DEPARTMENT OF INNOVATION & TECHNOLOGY

SERVICE ORGANIZATION CONTROL 1 REPORT

FOR THE PERIOD

JULY 1, 2017 – JUNE 30, 2018

TABLE OF CONTENTS

Section I

Section II

Section III

SECTION I

INDEPENDENT SERVICES AUDITOR’S REPORT

SPRINGFIELD OFFICE:
ILES PARK PLAZA
740 EAST ASH • 62703-3154
PHONE: 217/782-6046
FAX: 217/785-8222 • TTY: 888/261-2887
FRAUD HOTLINE: 1-855-217-1895

CHICAGO OFFICE:
MICHAEL A. BILANDIC BLDG. • SUITE S-900
160 NORTH LASALLE • 60601-3103
PHONE: 312/814-4000
FAX: 312/814-4006
FRAUD HOTLINE: 1-855-217-1895

OFFICE OF THE AUDITOR GENERAL
FRANK J. MAUTINO

INDEPENDENT SERVICE AUDITOR'S REPORT

Honorable Frank J. Mautino
Auditor General, State of Illinois

Scope

We have examined the State of Illinois, Department of Innovation & Technology's description of its information technology general controls and application controls that support its Information Technology Shared Services System and the State of Illinois, Department of Central Management Services' description of its maintenance and facility support, control and management of physical security, and human resource functions, both of which are included in the "Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services System" for the user agencies throughout the period July 1, 2017, through June 30, 2018, (description) and the suitability of the design and operating effectiveness of the State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services' controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in the State of Illinois, Department of Innovation & Technology's Assertion and the State of Illinois, Department of Central Management Services' Assertion (assertions). The State of Illinois, Department of Central Management Services is a subservice organization that provides maintenance and facility support, control and management of physical security, and human resource functions to the State of Illinois, Department of Innovation & Technology. The State of Illinois, Department of Innovation & Technology's description includes a description of the State of Illinois, Department of Central Management Services' maintenance and facility support, control and management of physical security, and human resource functions used by the State of Illinois, Department of Innovation & Technology to provide the information technology general controls and application controls for its user agencies, including controls relevant to control objectives stated in the description. The controls and control objectives included in the description are those that management of the State of Illinois, Department of Innovation & Technology and management of the State of Illinois, Department of Central Management Services believe are likely to be relevant to user agencies' internal control over financial reporting, and the description does not include those aspects of the Information Technology Shared Services System that are not likely to be relevant to user agencies' internal control over financial reporting.

The State of Illinois, Department of Innovation & Technology uses the Zayo Group, LLC, a subservice organization to provide an alternate data center for off-site storage and replication of the production environment, Microsoft, LLC, a subservice organization to provide cloud hosting services, BMC Software, Inc., a subservice organization to provide Software as a Service, and

Virtustream, Inc, a subservice organization to provide cloud hosting services for the State's Enterprