.	No deviations noted.
Firewalls and routers are used and configured to prevent unauthorized access via authentication servers, logging servers, banners prohibiting unauthorized access and warning of prosecution and access control lists (ACL) to deny and permit specific types of network traffic.	Interviewed staff and reviewed firewall, router and switch configurations to determine if these devices are used and configured to prevent unauthorized access via authentication servers, logging servers, banners prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific types of network traffic.	Two out of 60 firewalls, routers, and switches were not configured to utilize logging servers and 3 out of 60 were not configured to utilize banners.

Criteria 3.5 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The ability to install, modify, and replace operating systems is limited to authorized staff.	Interviewed staff and reviewed security reports and privileged access rights to ascertain whether the ability to install, modify, and replace operating systems is limited to authorized staff.	No deviations noted.
Access to sensitive system functions is restricted to authorized staff.	Interviewed staff and reviewed security reports and access rights to sensitive system functions to ascertain whether sensitive functions were restricted to authorized staff.	No deviations noted.
The Security and Compliance Solutions Team participates in user groups and subscribes to services related to computer viruses.	Interviewed staff and reviewed a sample of subscription notifications to ascertain whether the Security and Compliance Solutions Team participates in user groups and subscribes to services related to computer viruses.	No deviations noted.

Criteria 3.6 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Department makes available encryption technologies and access gateways for the transmission of sensitive or confidential information.	Interviewed staff and reviewed the Enterprise Virtual Private Network (VPN) standard and the web portal to ascertain whether the Department makes available encryption technologies and access gateways for the transmission of sensitive or confidential information.	No deviations noted.

Criteria related to execution and incident management used to achieve objectives.

Criteria 3.7 Procedures exist to identify, report, and act upon system security breaches and other incidents.

Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Department has tools in place to identify, log, and report security breaches and other incidents.	Interviewed staff, reviewed the General Security For Statewide IT Resources Policy, Security Fundamentals document, Situation Awareness and Continuous Monitoring Process, Major Outage Response Team Process, MORT Tickets, CIRT Case Reports, Remedy system, and observed monitoring tools to determine if the Department has tools in place to identify, log, and report security breaches and other incidents.	No deviations noted.
The Department has tools in place to identify and log network services security breaches.	Interviewed staff and reviewed network device configurations to ascertain whether the Department has tools in place to identify, log, and report security breaches and other incidents.	Two out of 60 devices were not configured to utilize logging servers and logging servers were not consistently defined in 35 out of 60 devices. In addition, log files were not proactively reviewed.
The Department's website provides users instructions for communicating security issues to the CMS Help Desk.	Reviewed the Department’s website to ascertain whether instructions for communicating security issues to the Help Desk are included.	No deviations noted.
The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets.	Interviewed staff, reviewed the Enterprise Desktop/Laptop Policy, the Mobile Device Security Policy, Laptop Data Encryption Policy, IT Coordinator Guide to BCCS Services, Remedy System, and the listing lost/stolen laptops to determine if the Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets.	The Help Desk was not informed of lost/stolen assets and 4 out of the 5 laptops lost/stolen did not have encryption installed as required by Policy.

Criteria related to the system components used to achieve objectives.

Criteria 3.8 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Business Reference Model collects and stores information related to application and data processing services provided based on the Data Classification and Protection Policy.	Interviewed staff and reviewed the Data Classification and Protection Policy to determine if the Business Reference Model collects and stores information related to application and data processing services provided based on the Policy.	No deviations noted.
The Business Reference Model is periodically updated by the applicable agency.	Reviewed the BRM listing to determine if the Department is periodically updating and classifying its applications.	The Department had not classified 91 out of 179 of its applications.

Criteria 3.9 Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
Department staff is assigned the responsibility for monitoring and ensuring compliance with security policies.	Interviewed staff, reviewed policies, and position descriptions to determine if Department staff are assigned the responsibility for monitoring and ensuring compliance with security policies.	The Department had not assigned the responsibility for monitoring and ensuring compliance with security policies.

Criteria 3.10 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The IT Governance Policy governs the acquisition of systems and technology.	Interviewed staff, reviewed the IT Governance Policy and a sample of project charters to ascertain whether the IT Governance Policy governs the acquisition of systems and technology.	No deviations noted.
As part of the Governance process, agencies are to classify the data and system in accordance with the Data Classification and Protection Policy.	Reviewed the IT Governance Policy and Data Classification and Protection Policy to ascertain whether agencies are to classify the data and system in accordance with the Data Classification and Protection Policy as part of the Governance process.	No deviations noted.
The Remedy Change Management Guide guides the development, implementation and maintenance of systems.	Reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if the Guide provides guidance on the development, implementation and maintenance of systems.	Forty-two RFCs were properly approved; however, 39 of 42 contained fields (primarily date requested) that were not completed as required by the Guide.
Standards provide guidance on the configuration and deployment of network devices.	Interviewed staff and reviewed standards and templates to determine if they provide guidance on the configuration and deployment of network devices.	No deviations noted.
Network diagrams are maintained.	Interviewed staff and reviewed network diagrams to determine if diagrams are maintained.	No deviations noted.

Criteria 3.11 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Department's position descriptions specify the position's qualifications and responsibilities.	Interviewed staff and reviewed a sample of position descriptions to ascertain whether position descriptions specify qualifications and responsibilities.	No deviations noted.
The State's hiring procedures are followed for the hiring of staff.	Interviewed staff and reviewed documentation outlining the hiring procedures, State of Illinois Personnel Code (20 ILCS 450), and Department of Central Management Service's Personnel Rules (80 Admin Code 301) to determine if procedures are followed for new hires.	No deviations noted.
New employees are required to have background checks.	Interviewed staff and reviewed a sample of documentation to determine if new employees are required to have background checks.	Eight out of 20 new employees did not have background checks
Annual performance evaluations are completed.	Interviewed staff and reviewed the Employee Evaluation Spreadsheet to determine if annual performance evaluations are completed.	248 employees listed on the employee evaluation spreadsheet had evaluations that were past due.
Staff is provided training.	Interviewed staff and reviewed a sample of employee training records and the list of employees who completed security awareness training to ascertain whether staff is provided training.	No deviations noted.
The Department conducts cross training.	Interviewed staff and reviewed a sample of employee training records to ascertain whether staff is provided training.	No deviations noted.

Change management-related criteria applicable to the system's security.

Criteria 3.12 Procedures exist to maintain system components, including configurations consistent with the defined system security policies.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Remedy Change Management Guide provides guidance in maintaining system components, including system configurations.	Interviewed staff and reviewed the Remedy Change Management Guide to ascertain if the Guide provides guidance on maintaining system components, including system configurations.	No deviations noted.
Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if changes are categorized and ranked according to priority and procedures are in place to handle urgent matters.	Fourty-two RFCs were properly categorized, and ranked; however, 12 of 14 emergency RFCs did not have all required fields completed.
Standards provide guidance on the configuration and deployment of network devices.	Interviewed staff and reviewed standards and templates to determine if there is guidance on the configuration and deployment of network devices.	No deviations noted
Tools are in place to assist in the deployment of and reporting on configurations.	Interviewed staff and reviewed standard configurations and a sample of networking devices to ascertain whether tools are in place to assist in the deployment of and reporting on configurations.	No deviations noted

Criteria 3.13 Procedures exist to provide that only authorized, tested and documented changes are made to the systems.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The Remedy Change Management Guide provides guidance for the authorization and documentation requirements for changes to systems.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if the Guide provides guidance for the authorization and documentation requirements for changes to systems.	The Guide did not provide documentation requirements for backout plans, testing plans, implementation plans, and post implementation reviews.
High impact changes require backout, test, and implementation plans to be attached to the RFC for the use in the event of a disruption.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if high impact changes require back-out, test, and implementation plans to be attached to the RFC for use in the in the event of a disruption.	Two out of 10 high impact RFCs did not have required backout plans, test plans, or implementation plans.

Criteria 3.14 Procedures exist to provide that emergency changes are documented and authorized timely.

Department's Control	**Auditor's Tests of Control**	**Test Results**
Emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide.	Reviewed the Remedy Change Management Guide, Change Management Policy, and sampled emergency Requests For Changes (RFCs) to ascertain if emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide.	The Guide did not provide documentation requirements for post implementation reviews which were required for emergency changes. Post implementation review documentation was lacking on 12 of 12 emergency RFCs.
Emergency changes require verbal approval prior to implementation. Standard approvals are to be obtained post implementation.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled emergency Requests For Changes (RFCs) to ascertain if emergency changes require verbal approval prior to implementation and if standard approvals are documented post implementation.	No deviations noted.
Emergency changes are communicated to users post implementation via the CAC meeting.	Interviewed staff, reviewed the Remedy Change Management Guide, ECM Sharepoint site, and sampled emergency Requests For Changes (RFCs) to ascertain if emergency changes are communicated to users post implementation via the CAC meeting.	Four of 12 emergency RFCs were not included in CAC meeting minutes.

4.0 – Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security policies.

Criteria 4.1	The entity's system security is periodically reviewed and compared with the defined system security policies.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Department utilizes various tools to review and assess the infrastructure and vulnerabilities.	Interviewed staff and reviewed a sample of Daily Shift Reports, Shift Change Checklists, Remedy System Tickets, monitoring and performance tools, and intruder alert reports to ascertain whether various tools are utilized to review and assess the infrastructure and vulnerabilities.	No deviations noted.
System performance and capacity is monitored via software tools.	Interviewed staff and reviewed software tool reports and a sample of monthly capacity emails to determine if system performance and capacity is monitored via software tools.	No deviations noted.

Criteria 4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
Logs are analyzed either manually or by automated tools to identify trends that may have the potential to impact the Department’s ability to achieve system security objectives.	Interviewed staff and reviewed a sample of Daily Shift Reports, Shift Change Checklists, and Remedy System Tickets to ascertain whether logs are analyzed either manually or by automated tools to identify trends that may have the potential to impact the Department’s ability to achieve system security objectives. Reviewed a sample of Shift Change Checklists and Daily Shift Reports to determine that a report was completed for each day. Reviewed a sample of referenced Remedy tickets on Daily Shift Reports to determine if a corresponding ticket in the Remedy System had been created.	No deviations noted.
Security issues are addressed with management at various meetings.	Reviewed a sample of communications with users and meeting agendas to ascertain whether security issues are addressed with management at various meetings.	No deviations noted.

Criteria 4.3	Environmental, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
Department management considers technological developments, and laws and regulations during the planning process.	Reviewed the BCCS Strategic Plan, a sample of communications with users, agendas, and the Department’s website to ascertain whether Department management considers technological developments, and laws and regulations during the planning process.	No deviations noted.
Management conducts meetings with user agencies to determine their future needs.	Reviewed a sample of communications with users, agendas, and the Department’s website to ascertain whether the management conducts meetings with user agencies to determine their future needs.	No deviations noted.

TRUST SERVICES - AVAILABILITY PRINCIPLE, CRITERIA, RELATED CONTROLS AND TEST OF CONTROLS

1.0 – Policies: The entity defines and documents its policies for the availability of its system.

Criteria 1.1 The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.

Department’s Control	Auditor’s Tests of Control	Test Results
The security policies addressing logical and physical security are reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel and the Chief Information Security Officer.	Reviewed the security policies addressing logical and physical security to determine if the policies had been reviewed and approved by the Department’s Director, Deputy Director, Deputy General Counsel, and the Chief Information Security Officer.	A formal process requiring periodic reviews of policies did not exist.
The Department has implemented security policies, which are posted on the Department's website.	Reviewed the Department’s website to ascertain whether the Department’s security policies are posted on the website.	No deviations noted.

Criteria 1.2 The entity's system availability and related security policies include, but may not be limited to, the following matters:

Criteria A Identifying and documenting the system availability and related security requirements of authorized users.

Department’s Control	Auditor’s Tests of Control	Test Results
The security policies identify and document the general security and availability requirements.	Interviewed staff and reviewed security policies to determine if they identify and document general security and availability requirements.	No deviations noted.

Criteria B Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.

Department’s Control	Auditor’s Tests of Control	Test Results
The Data Classification and Protection Policy documents the data classification schema used to value and classify information generated, accessed, transmitted or stored.	Interviewed staff and reviewed the Data Classification and Protection Policy to determine if it documents the data classification schema used to value and classify information generated, accessed, transmitted or stored.	No deviations noted.
The IT Resource Access Policy documents the requirements for obtaining access to resources.	Interviewed staff and reviewed the IT Resource Access Policy to determine if the Policy documents the process for obtaining access to resources.	No deviations noted.
The Electronically Stored Information Retention Policy documents the retention requirements for electronic information.	Interviewed staff and reviewed the Electronically Stored Information Retention Policy to determine if the Policy documents the retention requirements of electronic information.	No deviations noted.
The General Security For Statewide IT Resources Policy documents the destruction requirements.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy to determine if it documents destruction requirements.	No deviations noted.

Criteria C Assessing risks on a periodic basis.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The IT Risk Assessment Policy documents the requirements for assessing risk.	Interviewed staff and reviewed the IT Risk Assessment Policy to determine if it documents the requirements for assessing risk.	No deviations noted.
Criteria D Preventing unauthorized access.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The IT Resource Access Policy documents controls for preventing unauthorized access.	Interviewed staff and reviewed the IT Resource Access Policy to determine if the Policy documents the process for obtaining access to resources.	The Policy did not include specific requirements or procedures for requesting, modifying, approving, or periodically reviewing user access rights.
Criteria E Adding new users, modifying the access levels of existing users, and removing users who no longer need access.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the Statewide CMS/BCCS Facility Access Policy documents the requirements for granting, assigning and revoking user access.	Interviewed staff and reviewed the IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the Statewide CMS/BCCS Facility Access Policy to determine if the policies document the requirements for granting, assigning and revoking user access.	The IT Resource Access Policy and the General Security For Statewide IT Resources Policy did not include specific requirements or procedures for requesting, modifying, approving, or revoking user access rights. The CMS/BCCS Facility Access Policy did not address requirements for modifying physical access rights.
Criteria F Assigning responsibility and accountability for system availability and related security.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the General Security For Statewide Network Resource Policy documents the requirements for granting, assigning and revoking user access.	Interviewed staff and reviewed the IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the General Security For Statewide Network Resource Policy to determine if the policies document the responsibility and accountability of system security.	No deviations noted.

Criteria G Assigning responsibility and accountability for system changes and maintenance.

Department’s Control	Auditor’s Tests of Control	Test Results
The Change Management Policy documents the responsibility and accountability of Department staff for system changes and maintenance.	Interviewed staff and reviewed the Change Management Policy to determine if the Policy documents the responsibility and accountability of Department staff for system changes and maintenance.	No deviations noted.

Criteria H Testing, evaluating, and authorizing system components before implementation.

Department’s Control	Auditor’s Tests of Control	Test Results
The Change Management Policy documents the process in which infrastructure changes are to follow.	Interviewed staff and reviewed the Change Management Policy to determine if it documents the process in which infrastructure changes are to follow.	Testing requirements are not addressed in the Policy.
The processes outlined in the Application Lifecycle Management Manual are used to control changes to applications.	Interviewed staff, reviewed the Application Lifecycle Management Manual, and sampled change tickets, change tasks, and move sheets to determine if the processes outlined in the Manual are used to control changes to applications.	A suitable change management process was not in place from July 1, 2012 to November 30, 2012. The Application Lifecycle Management Manual was implemented on December 1, 2012. For changes after November 30, 2012: 10 out of 10 change tickets did not comply with the Manual and 55 out of 77 change tasks did not have appropriate documentation to support the move to production.

Criteria I Addressing how complaints and requests relating to system availability and related security issues are resolved.

Department’s Control	Auditor’s Tests of Control	Test Results
The General Security For Statewide IT Resources Policy states users are responsible for disclosing any actions or behaviors involving a State IT resource and report on actual or suspected breaches.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy to determine if the Policy documents the reporting and resolution of security breaches and other incidents.	The Policy did not address the entire process for reporting and resolving security issues.

Criteria J Identifying and mitigating system availability and related security breaches and other incidents.

Department's Control	Auditor's Tests of Control	Test Results
The General Security For Statewide IT Resources Policy and the Action Plan For Notification of a Security Breach documents the identification and notification of security breaches and other incidents.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy and the Action Plan For Notification of a Security Breach to determine if they document the identification, notification, and mitigation of security breaches and other incidents.	The Policy did not address the entire process for identifying, reporting, and mitigating security issues.

Criteria K Providing for training and other resources to support its system availability and related security policies.

Department's Control	Auditor's Tests of Control	Test Results
The General Security For Statewide IT Resources Policy documents the security awareness training requirements for Department staff.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy to determine if the Policy documents the security awareness training requirements for Department staff.	No deviations noted.

Criteria L Providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies.

Department's Control	Auditor's Tests of Control	Test Results
The General Security For Statewide IT Resources Policy and the General Security For Statewide Network Resources Policy indicates it is the responsibility of the users to inform the Department, in writing of any exceptions or special use requirements.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy and the General Security For Statewide Network Resources Policy to determine if the policies indicate it is the responsibility of the users to inform the Department, in writing of any exceptions or special use requirements.	No deviations noted.

Criteria M Providing for the identification of and consistency with, applicable laws and regulations defined commitments, service-level agreements, and other contractual requirements.

Department's Control	Auditor's Tests of Control	Test Results
The IT Governance Policy documents the Department and the agencies responsibilities for identifying applicable laws, regulations, and other requirements as part of the new IT projects requirements.	Interviewed staff and reviewed the IT Governance Policy to determine if the Policy documents the Department and the agencies responsibilities for identifying applicable laws, regulations, and other requirements as part of the new IT projects requirements**.**	No deviations noted.

Criteria N Recovering and continuing service in accordance with documented customer commitments or other agreements.

Department's Control	Auditor's Tests of Control	Test Results
The Information Technology Recovery Plan and the Recovery Methodology document the Department's responsibilities related to recovery and continuous services.	Interviewed staff and reviewed the Information Technology Recovery Plan and the Recovery Methodology to determine if the Plan and Methodology document the Department's responsibility related to recovery and continuous services.	The Plan and Methodology had not been updated to reflect changes in recovery vendors and backup processes.

Criteria O Monitoring system capacity to achieve customer commitments or other agreements regarding availability.

Department's Control	Auditor's Tests of Control	Test Results
The IT Governance Policy and associated documents outlined requirements for new applications.	Interviewed staff and reviewed the IT Governance Policy and associated documents to determine if requirements for new applications are outlined.	No deviations noted.

Criteria 1.3 Responsibility and accountability for developing and maintaining the entity's system availability and related security policies, and changes and updates to those policies, are assigned.

Department's Control	Auditor's Tests of Control	Test Results
The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of the security policies.	Reviewed the position description for the Chief Information Security Officer to ascertain whether responsibilities for the development and maintenance of security policies are included. Reviewed security policies to determine if approval by the Chief Information Security Officer is documented.	No deviations noted.

2.0 – Communications: The entity communicates the defined system availability policies to responsible parties and authorized users.

Criteria 2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

Department's Control	Auditor's Tests of Control	Test Results
The Department has published the Service Catalog on its website, which documents the services provided by the Department.	Interviewed staff and reviewed the Service Catalog on the website to determine if it documents the services provided by the Department.	No deviations noted.

Criteria 2.2 The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.

Department's Control	Auditor's Tests of Control	Test Results
The Department's security commitments and obligations are outlined in the Service Catalog, which is posted on the Department's website.	Reviewed Service Catalog on the website to determine if security commitments and obligations are outlined.	No deviations noted.
The security obligations of Department staff are communicated via the mandatory annual security awareness training, security policies, and periodic emails.	Interviewed staff, reviewed the General Security For Statewide IT Resources Policy, the CMS Security Fundamental web tutorial, and a sample of security communications to determine if security obligations are communicated to Department staff via the mandatory annual security awareness training, security policies, and periodic emails.	No deviations noted.
New Department staff is required to sign a statement signifying that they will comply with the security policies.	Reviewed the CMS Security Fundamentals web tutorial and the training certification list to determine if new Department staff is required to sign a statement signifying that they will comply with the security policies.	No deviations noted.
Department staff reconfirms their compliance with the security policies through the annual security training.	Reviewed the CMS Security Fundamental web tutorial and the listing of Department staff annual certifications to determine if staff reconfirms their compliance with the security policies through the annual security training.	No deviations noted.

Contractors are required to take the annual security awareness training and certify they will comply with security policies.	Interviewed staff and reviewed the CMS Security Fundamental web tutorial and the listing of contractor certifications to determine if contractors are required to take the annual security awareness training and certify they will comply with security policies.	No deviations noted.
The security obligations of users are communicated in several different fashions; policies published on the web, emails, and security notices on the website.	Reviewed a sample of emails and the Department's website to determine if security obligations of users are communicated via policies, security notices, and emails.	No deviations noted.

Criteria 2.3 Responsibility and accountability for the entity's system availability and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of security policies.	Reviewed the position description for the Chief Information Security Officer to ascertain whether responsibilities for the development and maintenance of security policies are included. Reviewed security policies to determine if approval by the Chief Information Security Officer is documented.	No deviations noted.
Position descriptions have been defined and communicated to employees.	Interviewed staff and reviewed a sample of position descriptions to ascertain whether position descriptions have been defined and communicated to employees.	No deviations noted.

Criteria 2.4 The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The process for users to inform the Department of possible security issues and other incidents is posted on the Department's website.	Interviewed staff and reviewed the Department's website to determine if the process for users to inform the Department of possible security issues and other incidents is posted on the website.	Procedures had not been developed to ensure security issues and incidents identified by users are communicated to management for review and resolution.
The General Security For Statewide IT Resources Access Policy documents the process for users to inform their supervisor of security incidents.	Reviewed the General Security For Statewide IT Resources Access Policy to determine if the Policy documents the process for users to inform their supervisor of security incidents.	The Policy does not address the process for supervisors to ensure security incidents identified by users are communicated to management for review and resolution.
The user manuals for applications provide instructions for users to contact the CMS Help Desk to report issues.	Interviewed staff and reviewed user manuals and reference documents to ascertain whether user manuals for application provide instructions for users to contact the CMS Help Desk to report issues.	No deviations noted.

Criteria 2.5	Changes that may affect system availability and system security are communicated to management and users who will be affected.	
Department's Control	**Auditor's Tests of Control**	**Test Results**
Changes are communicated to users and management via the CAC meetings; which the meeting minutes are posted on the ECM SharePoint site.	Interviewed staff, reviewed a sample of communications, ECM Sharepoint site, a sample of reports, and sampled Requests For Changes (RFCs) to ascertain if changes are communicated to users and management via the CAC meeting minutes posted on the ECM Sharepoint site.	Four of 32 RFCs and 4 of 12 emergency RFCs were not included in CAC meeting minutes.
Agencies have access to the ECM SharePoint site.	Interviewed staff and utilized auditor access to determine if agencies have access to the ECM Sharepoint site.	No deviations noted.
Changes to applications are communicated to users via email or phone.	Reviewed a sample of communication to determine if changes to applications are communicated to users via email or phone.	No deviations noted.
Planned changes to applications are conducted during the scheduled maintenance window.	Interviewed staff and reviewed the systems maintenance window schedules to ascertain whether planned changes to applications are conducted during the scheduled maintenance window.	No deviations noted.

3.0 – Procedures: The entity placed in operation procedures to achieve its documented system availability objectives in accordance with its defined policies.

Criteria 3.1	Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.	
Department's Control	**Auditor's Tests of Control**	**Test Results**
A risk assessment is performed periodically.	Interviewed staff and reviewed the IT Risk Assessment Framework to determine if a risk assessment is performed periodically.	Formal risk assessments, based on the Framework, had not been periodically performed.
As security threats are identified, they are assessed.	Interviewed staff and reviewed the IT Risk Assessment Framework to ascertain whether, as security threats are identified, they are assessed.	Threat analysis and treatment plans based on the Framework had not been developed.

Criteria 3.2	Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	
Department's Control	**Auditor's Tests of Control**	**Test Results**
Procedures exist for the identification, documentation, escalation, resolution, and review of problems.	Interviewed staff and reviewed the Data Processing Guide to ascertain whether procedures for the documentation, escalation, resolution, and review of problems are included.	No deviations noted.

The Department maintains measures to protect against environmental factors (fire extinguishers, fire suppression, sprinkler system, water detection, power failure, and cooling/heating) at the CCF and the Communications Building.	Observed and reviewed measures to determine if measures are maintained to protect against environmental factors (fire extinguishers, fire suppression, sprinkler system, water detection, power failure, and cooling/heating) at the CCF and Communications Building.	No deviations noted.
Environmental factors are monitored at the CFF and the Communications Building.	Observed the facility automation system and equipment to ascertain whether environmental factors are monitored at the CCF and the Communications Building.	No deviations noted.
Preventive maintenance agreements and scheduled maintenance procedures are in place for environmental factors.	Interviewed staff and reviewed contracts and maintenance reports to ascertain whether preventive maintenance agreements and scheduled maintenance procedures are in place for environmental factors.	There was no contract for preventive maintenance of the generators. Maintenance/testing reports for the water detection system, sprinkler system, automation system, heating/cooling systems and generators were not available.
Physical and logical security controls are implemented to reduce the opportunity for unauthorized actions that could impair system availability.	Observed and reviewed physical access controls at the CCF, Communications Building, Alternate Data Center, and Regional Vault to determine if controls are implemented to reduce the opportunity for unauthorized actions that could impair system availability.	No deviations noted.
Vendor agreements are in place for maintenance and support services associated with networking equipment.	Interviewed staff, reviewed vendor agreements, hardware models, and software versions to determine if vendor agreements are in place for maintenance and support services associated with networking equipment.	Four out of 60 hardware models were no longer supported and 3 of the 4 devices were running software no longer supported.
The network is configured in a redundant manner.	Interviewed staff and network device configurations to determine if the network is configured in a redundant manner.	No deviations noted.

Criteria 3.3 Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.

Department's Control	**Auditor's Tests of Control**	**Test Results**
CA-Scheduler is utilized to schedule and control backups.	Interviewed staff, reviewed documentation generated from CA-Scheduler to verify a sample of backups, and observed daily schedules to ascertain whether CA-Scheduler is utilized to schedule and control backups.	No deviations noted.
The backups are conducted routinely.	Interviewed staff, reviewed network device configurations, job schedules, backup configuration files, daily and weekly schedules for system backups, and observed agency data backups to determine if backup are conducted routinely.	No deviations noted.
The Department verifies the daily and weekly backups completed successfully.	Interviewed staff, reviewed documentation generated from CA-Scheduler to verify backups, logs, and observed documentation supporting the completion of scheduled agency backups to ascertain whether the Department verifies the daily and weekly backups completed successfully.	No deviations noted.

The Department is notified of failed backups.	Interviewed staff, reviewed email alerts, and observed automated notifications in the Command Center to determine if the Department is notified of failed backup.	No deviations noted.
Failed backups are recorded on the Shift Report.	Interviewed staff and reviewed a sample of Shift Reports to determine whether failed backups are recorded on the Shift Report.	No deviations noted.
The Department takes remedial action on failed backups.	Interviewed staff and reviewed a sample of Shift Reports and an associated Remedy Ticket to ascertain whether the Department takes remedial action on failed backups.	No deviations noted.
The Department has procedures to guide in remediating failed backups.	Interviewed staff and reviewed the BCCS/ISD Cleanup Procedures to determine whether the Department has procedures to guide in remediating failed backups.	No deviations noted.
The DCMS/BCCS Infrastructure Services Recovery Activation Plan is documented.	Reviewed the DCMS/BCCS Infrastructure Services Recovery Activation Plan to verify that the Plan was documented and current.	The Plan had not been updated to address the change from offsite physical backup tapes to the use of virtual tape technology at the Alternate Data Center.
The DCMS/BCCS Infrastructure Services Recovery Activation Plan documents the roles and responsibilities of personnel.	Reviewed the DCMS/BCCS Infrastructure Services Recovery Activation Plan to verify that the Plan documents the roles and responsibilities of personnel.	No deviations noted.
The agencies document their application recovery classification in the Business Reference Module.	Reviewed the Critical Applications Listing and the Business Reference Model (BRM) to determine if agencies documented their recovery classification in the Business Reference Model.	1,335 of 2,224 applications listed in the BRM had not been assigned a recovery classification.
Testing is conducted annually.	Interviewed staff and reviewed testing documentation from tests in November 2012 to determine if testing is conducted annually.	Test documentation lacked sufficient detail to determine test results, problems encountered, and problem resolution.
Critical personnel hold current versions of the various disaster recovery documents.	Interviewed staff and reviewed recovery documents to determine whether critical personnel hold current versions of disaster recovery documents.	No deviations noted.
Current versions of the various documents are stored offsite.	Reviewed recovery documents at the Alternate Data Center and Regional Vault to determine if current versions of various documents were maintained offsite.	No deviations noted.
Physical backup tapes are stored offsite.	Interviewed staff and reviewed a sample of physical backup tapes to determine if tapes are stored offsite.	No deviations noted.
Virtual tapes are replicated to the Alternate Data Center.	Interviewed staff and observed logs to determine whether virtual tapes are replicated to the Alternate Data Center.	No deviations noted.

Criteria 3.4 Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.

Department's Control	Auditor's Tests of Control	Test Results
The Library Guide and the Media Guide provide guidance on the maintenance, movement and inventory of tape media.	Interviewed staff and reviewed the Library Guide and the Media Guide to ascertain whether they provide guidance on the maintenance, movement and inventory of tape media.	The Guides had not been updated to reflect changes in backup processes and decommission of a facility.
The Department performs an annual verification of media stored at the offsite storage facility.	Interviewed staff and reviewed the November 2012 Inventory Report to determine if the Department performs an annual verification of media stored at the offsite storage facility.	No deviations noted.
Physical backup tapes are stored offsite.	Interviewed staff and reviewed a sample of physical backup tapes to determine if tapes are stored offsite.	No deviations noted.
The Tape Management System tracks the location of physical backups.	Interviewed staff and reviewed a sample of physical tapes to determine whether the Tape Management System tracks the location of physical backups.	No deviations noted.
Virtual tapes are replicated to the Alternate Data Center.	Interviewed staff and observed logs to determine whether virtual tapes are replicated to the Alternate Data Center.	No deviations noted.
Backup systems and data are restored as required.	Interviewed staff, reviewed the Restore Procedures, and a sample of Remedy Tickets to determine whether the backup systems and data are restored as required.	No deviations noted.
Backup systems and data are tested as part of the disaster recovery testing.	Interviewed staff and reviewed disaster recovery testing documentation to ascertain whether backup systems and data are tested as part of the disaster recovery testing.	No deviations noted.
Mainframe application changes moved to production libraries are conducted in accordance with Library Services standards and procedures.	Interviewed staff and reviewed Library Services standards and procedures, and a sample of moves to production to determine if mainframe application changes moved to production libraries are conducted in accordance with standards and procedures.	All moves in the sample were appropriately authorized; however, the "approver listing" for one agency had not been updated.

Security-related criteria relevant to the system's availability.

Criteria 3.5 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

Criteria A Logical access security measures to restrict access to information resources not deemed to be public.

Department's Control	Auditor's Tests of Control	Test Results
Logical access to information is protected through system security software and application security.	Interviewed staff and reviewed system options to determine if logical access is protected through system security software. We reviewed the User Manuals for applications and observed a user to ascertain whether application software is also used to protect access to information.	No deviations noted.
Access to resources is granted to authenticated users based on the user's identity.	Interviewed staff and reviewed security software manual, a sample of user profiles, and system options to determine that access to resources is granted to authenticated users based on the user's identity.	No deviations noted.
System options have been configured to protect system resources.	Reviewed reports and system settings to determine that system options have been configured to protect system resources.	No deviations noted.

Criteria B Identification and authentication of users.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
Users establish their identity and authentication to systems and applications through the use of user IDs and passwords.	Reviewed security software manual, user profiles, system options, and verified user sign-on process to determine that users establish their identity and authentication to systems and applications through the use of user IDs and passwords.	No deviations noted.
It is the standard practice to assign each valid user a unique and individual ID.	Interviewed staff and reviewed security reports and RACF procedures to ascertain whether it is the standard practice to assign each valid user a unique and individual ID.	No deviations noted.
Password configurations have been established.	Reviewed system options, password standards, and tested the use of the password standards to determine that password configurations have been established.	No deviations noted.
Users establish their identity and authentication to network services through the use of user IDs and passwords.	Interviewed staff and reviewed the architecture on a sample of authentication servers, and a sample of user accounts to determine that users establish their identity and authentication to network services through the use of user IDs and passwords.	Four of 91 user accounts on authentication servers no longer required access.
Password configurations have been established on authentication servers.	Reviewed password configurations and a sample of user accounts determine that password configurations have been established.	Eleven out of 91 user accounts on authentication servers had not been configured to disable accounts after the defined number of unsuccessful login attempts.
Criteria C Registration and authorization of new users.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
Network Services required manager review and approval of new access rights. LAN Services utilized the LAN Services Access Authorization Form in order for staff to obtain access rights.	Interviewed staff and reviewed the LAN Services' LAN Equipment Access Rights Standard, and a sample of LAN Services Access Authorization Forms to determine if Network Services required manager review and approval of new access rights and LAN Services utilized its Form for staff to obtain access rights.	Documentation of requests, reviews, and approvals was not maintained by all of Network Services.
Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form for new and modification requests and submit via a Remedy Enterprise Service Request.	Interviewed staff and reviewed the New RACF ID Procedures, ESR instructions, and a sample of new RACF IDs to determine if Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form for new and modification requests and submit via a Remedy Enterprise Service Request.	Six out of 19 new RACF ID requests did not utilize the Mainframe Security Request Form. Additionally, the Procedures did not address the methods for processing an ESR.

The Mainframe Application Access Request Form indicates the access required and proper approval.	Interviewed staff and reviewed the New RACF ID Procedures, ESR instructions, and a sample of new RACF IDs to determine if the Mainframe Application Access Request Form indicates the access required and proper approval.	Eleven out of 19 new RACF ID requests were not properly completed or approved.

Criteria D The process to make changes and updates to user profiles.

Department's Control	**Auditor's Tests of Control**	**Test Results**
Network Services is notified by Personnel of changes in an individual's employment status and makes changes to user's access rights accordingly. Changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization Form.	Interviewed staff and reviewed the LAN Services' LAN Equipment Access Rights Standard, and a sample of LAN Services Access Authorization Forms to determine if Network Services is notified by Personnel of changes in an individual's employment status and makes changes to user's access rights accordingly and changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization Form.	Documentation of changes to user access rights was not maintained by all of Network Services. One of 2 Forms for departed employees had not been completed by LAN Services.
Password resets to Department and proxy agency user profiles are completed by submitting an email request to the Help Desk, or by accessing the Identity Management website.	Interviewed staff, observed the Help Desk reset process, and reviewed the Identity Management website, RACF Password Reset Request Procedures, and a sample of RACF Password Resets to determine if password resets to Department and proxy agency user profiles are completed by submitting an email request to the Help Desk, or by accessing the Department's Identity Management website.	23 out of 23 RACF Password Resets did not follow the Procedures. (See page 105 for a listing of affected agencies.) In addition, Help Desk staff did not have adequate rights to reset passwords for all agencies.
Bi-monthly the Department's RACF Coordinator receives a separation report documenting separations from all agencies. The Department's RACF Coordinator will review and revokes the user's ID.	Interviewed staff and reviewed a sample of separation reports and a sample of IDs on the separation report to determine if Department's RACF Coordinator receives a bi-monthly separation report and revokes user IDs.	Documentation was not maintained of the review of the separation report and 1 out of 3 separated individuals' RACF ID had not been revoked.
Bi-annually, the Department's RACF Coordinator will send all agencies a listing of their users on the security authorization listing, requesting the agency to review for accuracy, note any modifications, and return to the Department.	Interviewed staff and reviewed update requests in September 2012 and May 2013 to determine if the Department's RACF Coordinator bi-annually sends all agencies a listing of their users on the security authorization listing, requesting the agency to review for accuracy, note any modifications, and return to the Department.	No deviations noted.

Criteria E Restriction of access to offline storage, backup data, systems and media.

Department’s Control	Auditor’s Tests of Control	Test Results
Access to offline storage, backup data, system and media is limited via physical and logical access controls.	Observed and reviewed physical access controls at the CCF, Communications Building, Alternate Data Center, and Regional Vault to determine that access is restricted. Interviewed staff, reviewed group and individual security profiles to determine if logical access controls are in place to limit access to off-line storage, backup data, system and media.	Two out of 40 individuals on the authorization listing no longer required access to the Alternate Data Center. Two out of the 32 individuals on the authorization listing no longer required access to the Regional Vault. Five individuals had excessive or inappropriate logical access rights.

Criteria F Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

Department’s Control	Auditor’s Tests of Control	Test Results
Logical security controls are in place to restrict access to operating system configurations.	Interviewed staff and reviewed system options, security reports, security software, exits, and access rights to sensitive system functions to determine if logical security controls are in place to restrict access to operating system configurations.	Four active IDs with the capability to modify operating system configurations were either not specifically assigned or were assigned to departed staff. Two IDs had excessive access to operating system resources.
Physical access controls are in place to restrict access to system consoles.	Interviewed staff and observed and reviewed physical access controls at the CCF to determine if physical controls are in place to restrict access to system consoles.	No deviations noted.
Records exist for monitoring and documenting operating system actions.	Interviewed staff and reviewed system files to determine if records exist for monitoring and documenting operating system actions.	No deviations noted.
Operating systems are configured and controlled to promote security and integrity.	Interviewed staff and reviewed system options, security reports, security software, exits, and libraries to determine if operating systems are configured and controlled to promote security and integrity.	No deviations noted.
Security software passwords are maintained in an encrypted database.	Reviewed security software manual and security reports to determine if security software passwords are maintained in an encrypted database.	No deviations noted.

Authentication servers are utilized to control access, log access attempts, and alert management.	Interviewed staff and reviewed authentication servers to determine if they are utilized to control access, log access attempts, and alert management.	Two out of 4 authentication servers were not configured to alert management of multiple failed access attempts.

Criteria 3.6	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	
Department's Control	**Auditor's Tests of Control**	**Test Results**
Physical access is restricted via card key systems.	Observed and reviewed physical access controls at the CCF and Communications Building to determine if physical access is restricted via card key systems.	No deviations noted.
Card keys are utilized to restrict access to authorized individuals to the CCF and Communications Building.	Reviewed card key system and sampled associated access rights to determine if card keys are utilized to restrict access to the CCF and Communications Building.	One out of the 40 individuals sampled was a former employee who no longer required access to the CCF.
In order to obtain a card key, an ID Badge Request Form is to be completed, approval must be obtained from an authorized manager, and presentation of a valid ID.	Interviewed staff, reviewed the ID Badge Request Form, and sampled ID Badge Request Forms to determine if the Forms were completed, properly approved, and a valid ID was presented prior to obtaining a card key.	Nine out of 9 Forms were properly approved and indicated that a valid ID was presented; however, 5 out of 9 Forms had fields that were not completed.
Visitors are required to sign in and out, in addition to being escorted.	Interviewed security guards, reviewed Security Procedure Manual and Post Orders, a sample of building admittance registers, and tested for compliance at the CCF and Communications Building to determine if visitors are required to sign in and out, in addition to being escorted.	Four out of 24 individuals sampled had expired badges; however, they were permitted access without being verified and escorted.
The CCF and the Communications Building are guarded by security guards.	Interviewed security guards, reviewed security guard contract, and observed security guards to determine that the CCF and Communications Building are guarded by security guards.	No deviations noted.
Video surveillance is utilized to monitor the CCF and the Communications Building.	Observed surveillance cameras to determine that video surveillance is utilized to monitor the CCF and the Communications Building.	No deviations noted.
Procedures exist for the identification and escalation of physical security breaches.	Interviewed staff and security guards, reviewed Security Procedure Manual and Post Orders, and sampled building incident reports to ascertain whether procedures for the identification and escalation of physical security breaches were included and followed.	No deviations noted.
Physical access controls are in place to restrict access to the offsite storage location.	Observed and reviewed physical access controls at the Alternate Data Center and Regional Vault to determine if physical access controls are in place to restrict access to offsite storage locations.	No deviations noted.

Access to the offsite media is limited to authorized Department personnel.	Interviewed staff and reviewed the authorization listings for the Alternate Data Center and Regional Vault to determine if access to offsite media is limited to authorized Department personnel.	Two out of the 40 individuals on the authorization listing no longer required access to the Alternate Data Center. Two out of the 32 individuals on the authorization listing no longer required access to the Regional Vault.

Criteria 3.7 Procedures exist to protect against unauthorized access to system resources.

Department's Control	Auditor's Tests of Control	Test Results
Access to system resources is restricted to authorized personnel through security software.	Interviewed staff, reviewed security reports, and sampled access rights to determine that access to system resources is restricted to authorized personnel through security software.	No deviations noted.
Access to high-level access privileges is limited to security administration personnel.	Interviewed staff and reviewed security reports and a sample of access rights to determine that access to high-level access privileges is limited to security administration personnel.	No deviations noted.
Firewalls and routers are used and configured to prevent unauthorized access via authentication servers, logging servers, banners prohibiting unauthorized access and warning of prosecution and access control lists (ACL) to deny and permit specific types of network traffic.	Interviewed staff and reviewed firewall, router and switch configurations to determine if these devices are used and configured to prevent unauthorized access via authentication servers, logging servers, banners prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific types of network traffic.	Two out of 60 firewalls, routers, and switches were not configured to utilize logging servers and 3 out of 60 were not configured to utilize banners.

Criteria 3.8 Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.

Department's Control	Auditor's Tests of Control	Test Results
The ability to install, modify, and replace operating systems is limited to authorized staff.	Interviewed staff and reviewed security reports and privileged access rights to ascertain whether the ability to install, modify, and replace operating systems is limited to authorized staff.	No deviations noted.
Access to sensitive system functions is restricted to authorized staff.	Interviewed staff and reviewed security reports and access rights to sensitive system functions to ascertain whether sensitive functions were restricted to authorized staff.	No deviations noted.
The Security and Compliance Solutions Team participates in user groups and subscribes to services related to computer viruses.	Interviewed staff and reviewed a sample of subscription notifications to ascertain whether the Security and Compliance Solutions Team participates in user groups and subscribes to services related to computer viruses.	No deviations noted.

Criteria 3.9 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Department makes available encryption technologies and access gateways for the transmission of sensitive or confidential information.	Interviewed staff, reviewed the Enterprise Virtual Private Network (VPN) standard, and the web portal to ascertain whether the Department makes available encryption technologies and access gateways for the transmission of sensitive or confidential information.	No deviations noted.

Criteria related to the execution and incident management used to achieve objectives.

Criteria 3.10 Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Department has tools in place to identify, log, and report security breaches and other incidents.	Interviewed staff, reviewed the General Security For Statewide IT Resources Policy, Security Fundamentals document, Situation Awareness and Continuous Monitoring Process, Major Outage Response Team Process, MORT Tickets, CIRT Case Reports, Remedy system, and observed monitoring tools to determine if the Department has tools in place to identify, log, and report security breaches and other incidents.	No deviations noted.
The Department has tools in place to identify and log network services security breaches.	Interviewed staff and reviewed network device configurations to ascertain whether the Department has tools in place to identify, log, and report security breaches and other incidents.	Two out of 60 devices were not configured to utilize logging servers and logging servers were not consistently defined in 35 out of 60 devices. In addition, log files were not proactively reviewed.
The Department's website provides users instructions for communicating security issues to the CMS Help Desk.	Reviewed the Department website to ascertain whether instructions for communicating security issues to the Help Desk are included.	No deviations noted.
The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets.	Interviewed staff and reviewed the Enterprise Desktop/Laptop Policy, the Mobile Device Security Policy, Laptop Data Encryption Policy, IT Coordinator Guide to BCCS Services, Remedy System, and the listing lost/stolen laptops to determine if the Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets.	The Help Desk was not informed of lost/stolen assets and 4 out of the 5 laptops lost/stolen did not have encryption installed as required by Policy.
The user manuals for applications provide instructions for users to contact the CMS Help Desk to report issues.	Interviewed staff and reviewed user manuals and reference documents to ascertain whether user manuals for applications provide instructions for users to contact the CMS Help Desk to report issues.	No deviations noted.

Criteria related to the system components used to achieve objectives.

Criteria 3.11 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.

Department's Control	Auditor's Tests of Control	Test Results
The Business Reference Model collects and stores information related to application and data processing services provided based on the Data Classification and Protection Policy.	Interviewed staff and reviewed the Data Classification and Protection Policy to determine if the Business Reference Model collects and stores information related to application and data processing services provided based on the Policy.	No deviations noted.
The Business Reference Model is periodically updated by the applicable agency.	Reviewed the BRM listing to determine if the Department is periodically updating and classifying its applications.	The Department had not classified 91 out of 179 of its applications.

Criteria 3.12 Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

Department's Control	Auditor's Tests of Control	Test Results
Department staff is assigned the responsibility for monitoring and ensuring compliance with security policies.	Interviewed staff and reviewed policies and position descriptions to determine if Department staff is assigned the responsibility for monitoring and ensuring compliance with security policies.	The Department had not assigned the responsibility for monitoring and ensuring compliance with security policies.

Criteria 3.13 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability and related security policies.

Department's Control	Auditor's Tests of Control	Test Results
The IT Governance Policy governs the acquisition of systems and technology.	Interviewed staff and reviewed the IT Governance Policy and a sample of project charters to ascertain whether the IT Governance Policy governs the acquisition of systems and technology.	No deviations noted.
As part of the Governance process, agencies are to classify the data and system in accordance with the Data Classification and Protection Policy.	Reviewed the IT Governance Policy and Data Classification and Protection Policy to ascertain whether agencies are to classify the data and system in accordance with the Data Classification and Protection Policy as part of the Governance process.	No deviations noted.
The Remedy Change Management Guide guides the development, implementation and maintenance of systems.	Reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if the Guide provides guidance on the development, implementation and maintenance of systems.	Forty-two RFCs were properly approved; however, 39 of 42 contained fields (primarily date requested) that were not completed as required by the Guide.
Standards provide guidance on the configuration and deployment of network devices.	Interviewed staff and reviewed standards and templates to determine if they provide guidance on the configuration and deployment of network devices.	No deviations noted.
Network diagrams are maintained.	Interviewed staff and reviewed network diagrams to determine if diagrams are maintained.	No deviations noted.

Criteria 3.14 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources to fulfill their responsibilities.

Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Department's position descriptions specify the position's qualifications and responsibilities.	Interviewed staff and reviewed a sample of position descriptions to ascertain whether position descriptions specify qualifications and responsibilities.	No deviations noted.
The State's hiring procedures are followed for the hiring of staff.	Interviewed staff and reviewed documentation outlining the hiring procedures, State of Illinois Personnel Code (20 ILCS 450), and Department of Central Management Service’s Personnel Rules (80 Admin Code 301) to determine if procedures are followed for new hires.	No deviations noted.
New employees are required to have background checks.	Interviewed staff and reviewed a sample of documentation to determine if new employees are required to have background checks.	Eight out of 20 new employees did not have background checks
Annual performance evaluations are completed.	Interviewed staff and reviewed the Employee Evaluation Spreadsheet to determine if annual performance evaluations are completed.	248 employees listed on the employee evaluation spreadsheet had evaluations that were past due.
Staff is provided training.	Interviewed staff and reviewed a sample of employee training records and the list of employees who completed security awareness training to ascertain whether staff is provided training.	No deviations noted.
The Department conducts cross training.	Interviewed staff and reviewed a sample of employee training records to ascertain whether staff is provided training.	No deviations noted.

Change management-related criteria applicable to the system’s availability.

Criteria 3.15 Procedures exist to maintain system components, including configurations consistent with the defined system availability and related security policies.

Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Remedy Change Management Guide provides guidance in maintaining system components, including system configurations.	Interviewed staff and reviewed the Remedy Change Management Guide to ascertain if the Guide provides guidance on maintaining system components, including system configurations.	No deviations noted.
Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if changes are categorized and ranked according to priority and procedures are in place to handle urgent matters.	Forty-two RFCs were properly categorized, and ranked; however, 12 of 14 emergency RFCs did not have all required fields completed.
Standards provide guidance on the configuration and deployment of network devices.	Interviewed staff and reviewed standards and templates to determine if there is guidance on the configuration and deployment of network devices.	No deviations noted.
Tools are in place to assist in the deployment of and reporting on configurations.	Interviewed staff and reviewed standard configurations and a sample of networking devices to ascertain whether tools are in place to assist in the deployment of and reporting on configurations.	No deviations noted.

Criteria 3.16 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

Department's Control	Auditor's Tests of Control	Test Results
The Remedy Change Management Guide provides guidance for the authorization and documentation requirements for changes to systems.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if the Guide provides guidance for the authorization and documentation requirements for changes to systems.	The Guide did not provide documentation requirements for backout plans, testing plans, implementation plans, and post implementation reviews.
High impact changes require backout, test, and implementation plans to be attached to the RFC for the use in the event of a disruption.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if high impact changes require back-out, test, and implementation plans to be attached to the RFC for use in the in the event of a disruption.	Two out of 10 high impact RFCs did not have required backout plans, test plans, or implementation plans.

Criteria 3.17 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).

Department's Control	Auditor's Tests of Control	Test Results
Emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide.	Reviewed the Remedy Change Management Guide, Change Management Policy, and sampled emergency Requests For Changes (RFCs) to ascertain if emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide.	The Guide did not provide documentation requirements for post implementation reviews which were required for emergency changes. Post implementation review documentation was lacking on 12 of 12 emergency RFCs.
Emergency changes require verbal approval prior to implementation. Standard approvals are to be obtained post implementation.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled emergency Requests For Changes (RFCs) to ascertain if emergency changes require verbal approval prior to implementation and if standard approvals are documented post implementation.	No deviations noted.
Emergency changes are communicated to users post implementation via the CAC meeting.	Interviewed staff, reviewed the Remedy Change Management Guide, ECM Sharepoint site, and sampled emergency Requests For Changes (RFCs) to ascertain if emergency changes are communicated to users post implementation via the CAC meeting.	Four of 12 emergency RFCs were not included in CAC meeting minutes.

4.0 – Monitoring: The entity monitors the system and takes action to maintain compliance with its defined availability policies.

Criteria 4.1 The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Department utilizes various tools to review and assess the infrastructure and vulnerabilities.	Interviewed staff and reviewed a sample of Daily Shift Reports, Shift Change Checklists, Remedy System Tickets, monitoring and performance tools, and intruder alert reports to ascertain whether various tools are utilized to review and assess the infrastructure and vulnerabilities.	No deviations noted.
System performance and capacity is monitored via software tools.	Interviewed staff and reviewed software tool reports and a sample of monthly capacity emails to determine if system performance and capacity is monitored via software tools.	No deviations noted.

Criteria 4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
Logs are analyzed either manually or by automated tools to identify trends that may have the potential to impact the Department's ability to achieve system security objectives.	Interviewed staff and reviewed a sample of Daily Shift Reports, Shift Change Checklists, and Remedy System Tickets to ascertain whether logs are analyzed either manually or by automated tools to identify trends that may have the potential to impact the Department's ability to achieve system security objectives. Reviewed a sample of Shift Change Checklists and Daily Shift Reports to determine that a report was completed for each day. Reviewed a sample of referenced Remedy tickets on Daily Shift Reports to determine if a corresponding ticket in the Remedy System had been created.	No deviations noted.
Security issues are addressed with management at various meetings.	Reviewed a sample of communications with users and meeting agendas to ascertain whether security issues are addressed with management at various meetings.	No deviations noted.

Criteria 4.3 Environmental, regulatory, and technological changes are monitored, and their effect on system availability and security is assessed on a timely basis; policies are updated for that assessment.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
Department management considers technological developments, and laws and regulations during the planning process.	Reviewed the BCCS Strategic Plan, a sample of communications with users, agendas, and the Department's website to ascertain whether Department management considers technological developments, and laws and regulations during the planning process.	No deviations noted.
Management conducts meetings with user agencies to determine their future needs.	Reviewed a sample of communications with users, agendas, and the Department's website to ascertain whether the management conducts meetings with user agencies to determine their future needs.	No deviations noted.

TRUST SERVICES - PROCESSING INTEGRITY PRINCIPLE, CRITERIA, RELATED CONTROLS AND TEST OF CONTROLS

1.0 – Policies: The entity defines and documents its policies for the processing integrity of its system.

Criteria 1.1 The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The security policies addressing logical and physical security are reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel and the Chief Information Security Officer.	Reviewed the security policies addressing logical and physical security to determine if the policies had been reviewed and approved by the Department's Director, Deputy Director, Deputy General Counsel, and the Chief Information Security Officer.	A formal process requiring periodic reviews of policies did not exist.
The Department has implemented security policies, which are posted on the Department's website.	Reviewed the Department's website to ascertain whether the Department's security policies are posted on the website.	No deviations noted.

Criteria 1.2 The entity's system processing integrity and related security policies include, but may not be limited to, the following matters:

Criteria A Identifying and documenting the system processing integrity and related security requirements of authorized users.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The security policies identify and document the general security requirements.	Interviewed staff and reviewed security policies to determine if they identify and document general security requirements.	No deviations noted.
The user manuals for applications outline the processing integrity and security requirements of authorized system users.	Interviewed staff and reviewed user manuals and reference documents to ascertain whether user manuals for applications outline the processing integrity and security requirements of authorized users.	No deviations noted.

Criteria B Classifying data based on their criticality and sensitivity; that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The Data Classification and Protection Policy documents the data classification schema used to value and classify information generated, accessed, transmitted or stored.	Interviewed staff and reviewed the Data Classification and Protection Policy to determine if it documents the data classification schema used to value and classify information generated, accessed, transmitted or stored.	No deviations noted.
The IT Resource Access Policy documents the requirements for obtaining access to resources.	Interviewed staff and reviewed the IT Resource Access Policy to determine if the Policy documents the process for obtaining access to resources.	No deviations noted.
The Electronically Stored Information Retention Policy documents the retention requirements for electronic information.	Interviewed staff and reviewed the Electronically Stored Information Retention Policy to determine if the Policy documents the retention requirements of electronic information.	No deviations noted.
The General Security For Statewide IT Resource Policy documents the destruction requirements.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy to determine if it documents destruction requirements.	No deviations noted.

Criteria C Assessing risks on a periodic basis.

Department’s Control	Auditor’s Tests of Control	Test Results
The IT Risk Assessment Policy documents the requirements for assessing risk.	Interviewed staff and reviewed the IT Risk Assessment Policy to determine if it documents the requirements for assessing risk.	No deviations noted.

Criteria D Preventing unauthorized access.

Department’s Control	Auditor’s Tests of Control	Test Results
The IT Resource Access Policy documents controls for preventing unauthorized access.	Interviewed staff and reviewed the IT Resource Access Policy to determine if the Policy documents the process for obtaining access to resources.	The Policy did not include specific requirements or procedures for requesting, modifying, approving, or periodically reviewing user access rights.

Criteria E Adding new users, modifying the access levels of existing users, and removing users who no longer need access.

Department’s Control	Auditor’s Tests of Control	Test Results
The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the Statewide CMS/BCCS Facility Access Policy documents the requirements for granting, assigning and revoking user access.	Interviewed staff and reviewed the IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the Statewide CMS/BCCS Facility Access Policy to determine if the policies document the requirements for granting, assigning and revoking user access.	The IT Resource Access Policy and the General Security For Statewide IT Resources Policy did not include specific requirements or procedures for requesting, modifying, approving, or revoking user access rights. The CMS/BCCS Facility Access Policy did not address requirements for modifying physical access rights.

Criteria F Assigning responsibility and accountability for system processing integrity and related security.

Department’s Control	Auditor’s Tests of Control	Test Results
The IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the General Security For Statewide Network Resource Policy document the responsibilities and accountability of system security.	Interviewed staff and reviewed the IT Resource Access Policy, General Security For Statewide IT Resources Policy, and the General Security For Statewide Network Resource Policy to determine if the policies document the responsibility and accountability of system security.	No deviations noted.

The user manuals for applications outline the responsibility and accountability for the processing integrity and related security.	Interviewed staff and reviewed user manuals and reference documents to ascertain whether user manuals for applications outline the responsibility and accountability for the processing integrity and related security.	No deviations noted.
Criteria G Assigning responsibility and accountability for system changes and maintenance.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Change Management Policy documents the responsibility and accountability of Department staff for system changes and maintenance.	Interviewed staff and reviewed the Change Management Policy to determine if the Policy documents the responsibility and accountability of Department staff for system changes and maintenance.	No deviations noted.
The Manager of the Enterprise Applications & Architecture Division is responsible and accountable for designing the control process for system changes and maintenance related to applications.	Interviewed staff and reviewed the manager’s position description to determine whether the Manager of the Enterprise Applications & Architecture Division is responsible and accountable for designing the control process for changes and maintenance related to applications.	No deviations noted.
Criteria H Testing, evaluating, and authorizing system components before implementation.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Change Management Policy documents the process in which infrastructure changes are to follow.	Interviewed staff and reviewed the Change Management Policy to determine if it documents the process in which infrastructure changes are to follow.	Testing requirements are not addressed in the Policy.
The processes outlined in the Application Lifecycle Management Manual are used to control changes to applications.	Interviewed staff and reviewed the Application Lifecycle Management Manual and a sample of change tickets, change tasks, and move sheets to determine if the processes outlined in the Manual are used to control changes to applications.	A suitable change management process was not in place from July 1, 2012 to November 30, 2012. The Application Lifecycle Management Manual was implemented on December 1, 2012. For changes after November 30, 2012: 10 out of 10 change tickets did not comply with the Manual and 55 out of 77 change tasks did not have appropriate documentation to support the move to production.

Criteria I Addressing how complaints and requests relating to system processing integrity and related security issues are resolved.

Department’s Control	Auditor’s Tests of Control	Test Results
The General Security For Statewide IT Resources Policy states users are responsible for disclosing any actions or behaviors involving a State IT resource and report on actual or suspected breaches.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy to determine if the Policy documents the identification and notification of security breaches and other incidents.	The Policy did not address the entire process for reporting and resolving security issues.
The user manuals for applications provide instructions for users to contact the CMS Help Desk to report issues.	Interviewed staff and reviewed user manuals and reference documents to ascertain whether user manuals for application provide instructions for users to contact the CMS Help Desk to report issues.	No deviations noted.

Criteria J Identifying and mitigating errors and omissions and other system processing integrity and related security breaches and other incidents.

Department’s Control	Auditor’s Tests of Control	Test Results
The General Security For Statewide IT Resources Policy and the Action Plan For Notification of a Security Breach documents the identification and notification of security breaches and other incidents.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy and the Action Plan For Notification of a Security Breach to determine if they document the identification, notification, and mitigation of security breaches and other incidents.	The Policy did not address the entire process for identifying, reporting, and mitigating security issues.
The user manuals for applications provide instructions for users to contact the CMS Help Desk to report issues.	Interviewed staff and reviewed user manuals and reference documents to ascertain whether user manuals for application provide instructions for users to contact the CMS Help Desk to report issues.	No deviations noted.

Criteria K Providing for training and other resources to support its system processing integrity and related system security policies.

Department’s Control	Auditor’s Tests of Control	Test Results
The General Security For Statewide IT Resources Policy documents the security awareness training requirements for Department staff.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy to determine if the Policy documents the security awareness training requirements for Department staff.	No deviations noted.

Criteria L Providing for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies.

Department’s Control	Auditor’s Tests of Control	Test Results
The General Security For Statewide IT Resources Policy and the General Security For Statewide Network Resources Policy indicates it is the responsibility of the users to inform the Department, in writing of any exceptions or special use requirements.	Interviewed staff and reviewed the General Security For Statewide IT Resources Policy and the General Security For Statewide Network Resources Policy to determine if the policies indicate it is the responsibility of the users to inform the Department, in writing of any exceptions or special use requirements.	No deviations noted.

Criteria M	Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The IT Governance Policy documents the Department and the agencies responsibilities for identifying applicable laws, regulations, and other requirements as part of the new IT projects requirements.	Interviewed staff and reviewed the IT Governance Policy to determine if the Policy documents the Department and the agencies responsibilities for identifying applicable laws, regulations, and other requirements as part of the new IT projects requirements**.**	No deviations noted.

Criteria 1.3	Responsibility and accountability for developing and maintaining entity's system processing integrity and related system security policies; changes, updates, and exceptions to those policies are assigned.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of the security policies.	Reviewed the position description for the Chief Information Security Officer to ascertain whether responsibilities for the development and maintenance of security policies are included. Reviewed security policies to determine if approval by the Chief Information Security Officer is documented.	No deviations noted.

2.0 – Communications: The entity communicates its documented system processing integrity policies to responsible parties and authorized users.

Criteria 2.1	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Department has published the Service Catalog on its website, which documents the services provided by the Department.	Interviewed staff and reviewed the Service Catalog on the website to determine if it documents the services provided by the Department.	No deviations noted.

Criteria 2.2	The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Department’s security commitments and obligations are outlined in the Service Catalog, which is posted on the Department’s website.	Reviewed Service Catalog on the website to determine if security commitments and obligations are outlined.	No deviations noted.
The security obligations of Department staff are communicated via the mandatory annual security awareness training, security policies, and periodic emails.	Interviewed staff, reviewed the General Security For Statewide IT Resources Policy, the CMS Security Fundamental web tutorial, and a sample of security communications to determine if security obligations are communicated to Department staff via the mandatory annual security awareness training, security policies, and periodic emails.	No deviations noted.
New Department staff is required to sign a statement signifying that they will comply with the security policies.	Reviewed the CMS Security Fundamentals web tutorial and the training certification list to determine if new Department staff is required to sign a statement signifying that they will comply with the security policies.	No deviations noted.

Department staff reconfirms their compliance with the security policies through the annual security training.	Reviewed the CMS Security Fundamental web tutorial and the listing of Department staff annual certifications to determine if staff reconfirms their compliance with the security policies through the annual security training.	No deviations noted.
Contractors are required to take the annual security awareness training and certify they will comply with security policies.	Interviewed staff and reviewed the CMS Security Fundamental web tutorial and the listing of contractor certifications to determine if contractors are required to take the annual security awareness training and certify they will comply with security policies.	No deviations noted.
The security obligations of users are communicated in several different fashions; policies published on the web, emails, and security notices on the website.	Reviewed a sample of emails and the Department's website to determine if security obligations of users are communicated via policies, security notices, and emails.	No deviations noted.
The user manuals for applications provide instructions for users to contact the CMS Help Desk to report processing and security issues.	Interviewed staff and reviewed user manuals and reference documents to ascertain whether user manuals for applications provide instructions for users to contact the CMS Help Desk to report issues.	No deviations noted.

Criteria 2.3 Responsibility and accountability for the entity's system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The Chief Information Security Officer has primary responsibility and accountability for the development and maintenance of the security policies.	Reviewed the position description for the Chief Information Security Officer to ascertain whether responsibilities for the development and maintenance of security policies are included. Reviewed security policies to determine if approval by the Chief Information Security Officer is documented.	No deviations noted.
Position descriptions have been defined and communicated to employees.	Interviewed staff and reviewed a sample of position descriptions to ascertain whether position descriptions have been defined and communicated to employees.	No deviations noted.
User manuals for applications provide information on processing integrity and security.	Interviewed staff and reviewed the user manuals and reference documents to determine if user manuals for applications provide information on processing integrity and security.	No deviations noted.
Managers of applications are responsible for updates to the applicable user manuals.	Interviewed staff and reviewed the user manuals and reference documents to determine if managers of applications are responsible for updates to the applicable user manuals.	No deviations noted.

Criteria 2.4 The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The process for users to inform the Department of possible security issues and other incidents is posted on the Department's website.	Interviewed staff and reviewed the Department's website to determine if the process for users to inform the Department of possible security issues and other incidents is posted on the website.	Procedures had not been developed to ensure security issues and incidents identified by users are communicated to management for review and resolution.

The General Security For Statewide IT Resources Access Policy documents the process for users to inform their supervisor of security incidents.	Reviewed the General Security For Statewide IT Resources Access Policy to determine if the Policy documents the process for users to inform their supervisor of security incidents.	The Policy does not address the process for supervisors to ensure security incidents identified by users are communicated to management for review and resolution.
User manuals for applications include information concerning processing integrity issues, and the process for informing the CMS Help Desk.	Interviewed staff and reviewed the user manuals and reference documents to determine if user manuals for applications include information concerning processing integrity issues, and the process for informing the CMS Help Desk.	No deviations noted.

Criteria 2.5 Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.

Department's Control	**Auditor's Tests of Control**	**Test Results**
Changes are communicated to users and management via the CAC meetings; which the meeting minutes are posted on the ECM SharePoint site.	Interviewed staff, reviewed a sample of communications, ECM Sharepoint site, a sample of reports, and sampled Requests For Changes (RFCs) to ascertain if changes are communicated to users and management via the CAC meeting minutes posted on the ECM Sharepoint site.	Four of 32 RFCs and 4 of 12 emergency RFCs were not included in CAC meeting minutes.
Agencies have access to the ECM SharePoint site.	Interviewed staff and utilized auditor access to determine if agencies have access to the ECM Sharepoint site.	No deviations noted.
Changes to applications are communicated to users via email or phone.	Reviewed a sample of communication to determine if changes to applications are communicated to users via email or phone.	No deviations noted.
Planned changes to applications are conducted during the scheduled maintenance window.	Interviewed staff and reviewed the systems maintenance window schedules to ascertain whether planned changes to applications are conducted during the scheduled maintenance window.	No deviations noted.

3.0 – Procedures: The entity placed in operation procedures to achieve its documented system processing integrity objectives in accordance with defined policies.

Criteria 3.1 Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair processing integrity commitments and (2) assess the risks associated with the identified threats.

Department's Control	**Auditor's Tests of Control**	**Test Results**
A risk assessment is performed periodically.	Interviewed staff and reviewed the IT Risk Assessment Framework to determine if a risk assessment is performed periodically.	Formal risk assessments, based on the Framework, had not been periodically performed.
As security threats are identified, they are assessed.	Interviewed staff and reviewed the IT Risk Assessment Framework to ascertain whether, as security threats are identified, they are assessed.	Threat analysis and treatment plans based on the Framework had not been developed.

Criteria 3.2 The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies.

Department's Control	Auditor's Tests of Control	Test Results
User manuals for applications provide procedures related to the completeness and accuracy of transactions, which are to be followed by users.	Interviewed staff and reviewed user manuals and reference documents to determine if user manuals for applications provide procedures related to the completeness and accuracy of transactions, which are to be followed by users.	No deviations noted.
Data entry screens contain field edits and range checks.	Interviewed staff, reviewed user manuals and reference documents, and sampled edits to determine if data entry screens contain field edits and range checks.	No deviations noted.
Error handling procedures are followed during data origination to ensure that errors and irregularities are detected, reported, and corrected.	Interviewed staff, reviewed user manuals and reference documents, and sampled agency data to determine if error handling procedures are followed during data origination to ensure that errors and irregularities are detected, reported, and corrected.	No deviations noted.
Logical access controls restrict data entry capabilities to applications to authorized personnel.	Interviewed staff, reviewed user manuals, and observed user sign-on process to determine if logical access controls restrict data entry capabilities to applications to authorized personnel.	No deviations noted.

Criteria 3.3 The procedures related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies.

Department's Control	Auditor's Tests of Control	Test Results
User manuals for applications provide procedures related to the completeness and accuracy of transactions, which are to be followed by users.	Interviewed staff and reviewed user manuals and reference documents to determine if user manuals for applications provide procedures related to the completeness and accuracy of transactions, which are to be followed by users.	No deviations noted.
Data entry screens contain field edits and range checks.	Interviewed staff, reviewed user manuals and reference documents, and sampled edits to determine if data entry screens contain field edits and range checks.	No deviations noted.
Error handling procedures are followed during data origination to ensure that errors and irregularities are detected, reported, and corrected.	Interviewed staff, reviewed the user manuals and reference documents, and sampled agency data to determine if error handling procedures are followed during data origination to ensure that errors and irregularities are detected, reported, and corrected.	No deviations noted.
Applications provide various balancing reports to ensure accuracy of information.	Interviewed staff and reviewed the user manuals and reference documents to determine if applications provide various balancing reports to ensure accuracy of information.	No deviations noted.

Criteria 3.4 The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies.

Department's Control	Auditor's Tests of Control	Test Results
User manuals for applications outline various reports which may be produced for the user agency.	Interviewed staff and reviewed user manuals and reference documents to determine if the user manuals for applications outline various reports which may be produced for the user agency.	No deviations noted.

Criteria 3.5 There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa.

Department’s Control	Auditor’s Tests of Control	Test Results
Each transaction is assigned an identifying number.	Reviewed user manuals and a sample of agency data to determine if each transaction is assigned an identifying number.	No deviations noted.
The Department maintains transaction history for a defined period of time.	Interviewed staff to determine whether the Department maintains transaction history for a defined period of time.	No deviations noted.

Security-related criteria relevant to the system’s processing integrity

Criteria 3.6 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

Criteria A Logical access security measures to access information not deemed to be public.

Department’s Control	Auditor’s Tests of Control	Test Results
Logical access to information is protected through system security software and application security.	Interviewed staff and reviewed system options to determine if logical access is protected through system security software. Reviewed the User Manuals and reference documents for applications, and observed a user to ascertain whether application software is also used to protect access to information.	No deviations noted.
Access to resources is granted to authenticated users based on the user's identity.	Interviewed staff, reviewed security software manual, a sample of user profiles, and system options to determine that access to resources is granted to authenticated users based on the user’s identity.	No deviations noted.
System options have been configured to protect system resources.	Reviewed reports and system settings to determine that system options have been configured to protect system resources.	No deviations noted.
Logical access controls restrict access to applications to authorized Department personnel.	Interviewed staff and reviewed a sample of access rights to determine if logical access controls restrict access to authorized Department personnel.	Eight programmers had inappropriate alter access to production libraries. An excessive number of users had unneeded read access to production libraries. Twenty-nine active IDs were either not specifically assigned or were assigned to departed staff.

Criteria B Identification and authentication of authorized users.

Department’s Control	Auditor’s Tests of Control	Test Results
Users establish their identity and authentication to systems through the use of user IDs and passwords.	Reviewed security software manual, user profiles, system options, and verified user sign-on process to determine that users establish their identity and authentication to systems and applications through the use of user IDs and passwords.	No deviations noted.

Users establish their identity and authentication to applications through the use of user IDs and passwords.	Interviewed staff, reviewed user manuals and reference documents, and observed user identification and authentication to determine if users establish their identity and authentication to systems and applications through the use of user IDs and passwords.	No deviations noted.
Each user agency is responsible for maintaining access rights for all users in that agency.	Interviewed staff and reviewed user manuals to determine if each user agency is responsible for maintaining the access rights for all users in that agency.	No deviations noted.
It is the standard practice to assign each valid user a unique and individual ID.	Interviewed staff and reviewed security reports and RACF procedures to ascertain whether it is the standard practice to assign each valid user a unique and individual ID.	No deviations noted.
Password configurations have been established.	Reviewed system options, password standards, and tested the use of the password standards to determine that password configurations have been established.	No deviations noted.
Users establish their identity and authentication to network services through the use of user IDs and passwords.	Interviewed staff and reviewed the architecture on a sample of authentication servers and a sample of user accounts to determine that users establish their identity and authentication to network services through the use of user IDs and passwords.	Four of 91 user accounts on authentication servers no longer required access.
Password configurations have been established on authentication servers.	Reviewed password configurations and a sample of user accounts determine that password configurations have been established.	Eleven out of 91 user accounts on authentication servers had not been configured to disable accounts after the defined number of unsuccessful login attempts.

Criteria C Registration and authorization of new users.

Department's Control	**Auditor's Tests of Control**	**Test Results**
Network Services required manager review and approval of new access rights. LAN Services utilized the LAN Services Access Authorization Form in order for staff to obtain access rights.	Interviewed staff and reviewed the LAN Services' LAN Equipment Access Rights Standard and a sample of LAN Services Access Authorization Forms to determine if Network Services required manager review and approval of new access rights and LAN Services utilized its Form for staff to obtain access rights.	Documentation of requests, reviews, and approvals was not maintained by all of Network Services.
Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form for new and modification requests and submit via a Remedy Enterprise Service Request.	Interviewed staff and reviewed the New RACF ID Procedures, ESR instructions and a sample of new RACF IDs to determine if Department staff or proxy agency users are required to complete the Mainframe Application Access Request Form for new and modification requests and submit via a Remedy Enterprise Service Request.	Six out of 19 new RACF ID requests did not utilize the Mainframe Security Request Form. Additionally, the Procedures did not address the methods for processing an ESR.
The Mainframe Application Access Request Form indicates the access required and proper approval	Interviewed staff and reviewed the New RACF ID Procedures, ESR instructions and a sample of new RACF IDs to determine if the Mainframe Application Access Request Form indicates the access required and proper approval.	Eleven out of 19 new RACF ID requests were not properly completed or approved.

Criteria D The process to make changes and updates to user profiles.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
Network Services is notified by Personnel of changes in an individual’s employment status and makes changes to user’s access rights accordingly. Changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization Form.	Interviewed staff, reviewed the LAN Services’ LAN Equipment Access Rights Standard, and a sample of LAN Services Access Authorization Forms to determine if Network Services is notified by Personnel of changes in an individual’s employment status and makes changes to user’s access rights accordingly and changes to LAN Services staff access rights are made based on the approved LAN Services Access Rights Authorization Form.	Documentation of changes to user access rights was not maintained by all of Network Services. One of 2 Forms for departed employees had not been completed by LAN Services.
Password resets to Department and proxy agency user profiles are completed by submitting an email request to the Help Desk, or by accessing the Department’s Identity Management website.	Interviewed staff, observed the Help Desk reset process, reviewed the Identity Management website, RACF Password Reset Request Procedures, and a sample of RACF Password Resets to determine if password resets to Department and proxy agency user profiles are completed by submitting an email request to the Help Desk, or by accessing the Department’s Identity Management website.	23 out of 23 RACF Password Resets did not follow the Procedures. (See page 105 for a listing of affected agencies.) In addition, Help Desk staff did not have adequate rights to reset passwords for all agencies.
Bi-monthly the Department’s RACF Coordinator receives a separation report documenting separations from all agencies. The Department’s RACF Coordinator will review and revokes the user’s ID.	Interviewed staff and reviewed a sample of separation reports and a sample of IDs on the separation report to determine if Department’s RACF Coordinator receives a bi-monthly separation report and revokes user IDs.	Documentation was not maintained of the review of the separation report and 1 out of 3 separated individuals’ RACF ID had not been revoked.
Bi-annually, the Department’s RACF Coordinator will send all agencies a listing of their users on the security authorization listing, requesting the agency to review for accuracy, note any modifications, and return to the Department.	Interviewed staff and reviewed update requests in September 2012 and May 2013 to determine if the Department’s RACF Coordinator bi-annually sends all agencies a listing of their users on the security authorization listing, requesting the agency to review for accuracy, note any modifications, and return to the Department.	No deviations noted.
Criteria E Distribution of output restricted to authorized users.		
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The distribution of output is restricted to authorized users via logical and physical security barriers.	Interviewed staff, assessed physical security barriers, observed distribution process, and reviewed logical security controls to ascertain whether the distribution of output is restricted to authorized users via logical and physical security barriers.	No deviations noted.
Distribution of digital output is restricted to authorized users through the management of system software tools or the online viewing software.	Interviewed staff and reviewed logical security controls to ascertain whether the distribution of digital output is restricted to authorized users through the management of system software tools or the online viewing software.	No deviations noted.

Distribution of hardcopy output is restricted through physical and manual controls.	Interviewed staff, assessed physical security barriers, and observed the distribution process to ascertain whether the distribution of hardcopy output is restricted through physical and manual controls.	No deviations noted.
Hardcopy output is printed at a secure facility with security guards.	Interviewed staff and assessed the physical security barriers to ascertain whether hardcopy output is printed at a secure facility with security guards.	No deviations noted.
Upon request for pick up, the individual must identify themselves and be on the authorization listing.	Observed the distribution process and sampled individuals from the authorization list to determine whether individuals must identify themselves and be on the authorization listing for report pick-ups.	One out of 25 individuals was not on the authorization list.
Criteria F	Restriction of access to offline storage, backup data, systems, and media.	
Department's Control	**Auditor's Tests of Control**	**Test Results**
Access to offline storage, backup data, system and media is limited via physical and logical access controls.	Observed and reviewed physical access controls at the CCF, Communications Building, Alternate Data Center, and Regional Vault to determine that access is restricted. Interviewed staff, reviewed group and individual security profiles to determine if logical access controls are in place to limit access to off-line storage, backup data, system and media.	Two out of 40 individuals on the authorization listing no longer required access to the Alternate Data Center. Two out of the 32 individuals on the authorization listing no longer required access to the Regional Vault. Five individuals had excessive or inappropriate logical access rights.
Criteria G	Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	
Department's Control	**Auditor's Tests of Control**	**Test Results**
Logical security controls are in place to restrict access to operating system configurations.	Interviewed staff and reviewed system options, security reports, security software, exits, and access rights to sensitive system functions to determine if logical security controls are in place to restrict access to operating system configurations.	Four active IDs with the capability to modify operating system configurations were either not specifically assigned or were assigned to departed staff. Two IDs had excessive access to operating system resources.
Physical access controls are in place to restrict access to system consoles.	Interviewed staff and observed and reviewed physical access controls at the CCF to determine if physical controls are in place to restrict access to system consoles.	No deviations noted.
Records exist for monitoring and documenting operating system actions.	Interviewed staff and reviewed system files to determine if records exist for monitoring and documenting operating system actions.	No deviations noted.

Operating systems are configured and controlled to promote security and integrity.	Interviewed staff and reviewed system options, security reports, security software, exits, and libraries to determine if operating systems are configured and controlled to promote security and integrity.	No deviations noted.
Security software passwords are maintained in an encrypted database.	Reviewed security software manual and security reports to determine if security software passwords are maintained in an encrypted database.	No deviations noted.
Authentication servers are utilized to control access, log access attempts, and alert management.	Interviewed staff and reviewed authentication servers to determine if they are utilized to control access, log access attempts, and alert management.	Two out of 4 authentication servers were not configured to alert management of multiple failed access attempts.

Criteria 3.7 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, offline storage media, backup media and systems, and other system components such as firewalls, routers, and servers.

Department's Control	**Auditor's Tests of Control**	**Test Results**
Physical access is restricted via card key systems.	Observed and reviewed physical access controls at the CCF and Communications Building to determine if physical access is restricted via card key systems.	No deviations noted.
Card keys are utilized to restrict access to authorized individuals to the CCF and Communications Building.	Reviewed card key system and sampled associated access rights to determine if card keys are utilized to restrict access to the CCF and Communications Building.	One out of the 40 individuals sampled was a former employee who no longer required access to the CCF.
In order to obtain a card key, an ID Badge Request Form is to be completed, approval must be obtained from an authorized manager, and presentation of a valid ID.	Interviewed staff, reviewed the ID Badge Request Form, and sampled ID Badge Request Forms to determine if the Forms were completed, properly approved, and a valid ID was presented prior to obtaining a card key.	Nine out of 9 Forms were properly approved and indicated a valid ID was presented; however, 5 out of 9 had fields that were not completed.
Visitors are required to sign in and out, in addition to being escorted.	Interviewed security guards, reviewed Security Procedure Manual and Post Orders, sampled building admittance registers, and tested for compliance at the CCF and Communications Building to determine if visitors are required to sign in and out, in addition to being escorted.	Four out of 24 individuals sampled had expired badges; however, they were permitted access without being verified and escorted.
The CCF and the Communications Building are guarded by security guards.	Interviewed security guards, reviewed security guard contract, and observed security guards to determine if the CCF and Communications Building are guarded by security guards.	No deviations noted.
Video surveillance is utilized to monitor the CCF and the Communications Building.	Observed surveillance cameras to determine if video surveillance is utilized to monitor the CCF and the Communications Building.	No deviations noted.

Procedures exist for the identification and escalation of physical security breaches.	Interviewed staff and security guards, reviewed Security Procedure Manual and Post Orders, and reviewed a sample of building incident reports to ascertain whether procedures for the identification and escalation of physical security breaches were included and followed.	No deviations noted.
Physical access controls are in place to restrict access to the offsite storage location.	Observed and reviewed physical access controls at the Alternate Data Center and Regional Vault to determine if physical access controls are in place to restrict access to offsite storage locations.	No deviations noted
Access to the offsite media is limited to authorized Department personnel.	Interviewed staff and reviewed the authorization listings for the Alternate Data Center and Regional Vault to determine if access to offsite media is limited to authorized Department personnel.	Two out of the 40 individuals on the authorization listing no longer required access to the Alternate Data Center. Two out of the 32 individuals on the authorization listing no longer required access to the Regional Vault

Criteria 3.8 Procedures exist to protect against unauthorized access to system resources.

Department's Control	**Auditor's Tests of Control**	**Test Results**
Access to system resources is restricted to authorized personnel through security software.	Interviewed staff, reviewed security reports, and a sampled access rights to determine that access to system resources is restricted to authorized personnel through security software.	No deviations noted.
Access to high-level access privileges is limited to security administration personnel.	Interviewed staff, reviewed security reports, and sampled access rights to determine that access to high-level access privileges is limited to security administration personnel.	No deviations noted.
Firewalls and routers are used and configured to prevent unauthorized access via authentication servers, logging servers, banners prohibiting unauthorized access and warning of prosecution and access control lists (ACL) to deny and permit specific types of network traffic.	Interviewed staff and reviewed firewall, router and switch configurations to determine if these devices are used and configured to prevent unauthorized access via authentication servers, logging servers, banners prohibiting unauthorized access and warning of prosecution and ACLs to deny and permit specific types of network traffic.	Two out of 60 firewalls, routers, and switches were not configured to utilize logging servers and 3 out of 60 were not configured to utilize banners.

Criteria 3.9 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The ability to install, modify, and replace operating systems is limited to authorized staff.	Interviewed staff and reviewed security reports and privileged access rights to ascertain whether the ability to install, modify, and replace operating systems is limited to authorized staff.	No deviations noted.
Access to sensitive system functions is restricted to authorized staff.	Interviewed staff and reviewed security reports access rights to sensitive system functions to ascertain whether sensitive functions were restricted to authorized staff.	No deviations noted.
The Security and Compliance Solutions Team participates in user groups and subscribes to services related to computer viruses.	Interviewed staff and reviewed a sample of subscription notifications to ascertain whether the Security and Compliance Solutions Team participates in user groups and subscribes to services related to computer viruses.	No deviations noted.

Criteria 3.10 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Department makes available encryption technologies and access gateways for the transmission of sensitive or confidential information.	Interviewed staff, reviewed the Enterprise Virtual Private Network (VPN) standard, and the web portal to ascertain whether the Department utilizes encryption technologies and access gateways for the transmission of sensitive or confidential information.	No deviations noted.

Criteria related to the execution and incident management used to achieve objectives.

Criteria 3.11 Procedures exist to identify, report, and act upon system processing integrity issues and related security breaches and other incidents.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Department has tools in place to identify, log, and report security breaches and other incidents.	Interviewed staff, reviewed the General Security For Statewide IT Resources Policy, Security Fundamentals document, Situation Awareness and Continuous Monitoring Process, Major Outage Response Team Process, MORT Tickets, CIRT Case Reports, Remedy system, and observed monitoring tools to determine if the Department has tools in place to identify, log, and report security breaches and other incidents.	No deviations noted.
The Department has tools in place to identify and log network services security breaches.	Interviewed staff and reviewed network device configurations to ascertain whether the Department has tools in place to identify, log, and report security breaches and other incidents.	Two out of 60 devices were not configured to utilize logging servers and logging servers were not consistently defined in 35 out of 60 devices. In addition, log files were not proactively reviewed.
The Department's website provides users instructions for communicating security issues to the CMS Help Desk.	Reviewed the Department's website to ascertain whether instructions for communicating security issues to the Help Desk are included.	No deviations noted.
The Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets.	Interviewed staff and reviewed the Enterprise Desktop/Laptop Policy, the Mobile Device Security Policy, Laptop Data Encryption Policy, IT Coordinator Guide to BCCS Services, Remedy System, and the listing lost/stolen laptops to determine if the Enterprise Desktop/Laptop Policy and the Mobile Device Security Policy provided guidance to users for the reporting of lost or stolen assets.	The Help Desk was not informed of the lost/stolen assets and 4 out of the 5 laptops lost/stolen did not have encryption installed as required by Policy.

Criteria related to the system components used to achieve the objectives

Criteria 3.12	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Business Reference Model collects and stores information related to application and data processing services provided based on the Data Classification and Protection Policy.	Interviewed staff and reviewed the Data Classification and Protection Policy to determine if the Business Reference Model collects and stores information related to application and data processing services provided based on the Policy.	No deviations noted.
The Business Reference Model is periodically updated by the applicable agency.	Reviewed the BRM listing to determine if the Department is periodically updating and classifying its applications.	The Department had not classified 91 out of 179 of its applications.

Criteria 3.13	Procedures exist to provide that issues of noncompliance with system processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
Department staff is assigned the responsibility for monitoring and ensuring compliance with security policies.	Interviewed staff and reviewed policies and position descriptions to determine if Department staff is assigned the responsibility for monitoring and ensuring compliance with security policies.	The Department had not assigned the responsibility for monitoring and ensuring compliance with security policies.

Criteria 3.14	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.	
Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The IT Governance Policy governs the acquisition of systems and technology.	Interviewed staff and reviewed the IT Governance Policy and a sample of project charters to ascertain whether the IT Governance Policy governs the acquisition of systems and technology.	No deviations noted.
As part of the Governance process, agencies are to classify the data and system in accordance with the Data Classification and Protection Policy.	Reviewed the IT Governance Policy and Data Classification and Protection Policy to ascertain whether agencies are to classify the data and system in accordance with the Data Classification and Protection Policy as part of the Governance process.	No deviations noted.
The Remedy Change Management Guide guides the development, implementation and maintenance of systems.	Reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if the Guide provides guidance on the development, implementation and maintenance of systems.	Forty-two RFCs were properly approved: however, 39 of 42 contained fields (primarily date requested) that were not completed as required by the Guide.
Standards provide guidance on the configuration and deployment of network devices.	Interviewed staff and reviewed standards and templates to determine if they provide guidance on the configuration and deployment of network devices.	No deviations noted.

Mainframe application changes moved to production libraries are conducted in accordance with Library Services standards and procedures.	Interviewed staff and reviewed Library Services standards and procedures and a sample of moves to production to determine if mainframe application changes moved to production libraries are conducted in accordance with standards and procedures.	All moves in the sample were appropriately authorized; however, the “approver listing” for one agency had not been updated.
Network diagrams are maintained.	Interviewed staff and reviewed network diagrams to determine if diagrams are maintained.	No deviations noted.
The Application Lifecycle Management Manual provides guidance and requirements to implement changes to applications.	Interviewed staff and reviewed the Application Lifecycle Management Manual to determine if the Manual provides guidance and requirements to implement system changes to applications.	A suitable change management process was not in place from July 1, 2012 to November 30, 2012. The Application Lifecycle Management Manual was implemented on December 1, 2012; however, the Manual did not provide guidance or requirements related to: prioritization of requests, required approvals, testing, documentation, or post implementation review.

Criteria 3.15 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting processing integrity and security have qualifications and resources to fulfill their responsibilities.

Department’s Control	**Auditor’s Tests of Control**	**Test Results**
The Department's position descriptions specify the position's qualifications and responsibilities.	Interviewed staff and reviewed a sample of position descriptions to ascertain whether position descriptions specify qualifications and responsibilities.	No deviations noted.
The State's hiring procedures are followed for the hiring of staff.	Interviewed staff and reviewed documentation outlining the hiring procedures, State of Illinois Personnel Code (20 ILCS 450), and Department of Central Management Service’s Personnel Rules (80 Admin Code 301) to determine if procedures are followed for new hires.	No deviations noted.
New employees are required to have background checks.	Interviewed staff and reviewed a sample of documentation to determine if new employees are required to have background checks.	Eight out of 20 new employees did not have background checks

Annual performance evaluations are completed.	Interviewed staff and reviewed the Employee Evaluation Spreadsheet to determine if annual performance evaluations are completed.	248 employees listed on the employee evaluation spreadsheet had evaluations that were past due.
Staff is provided training.	Interviewed staff and reviewed a sample of employee training records and the list of employees who completed security awareness training to ascertain whether staff is provided training.	No deviations noted.
The Department conducts cross training.	Interviewed staff and reviewed a sample of employee training records to ascertain whether staff is provided training.	No deviations noted.

Change management-related criteria applicable to the system's processing integrity.

Criteria 3.16 Procedures exist to maintain system components, including configurations consistent with the defined system processing integrity and related security policies.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Remedy Change Management Guide provides guidance in maintaining system components, including system configurations.	Interviewed staff and reviewed the Remedy Change Management Guide to ascertain if the Guide provides guidance on maintaining system components, including system configurations.	No deviations noted.
Changes are categorized and ranked according to priority, and procedures are in place to handle urgent matters.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if changes are categorized and ranked according to priority and procedures are in place to handle urgent matters.	Foury-two RFCs were properly categorized, and ranked; however, 12 of 14 emergency RFCs did not have all required fields completed.
Standards provide guidance on the configuration and deployment of network devices.	Interviewed staff and reviewed standards and templates to determine if there is guidance on the configuration and deployment of network devices.	No deviations noted.
Tools are in place to assist in the deployment of and reporting on configurations.	Interviewed staff and reviewed standard configurations and a sample of networking devices to ascertain whether tools are in place to assist in the deployment of and reporting on configurations.	No deviations noted.

The processes outlined in the Application Lifecycle Management Manual are used to control changes to applications.	Interviewed staff and reviewed the Application Lifecycle Management Manual and a sample of change tickets, change tasks, and move sheets to determine if the processes outlined in the Manual are used to control changes to applications.	A suitable change management process was not in place from July 1, 2012 to November 30, 2012. The Application Lifecycle Management Manual was implemented on December 1, 2012. For changes after November 30, 2012: 10 out of 10 change tickets did not comply with the Manual and 55 out of 77 change tasks did not have appropriate documentation to support the move to production.
Mainframe application changes moved to production libraries are conducted in accordance with Library Services standards and procedures.	Interviewed staff and reviewed Library Services standards and procedures and a sample of moves to production to determine if mainframe application changes moved to production libraries are conducted in accordance with standards and procedures.	All moves in the sample were appropriately authorized; however, the "approver listing" for one agency had not been updated.
The Manager of the Enterprise Applications & Architecture Division is responsible and accountable for designing the control process for system changes and maintenance related to applications.	Interviewed staff and reviewed the manager's position description to determine whether the Manager of the Enterprise Applications & Architecture Division is responsible and accountable for designing the control process for changes and maintenance to applications.	No deviations noted.
Changes to applications are communicated to users via email or phone.	Reviewed a sample of communication to determine if changes to applications are communicated to users via email or phone.	No deviations noted.

Criteria 3.17 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

Department's Control	**Auditor's Tests of Control**	**Test Results**
The Remedy Change Management Guide provides guidance for the authorization and documentation requirements for changes to systems.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if the Guide provides guidance for the authorization and documentation requirements for changes to systems.	The Guide did not provide documentation requirements for backout plans, testing plans, implementation plans, and post implementation reviews.

High impact changes require backout, test, and implementation plans to be attached to the RFC for the use in the event of a disruption.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled Requests For Changes (RFCs) to ascertain if high impact changes require back-out, test and implementation plans to be attached to the RFC for use in the in the event of a disruption.	Two out of 10 high impact RFCs did not have required backout plans, test plans, or implementation plans.
The processes outlined in the Application Lifecycle Management Manual are used to control changes to applications.	Interviewed staff and reviewed the Application Lifecycle Management Manual and a sample of change tickets, change tasks, and move sheets to determine if the processes outlined in the Manual are used to control changes to applications.	A suitable change management process was not in place from July 1, 2012 to November 30, 2012. The Application Lifecycle Management Manual was implemented on December 1, 2012. For changes after November 30, 2012: 10 out of 10 change tickets did not comply with the Manual and 55 out of 77 change tasks did not have appropriate documentation to support the move to production.
Mainframe application changes moved to production libraries are conducted in accordance with Library Services standards and procedures.	Interviewed staff and reviewed Library Services standards and procedures and a sample of moves to production to determine if mainframe application changes moved to production libraries are conducted in accordance with standards and procedures.	All moves in the sample were appropriately authorized; however, the “approver listing” for one agency had not been updated.

Criteria 3.18 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).		
Department's Control	**Auditor's Tests of Control**	**Test Results**
Emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide.	Reviewed the Remedy Change Management Guide, Change Management Policy, and sampled emergency Requests For Changes (RFCs) to ascertain if emergency changes are required to complete the standard documentation outlined in the Change Management Policy and the Remedy Change Management Guide.	The Guide did not provide documentation requirements for post implementation reviews which were required for emergency changes. Post implementation review documentation was lacking on 12 of 12 emergency RFCs.
Emergency changes require verbal approval prior to implementation. Standard approvals are to be obtained post implementation.	Interviewed staff, reviewed the Remedy Change Management Guide and sampled emergency Requests For Changes (RFCs) to ascertain if emergency changes require verbal approval prior to implementation and if standard approvals are documented post implementation.	No deviations noted.
Emergency changes are communicated to users post implementation via the CAC meeting.	Interviewed staff, reviewed the Remedy Change Management Guide, ECM Sharepoint site, and sampled emergency Requests For Changes (RFCs) to ascertain if emergency changes are communicated to users post implementation via the CAC meeting.	Four of 12 emergency RFCs were not included in CAC meeting minutes.
Emergency changes to applications follow the Application Lifecycle Management Manual.	Interviewed staff and reviewed the Application Lifecycle Management Manual to determine if emergency changes to applications follow the Application Lifecycle Management Manual.	The Manual did not provide guidance related to emergency changes.
Mainframe application changes moved to production libraries are conducted in accordance with Library Services standards and procedures.	Interviewed staff and reviewed Library Services standards and procedures and a sample of moves to production to determine if mainframe application changes moved to production libraries are conducted in accordance with standards and procedures.	All moves in the sample were appropriately authorized; however, the "approver listing" for one agency had not been updated.

Availability-related criteria applicable to the system's processing integrity.

Criteria 3.19 Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Department maintains measures to protect against environmental factors (fire extinguishers, fire suppression, sprinkler system, water detection, power failure, and cooling/heating) at the CCF and the Communications Building.	Observed and reviewed measures to determine if measures are maintained to protect against environmental factors (fire extinguishers, fire suppression, sprinkler system, water detection, power failure, and cooling/heating) at the CCF and Communications Building.	No deviations noted.

Environmental factors are monitored at the CFF and the Communications Building.	Observed the facility automation system and equipment to ascertain whether environmental factors are monitored at the CCF and the Communications Building.	No deviations noted.
Preventive maintenance agreements and scheduled maintenance procedures are in place for environmental factors.	Interviewed staff, reviewed contracts and reviewed maintenance reports to ascertain whether preventive maintenance agreements and scheduled maintenance procedures are in place for environmental factors.	There was no contract for preventive maintenance of the generators. Maintenance/testing reports for the water detection system, sprinkler system, automation system, heating/cooling systems and generators were not available.
The user manuals for applications instruct users to contact the CMS Help Desk to report any issues.	Reviewed user manuals and reference documents for applications to verify that the user manuals provided instructions for users to contact the CMS Help Desk to report issues.	No deviations noted.
Logical access to information is protected through system security software and application security.	Interviewed staff and reviewed system options to determine that logical access is protected through system security software. Reviewed the user manuals and reference documents for applications and observed a user to ascertain whether application software is also used to protect access to information.	No deviations noted.
Physical access controls restrict access via card key systems.	Observed and reviewed physical access controls at the CCF and Communications Building to determine that physical access is restricted via card key systems.	No deviations noted.

Criteria 3.20	Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies.	
Department's Control	**Auditor's Tests of Control**	**Test Results**
CA-Scheduler is utilized to schedule and control backups.	Interviewed staff, reviewed documentation generated from CA-Scheduler to verify a sample of backups, and observed daily schedules to ascertain whether CA-Scheduler is utilized to schedule and control backups.	No deviations noted.
The backups are conducted routinely.	Interviewed staff, reviewed network device configurations, job schedules, backup configuration files, daily and weekly schedules for system backups, and observed agency data backups to determine if backup are conducted routinely.	No deviations noted.
The Department verifies the daily and weekly backups completed successfully.	Interviewed staff, reviewed documentation generated from CA-Scheduler to verify backups, logs, and observed documentation supporting the completion of scheduled agency backups to ascertain whether the Department verifies the daily and weekly backups completed successfully.	No deviations noted.
The Department is notified of failed backups.	Interviewed staff, reviewed email alerts, and observed automated notifications in the Command Center to determine if the Department is notified of failed backup.	No deviations noted.
Failed backups are recorded on the Shift Report.	Interviewed staff and reviewed a sample of Shift Reports to determine whether failed backups are recorded on the Shift Report.	No deviations noted.
The Department takes remedial action on failed backups.	Interviewed staff, reviewed a sample of Shift Reports and an associated Remedy Ticket to ascertain whether the Department takes remedial action on failed backups.	No deviations noted.

The Department has procedures to guide in remediating failed backups.	Interviewed staff and reviewed the BCCS/ISD Cleanup Procedures to determine whether the Department has procedures to guide in remediating failed backups.	No deviations noted.
The DCMS/BCCS Infrastructure Services Recovery Activation Plan is documented.	Reviewed the DCMS/BCCS Infrastructure Services Recovery Activation Plan to verify that the Plan was documented and current.	The Plan had not been updated to address the change from offsite physical backup tapes to the use of virtual tape technology at the Alternate Data Center.
The DCMS/BCCS Infrastructure Services Recovery Activation Plan documents the roles and responsibilities of personnel.	Reviewed the DCMS/BCCS Infrastructure Services Recovery Activation Plan to verify that the Plan documents the roles and responsibilities of personnel.	No deviations noted.
The agencies document their application recovery classification in the Business Reference Module.	Reviewed the Critical Applications Listing and the Business Reference Model (BRM) to determine if agencies documented their recovery classification in the Business Reference Model.	1,335 of 2,224 applications listed in the BRM had not been assigned a recovery classification.
Testing is conducted annually.	Interviewed staff and reviewed testing documentation from tests in November 2012 to determine if testing is conducted annually.	Test documentation for tests November 2012 lacked sufficient detail to determine test results, problems encountered, and problem resolution.
Critical personnel hold current versions of the various disaster recovery documents.	Interviewed staff and reviewed recovery documents to determine whether critical personnel hold current versions of disaster recovery documents.	No deviations noted.
Current versions of the various documents are stored offsite.	Reviewed recovery documents at the Alternate Data Center and Regional Vault to determine if current versions of various documents were maintained offsite.	No deviations noted.
Disaster recovery procedures for applications provide guidance for the restoration and recovery of applications.	Interviewed staff and reviewed disaster recovery procedures for applications to determine if the procedures provide guidance for the restoration and recovery of applications.	Required testing of the CIS Plan had not been conducted. The CTAS Plan had not been updated to reflect changes in the backup process. Documentation for eTime recovery did not outline responsibilities, testing, location of recovery documentation, and the required recovery timeframe.

Criteria 3.21 Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Library Guide and the Media Guide provide guidance on the maintenance, movement and inventory of tape media.	Interviewed staff and reviewed the Library Guide and the Media Guide to ascertain whether they provide guidance on the maintenance, movement and inventory of tape media.	The Guides had not been updated to reflect changes in backup processes and decommission of a facility.
The Department performs an annual verification of media stored at the offsite storage facility.	Interviewed staff and reviewed the November 2012 Inventory Report to determine if the Department performs an annual verification of media stored at the offsite storage facility.	No deviations noted.
Physical backup tapes are stored offsite.	Interviewed staff and reviewed a sample of physical backup tapes to determine if tapes are stored offsite.	No deviations noted.
The Tape Management System tracks the location of physical backups.	Interviewed staff and reviewed a sample of physical tapes to determine whether the Tape Management System tracks the location of physical backups.	No deviations noted.
Virtual tapes are replicated to the Alternate Data Center.	Interviewed staff and observed logs to determine whether virtual tapes are replicated to the Alternate Data Center.	No deviations noted.
Backup systems and data are restored as required.	Interviewed staff and reviewed the Restore Procedures and a sample of Remedy Tickets to determine whether the backup systems and data are restored as required.	No deviations noted.
Backup systems and data are tested as part of the disaster recovery testing.	Interviewed staff and reviewed disaster recovery testing documentation to ascertain whether backup systems and data are tested as part of the disaster recovery testing.	No deviations noted.

4.0 – Monitoring: The entity monitors the system and takes action to maintain compliance with the defined system processing integrity policies.

Criteria 4.1 System processing integrity and security performance are periodically reviewed and compared with the defined system processing integrity and related security policies.		
Department's Control	**Auditor's Tests of Control**	**Test Results**
The Department utilizes various tools to review and assess the infrastructure and vulnerabilities.	Interviewed staff and reviewed a sample of Daily Shift Reports, Shift Change Checklists, Remedy System Tickets, monitoring and performance tools, and intruder alert reports to ascertain whether various tools are utilized to review and assess the infrastructure and vulnerabilities.	No deviations noted.
System performance and capacity is monitored via software tools.	Interviewed staff and reviewed software tool reports and a sample of monthly capacity emails to determine if system performance and capacity is monitored via software tools.	No deviations noted.
The Department reviews the violations and takes necessary action.	Interviewed staff and reviewed a sample of Daily Shift Reports, Shift Change Checklists, and Remedy System Tickets to determine the review of violations and action taken.	No deviations noted.

Criteria 4.2	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system processing integrity and related security policies.	
Department's Control	**Auditor's Tests of Control**	**Test Results**
Logs are analyzed either manually or by automated tools to identify trends that may have the potential to impact the Department's ability to achieve system security objectives.	Interviewed staff and reviewed a sample of Daily Shift Reports, Shift Change Checklists, and Remedy System Tickets to ascertain whether logs are analyzed either manually or by automated tools to identify trends that may have the potential to impact the Department's ability to achieve system security objectives. Reviewed a sample of Shift Change Checklists and Daily Shift Reports to determine that a report was completed for each day. Reviewed a sample of referenced Remedy tickets on Daily Shift Reports to determine if a corresponding ticket in the Remedy System had been created.	No deviations noted.
Security issues are addressed with management at various meetings.	Reviewed a sample of communications with users and meeting agendas to ascertain whether security issues are addressed with management at various meetings.	No deviations noted.

Criteria 4.3	Environmental, regulatory, and technological changes are monitored, their impact on system processing integrity and security is assessed on a timely basis, and policies are updated for that assessment.	
Department's Control	**Auditor's Tests of Control**	**Test Results**
Department management considers technological developments, and laws and regulations during the planning process.	Reviewed the BCCS Strategic Plan, a sample of communications with users, agendas, and the Department's website to ascertain whether Department management considers technological developments, and laws and regulations during the planning process.	No deviations noted.
Management conducts meetings with user agencies to determine their future needs.	Reviewed a sample of communications with users, agendas, and the Department's website to ascertain whether the management conducts meetings with user agencies to determine their future needs.	No deviations noted.

This page intentionally left blank

Other Information Provided by the Department of Central Management Services, Bureau of Communications and Computer Services that is Not Covered by the Service Auditor's Report

Department’s Corrective Action Plan
(Not Examined)

The deficiencies noted in the Auditor’s report were considered significant by both the Auditors and Department Management. The Department is taking the following actions to address the noted deficiencies.

The Department’s Enterprise Applications and Architecture Division has finalized policies and procedures documenting the change control process over application changes and will ensure they are fully implemented. Additionally, we will ensure all changes are tracked from initiation to implementation.

The Department has implemented a new procedure related to password resets under which the bulk of the resets will be performed by the Department’s Help Desk. This centralization ensures that policies and procedures related to password resets are properly communicated to help prevent future non-compliance issues. The compliance issues noted in the report were attributable to one individual not associated with the Help Desk, and the deficiencies have been addressed.

The Department will review the specific policy language regarding monitoring compliance with security policies. It is likely the language will be modified to reflect what can reasonably be accomplished given current resource constraints.

The Department will continue to implement the risk assessment framework developed during the past audit cycle and perform other risk assessments as resources are available.

Principle	**Criteria**	**Corrective Action Plan**
Security	1.1	The Department will review policies at a monthly meeting on security issues and update as appropriate.
	1.2 D	The Department will review policies at a monthly meeting on security issues and update as appropriate.
	1.2 E	The Department will review policies at a monthly meeting on security issues and update as appropriate.
	1.2 H	The Change Policy will be reviewed and updated as appropriate.
	1.2 I	The Department has an active project underway to solidify the processes for reporting and resolving user security issues.
	1.2 J	The Department has an active project underway to solidify the processes for reporting and resolving user security issues.
	2.4	The Department has an active project underway to solidify the processes for reporting and resolving user security issues.
	2.5	The Department will ensure all relevant items are discussed in change meetings and documented.
	3.1	The Department will continue to implement the risk assessment framework developed during the past audit cycle and perform other risk assessments as resources are available.

	3.2 B	The Department will make every possible effort to comply with access and password policies and procedures.
	3.2 C	The Department will develop procedures for granting access to staff and will ensure documentation is completed and maintained.
	3.2 D	The Department will ensure the RACF password reset and revocation procedures are followed by all parties, and that requests for access are documented.
	3.2E	The Department will work to ensure the report pickup procedures are followed.
	3.2F	The Department will review access rights to facilities and correct them as needed.
	3.2 G	The Department will make every possible effort to comply with access and password policies and procedures.
	3.3	The Department will work with its managers and the CMS Bureau of Facilities Management to ensure the ID badge request process is properly followed, building access rules are followed and access rights are revoked as necessary.
	3.4	The Department will review firewall, router and switch configurations and set them at optimal levels.
	3.7	The Department will review firewall, router and switch configurations and set them at optimal levels, and emphasize the importance of following security policies and procedures.
	3.8	The Department has classified all of its major applications and will work on the minor ones as resources permit.
	3.9	The Department will review the specific policy language regarding monitoring compliance with security policies. It is likely the language will be modified to reflect what can reasonably be accomplished given current resource constraints.
	3.10	The Department will emphasize the importance of completing all fields of the change control forms.
	3.11	The Department will continue to emphasize the importance of performing performance evaluations in a timely manner. The Department will work with the A&R Shared Services Group to ensure background checks are completed when needed.
	3.12	The Department will emphasize the importance of completing all fields of the change control forms.
	3.13	The Change Management Guide will be reviewed and updated as necessary and the Department will emphasize compliance.
	3.14	The Change Management Guide will be reviewed and updated as necessary and the Department will emphasize compliance and proper documentation of meetings.
Availability	1.1	The Department will review policies at a monthly meeting on security issues and update as appropriate.
	1.2 D	The Department will review policies at a monthly meeting on security issues and update as appropriate.

Information provided by the Department of Central Management Services – Not Examined

	1.2 E	The Department will review policies at a monthly meeting on security issues and update as appropriate.
	1.2 H	The Department's Enterprise Applications and Architecture Division has finalized policies and procedures documenting the change control process over application changes and will ensure they are fully implemented. Additionally, we will ensure all changes are tracked from initiation to implementation.
	1.2 I	The Department has an active project underway to solidify the processes for reporting and resolving user security issues.
	1.2 J	The Department has an active project underway to solidify the processes for reporting and resolving user security issues.
	1.2 N	The Department will review the Methodology and make appropriate changes.
	2.4	The Department has an active project underway to solidify the processes for the handling of security issues reported by users, including an appropriate escalation procedure for the handling of security breaches and incidents
	2.5	The Department will ensure all relevant items are discussed in change meetings and documented.
	3.1	The Department will continue to implement the risk assessment framework developed during the past audit cycle and perform other risk assessments as resources are available.
	3.2	The Department is in negotiations for a maintenance contract for the generators, and will ensure all maintenance reports are completed. The Department has determined certain end-of-life equipment is not of a critical nature and spares have been procured for failures.
	3.3	The Department will review the Recovery plan and update as needed and emphasize proper documentation of testing. The Department will work with user agencies to provide recovery classifications for their applications.
	3.4	The Department will review its Library and Media Guides and update as needed, and ensure all procedures are followed.
	3.5 B	The Department will make every possible effort to comply with access and password policies and procedures.
	3.5 C	The Department will develop procedures for granting access to staff and will ensure documentation is completed and maintained.
	3.5 D	The Department will ensure the RACF password reset and revocation procedures are followed by all parties, and that requests for access are documented.
	3.5 E	The Department will review access rights to facilities and correct them as needed.
	3.5 F	The Department will make every possible effort to comply with access and password policies and procedures.

	3.6	The Department will work with its managers and the CMS Bureau of Facilities Management to ensure the ID badge request process is properly followed, building access rules are followed and access rights are revoked as necessary.
	3.7	The Department will review firewall, router and switch configurations and set them at optimal levels.
	3.10	The Department will review firewall, router and switch configurations and set them at optimal levels, and emphasize the importance of following security policies and procedures.
	3.11	The Department has classified all of its major applications and will work on the minor ones as resources permit.
	3.12	The Department will review the specific policy language regarding monitoring compliance with security policies. It is likely the language will be modified to reflect what can reasonably be accomplished given current resource constraints.
	3.13	The Department will emphasize the importance of completing all fields of the change control forms.
	3.14	The Department will continue to emphasize the importance of performing performance evaluations in a timely manner. The Department will work with the A&R Shared Services Group to ensure background checks are completed when needed.
	3.15	The Department will emphasize the importance of completing all fields of the change control forms.
	3.16	The Change Management Guide will be reviewed and updated as necessary and the Department will emphasize compliance.
	3.17	The Change Management Guide will be reviewed and updated as necessary and the Department will emphasize compliance and proper documentation of meetings.
Processing Integrity	1.1	The Department will review policies at a monthly meeting on security issues and update as appropriate
	1.2 D	The Department will review policies at a monthly meeting on security issues and update as appropriate
	1.2 E	The Department will review policies at a monthly meeting on security issues and update as appropriate
	1.2 H	Applications and Architecture Division has finalized policies and procedures documenting the change control process over application changes and will ensure they are fully implemented. Additionally, we will ensure all changes are tracked from initiation to implementation.
	1.2 I	The Department has an active project underway to solidify the processes for the handling of security issues reported by users, including an appropriate escalation procedure for the handling of security breaches and incidents.
	1.2 J	The Department has an active project underway to solidify the processes for the handling of security issues reported by users.

	2.4	The Department has an active project underway to solidify the processes for the reporting and resolution of security issues reported by users.
	2.5	The Department will ensure all relevant items are discussed in change meetings and documented.
	3.1	The Department will continue to implement the risk assessment framework developed during the past audit cycle and perform other risk assessments as resources are available.
	3.6 A	The Department will review access rights and correct them as needed.
	3.6 B	The Department will make every possible effort to comply with access and password policies and procedures.
	3.6 C	The Department will develop procedures for granting access to staff and will ensure documentation is maintained.
	3.6 D	The Department will ensure the RACF password reset and revocation procedures are followed by all parties, and that requests for access are documented.
	3.6 E	The Department will work to ensure the report pickup procedures are followed.
	3.6 F	The Department will review access rights to facilities and correct them as needed.
	3.6 G	The Department will make every possible effort to comply with access and password policies and procedures and to ensure server configurations are updated.
	3.7	The Department will work with its managers and the CMS Bureau of Facilities Management to ensure the ID badge request process is properly followed, building access rules are followed and access rights are revoked as necessary.
	3.8	The Department will review firewall, router and switch configurations and set them at optimal levels.
	3.11	The Department will review firewall, router and switch configurations and set them at optimal levels, and emphasize the importance of following security policies and procedures.
	3.12	The Department has classified all of its major applications and will work on the minor ones as resources permit.
	3.13	The Department will review the specific policy language regarding monitoring compliance with security policies. It is likely the language will be modified to reflect what can reasonably be accomplished given current resource constraints.
	3.14	The Department will emphasize the importance of completing all fields of the change control forms and update the Library Services approver listing.
	3.15	The Department will continue to emphasize the importance of performing performance evaluations in a timely manner. The Department will work with the A&R Shared Services Group to ensure background checks are completed when needed.

Information provided by the Department of Central Management Services – Not Examined

	3.16	The Department will emphasize the importance of completing all fields of the change control forms. The Department's Enterprise Applications and Architecture Division has finalized policies and procedures documenting the change control process over application changes and will ensure they are fully implemented. Library Services will update the agency approver listing.
	3.17	The Change Management Guide will be reviewed and updated as necessary and the Department will emphasize compliance and proper documentation. The Department's Enterprise Applications and Architecture Division has finalized policies and procedures documenting the change control process over application changes and will ensure they are fully implemented.
	3.18	The Change Management Guide will be reviewed and updated as necessary and the Department will emphasize compliance and proper documentation. Library Services will update the agency approver listing.
	3.19	The Department is in negotiations for a maintenance contract for the generators, and will ensure all maintenance reports are completed.
	3.20	The Department will review the Recovery plan and update as needed and emphasize proper documentation of testing in all cases. The Department will work with user agencies to provide recovery classifications for their applications.
	3.21	The Department will review its Library and Media Guides and update as needed, and ensure all procedures are followed.

Department's Analysis of Staffing Trends
(Not Examined)

The following table reflects staff losses experienced by the Bureau since FY07. As shown, the Bureau has lost a significant number of staff during this period, which has affected its ability to operate effectively, particularly in some areas. The net staff losses alone would create a challenge, but the numbers do not reflect the institutional knowledge that has been lost, as many long-term employees have reached retirement age. In addition, a recent analysis has shown a high number of staff will be eligible to retire in the next two years. These issues are compounded by difficulty hiring qualified staff, especially in areas that require knowledge and experience on older technologies. Bureau Management has been proactive in attempting to address this issue, but nevertheless, it should be considered a major risk.

Fiscal Year	**Number of Separations**	**Number of Hires**	**Net Staff Loss**
2007	57	39	18
2008	49	12	37
2009	38	23	15
2010	47	9	38
2011	49	7	42
2012	72	16	56
2013	51	37	14
TOTAL	**363**	**143**	**220**

**12 of 37 hires were from consolidation.

Listing of User Agencies of the State of Illinois Information Technology Environment (Not Examined)

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 Lottery
20. Department of Military Affairs
21. Department of Natural Resources
22. Department of Public Health
23. Department of Revenue
24. Department of Transportation
25. Department of Veterans' Affairs
26. Department on Aging
27. East St. Louis Financial Advisory Authority
28. Eastern Illinois University
29. Environmental Protection Agency
30. Executive Ethics Commission
31. General Assembly Retirement System
32. Governors State University
33. Guardianship and Advocacy Commission
34. House of Representatives
35. Human Rights Commission
36. Illinois Arts Council
37. Illinois Civil Service Commission
38. Illinois Commerce Commission
39. Illinois Comprehensive Health Insurance Plan
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 Emergency Management Agency
46. Illinois Finance Authority
47. Illinois Gaming Board
48. Illinois Historic Preservation Agency
49. Illinois Housing Development Authority
50. Illinois Labor Relations Board
51. Illinois Law Enforcement Training and Standards Board
52. Illinois Math and Science Academy

Information provided by the Department of Central Management Services – Not Examined

53. Illinois Medical District Commission
54. Illinois Office of the State's Attorneys Appellate Prosecutor
55. Illinois Power Agency
56. Illinois Prisoner Review Board
57. Illinois Procurement Policy Board
58. Illinois Racing Board
59. Illinois State Board of Investment
60. Illinois State Police
61. Illinois State Toll Highway Authority
62. Illinois State University
63. Illinois Student Assistance Commission
64. Illinois Violence Prevention Authority
65. Illinois Workers' Compensation Commission
66. Joint Committee on Administrative Rules
67. Judges' Retirement System
68. Judicial Inquiry Board
69. Legislative Audit Commission
70. Legislative Ethics Commission
71. Legislative Information System
72. Legislative Printing Unit
73. Legislative Reference Bureau
74. Legislative Research Unit
75. Northeastern Illinois University
76. Northern Illinois University
77. Office of Management and Budget
78. Office of the Architect of the Capitol
79. Office of the Attorney General
80. Office of the Auditor General
81. Office of the Comptroller
82. Office of the Executive Inspector General
83. Office of the Governor
84. Office of the Legislative Inspector General
85. Office of the Lieutenant Governor
86. Office of the Secretary of State
87. Office of the State Appellate Defender
88. Office of the State Fire Marshal
89. Office of the Treasurer
90. Property Tax Appeal Board
91. Senate Operations
92. Sex Offender Management Board
93. Southern Illinois University
94. State Board of Education
95. State Board of Elections
96. State Employees' Retirement System
97. State Police Merit Board
98. State Universities Civil Service System
99. State Universities Retirement System
100. Supreme Court of Illinois
101. Teachers' Retirement System of the State of Illinois
102. University of Illinois
103. Western Illinois University

Listing of User Agencies of the Accounting Information System
(Not Examined)

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 Lottery
11. Department of Military Affairs
12. Department of Natural Resources
13. Department of Public Health
14. Department of Revenue
15. Department on Aging
16. Department of Veterans' Affairs
17. Environmental Protection Agency
18. Guardianship and Advocacy Commission
19. Historic Preservation 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 Gaming Board
30. Illinois Labor Relations Board
31. Illinois Law Enforcement Training and Standards Board
32. Illinois Office of the State's Attorneys Appellate Prosecutor
33. Illinois Prisoner Review Board
34. Illinois Procurement Policy Board
35. Illinois Racing Board
36. Illinois Student Assistance Commission
37. Illinois Violence Prevention Authority
38. Illinois Workers' Compensation Commission

Information provided by the Department of Central Management Services – Not Examined

39. Judges’ Retirement System
40. Judicial Inquiry Board
41. Office of Management and Budget
42. Office of the Attorney General
43. Office of the Auditor General
44. Office of the Executive Inspector General
45. Office of the Governor
46. Office of the Lieutenant Governor
47. Office of the State Appellate Defender
48. Office of the State Fire Marshal
49. Property Tax Appeal Board
50. State Board of Elections
51. State Employees’ Retirement System
52. State Police Merit Board
53. State Universities Civil Service System
54. Supreme Court of Illinois

Listing of Users Agencies of the Central Inventory System
(Not Examined)

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. Historic Preservation Agency
14. Illinois Arts Council
15. Illinois Deaf and Hard of Hearing Commission
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

Information provided by the Department of Central Management Services – Not Examined

Listing of User Agencies of the Central Payroll System

(Not Examined)

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 Lottery
16. Department of Military Affairs
17. Department of Natural Resources
18. Department of Public Health
19. Department of Revenue
20. Department on Aging
21. East St. Louis Financial Advisory Authority*
22. Environmental Protection Agency
23. Executive Ethics Commission
24. General Assembly
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 Emergency Management Agency
37. Illinois Gaming Board
38. Illinois Historic Preservation Agency
39. Illinois Labor Relations Board
40. Illinois Law Enforcement Training and Standards Board
41. Illinois Math and Science Academy
42. Illinois Office of the State's Attorneys Appellate Prosecutor
43. Illinois Power Agency
44. Illinois Prisoner Review Board
45. Illinois Procurement Policy Board
46. Illinois Racing Board
47. Illinois State Board of Investment *
48. Illinois State Police
49. Illinois Student Assistance Commission
50. Illinois Supreme Court Historic Preservation Commission
51. Illinois Violence Prevention Authority
52. Illinois Workers' Compensation Commission
53. Joint Committee on Administrative Rules
54. Judges' Retirement System
55. Judicial Inquiry Board
56. Legislative Audit Commission
57. Legislative Ethics Commission
58. Legislative Information System
59. Legislative Printing Unit
60. Legislative Reference Bureau
61. Legislative Research Unit
62. Office of Management and Budget
63. Office of the Architect of the Capitol
64. Office of the Attorney General
65. Office of the Auditor General
66. Office of the Executive Inspector General
67. Office of the Governor
68. Office of the Lieutenant Governor
69. Office of the State Appellate Defender
70. Office of the State Fire Marshal
71. Office of the Treasurer
72. Property Tax Appeal Board
73. Sex Offender Board
74. State Board of Education
75. State Board of Elections
76. State Employees' Retirement System
77. State of Illinois Comprehensive Health Insurance Board
78. State Police Merit Board
79. State Universities Civil Service System
80. Teachers' Retirement System of the State of Illinois

* Agency Payroll information entered into the system by CPS staff.

Information provided by the Department of Central Management Services – Not Examined

Listing of User Agencies of the Central Time and Attendance System (Not Examined)

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 Insurance
8. Department of Labor
9. Department of Lottery
10. Department of Natural Resources
11. Department of Public Health
12. Department of Revenue
13. Department of Veterans’ Affairs
14. Department on Aging
15. Environmental Protection Agency
16. Guardianship and Advocacy Commission
17. Human Rights Commission
18. Illinois Civil Service Commission
19. Illinois Comprehensive Health Insurance Plans
20. Illinois Criminal Justice Information Authority
21. Illinois Deaf and Hard of Hearing Commission
22. Illinois Educational Labor Relations Board
23. Illinois Gaming Board
24. Illinois Law Enforcement Training and Standards Board
25. Illinois Planning Council on Developmental Disabilities
26. Illinois Procurement Policy Board
27. Illinois Racing Board
28. Illinois Workers’ Compensation Commission
29. Office of the Attorney General
30. Office of the Executive Inspector General
31. Office of the Governor
32. Office of the Lt. Governor
33. Office of the State Fire Marshal
34. Property Tax Appeal Board
35. State Board of Elections

Information provided by the Department of Central Management Services – Not Examined

Listing of User Agencies of the eTime System
(Not Examined)

1. Capitol 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 Regulations
6. Department of Insurance
7. Department of Labor
8. Department of Public Health
9. Department of Revenue
10. Executive Ethics Commission
11. Guardianship and Advocacy Commission
12. Judges Retirement System
13. Office of the Lieutenant Governor
14. Property Tax Appeal Board
15. State Employees Retirement System

Listing of Security Software Proxy Agencies
(Not Examined)

1. Capital Development Board
2. Chicago State University
3. Commission on Government Forecasting and Accountability
4. Court of Claims
5. Department of Agriculture
6. Department of Central Management Services
7. Department of Human Rights
8. Department of Labor
9. Department of Military Affairs
10. Department of Veterans Affairs
11. Eastern Illinois University
12. Executive Ethics Commission
13. Governor’s State University
14. Guardianship and Advocacy Commission
15. House of Representatives
16. Human Rights Commission
17. Illinois Arts Council
18. Illinois Civil Service Commission
19. Illinois Commerce Commission
20. Illinois Community College Board
21. Illinois Comprehensive Health Insurance Plan
22. Illinois Council on Developmental Disabilities
23. Illinois Deaf and Hard of Hearing Commission
24. Illinois Educational Labor Relations Board
25. Illinois Emergency Management Agency
26. Illinois Historic Preservation Agency
27. Illinois Housing Development Authority
28. Illinois Labor Relations Board
29. Illinois Law Enforcement Training and Standards Board
30. Illinois Math and Science Academy
31. Illinois Medical District Commission
32. Illinois Office of the State’s Attorneys Appellate Prosecutor
33. Illinois Power Agency
34. Illinois Prisoner Review Board
35. Illinois Procurement Policy Board
36. Illinois State Board of Investment

Information provided by the Department of Central Management Services – Not Examined

37. Illinois State Toll Highway Authority
38. Illinois State University
39. Illinois Violence Prevention Authority
40. Joint Committee on Administrative Rules
41. Judicial Inquiry Board
42. Legislative Audit Commission
43. Legislative Ethics Commission
44. Legislative Information Systems
45. Legislative Printing Unit
46. Legislative Preference Bureau
47. Legislative Research Unit
48. Northeastern Illinois University
49. Northern Illinois University
50. Office of Management and Budget
51. Office of the Architect of the Capital
52. Office of the Attorney General
53. Office of the Comptroller
54. Office of the Executive Inspector General
55. Office of the Governor
56. Office of the Lieutenant Governor
57. Office of the Secretary of State
58. Office of the State Appellate Defender
59. Office of the State Fire Marshall
60. Office of the Treasurer
61. Property Tax Appeal Board
62. Senate Operations
63. Southern Illinois University
64. State Board of Education
65. State Board of Elections
66. State Police Merit Board
67. State Universities Civil Service System
68. State Universities Retirement System
69. University of Illinois
70. Western Illinois University

ACRONYM GLOSSARY

ACL – Access Control List
ADC – Alternate Data Center
AIS – Accounting Information System
BCCS – Bureau of Communication and Computer Services
Bureau – Bureau of Communication and Computer Services
BRM – Business Reference Model
CAC – Change Advisory Committee
CCF – Central Computer Facility
CICS – Customer Information Control System
CIRT – Critical Incident Response Team
CIS – Central Inventory System
CISO – Chief Information Security Officer
CMC – Customer Management Center
CMS – Central Management Services
CPS – Central Payroll System
CPU – Central Processing Unit
CTAS – Central Time and Attendance
CTO – Chief Technology Officer
DASD – Direct Access Storage Device
DB2 – Database 2
DCMS – Department of Central Management Services
Department – Department of Central Management Services
DNS – Domain Name Service
DP – Data Processing
DR – Disaster Recovery
EAA – Enterprise Application & Architecture
ECM – Enterprise Change Management
EoL – End of Life
EPMO – Enterprise Program Management Office
ESR – Enterprise Service Request
FISMA – Federal Information Security Management Act
FY – Fiscal Year
HIPAA – Health Insurance Portability and Accountability Act
HR – Human Resources
ICN – Illinois Century Network
ID – Identification
ISD – Infrastructure Services Division
ILCS – Illinois Compiled Statutes
IMS – Information Management System
IT – Information Technology
ITG – Information Technology Governance
LAN – Local Area Network
MORT – Major Outage Response Team
NCC – Network Control Center

NIST– National Institute of Standards and Technology
PKI – Public Key Infrastructure
POP – Point of Presence
RACF – Resource Access Control Facility
RFC – Request for Change
RMF – Resource Monitoring Facility
RTC – Regional Technology Center
RTO – Recovery Time Objective
SSL – Secure Socket Level
UPS – Uninterruptible Power Supply
VOIP – Voice Over Internet Protocol
VPN – Virtual Private Network
WAN – Wide Area Network
z/OS – Zero Downtime Operating System
z/VM – Zero Downtime Virtual Machine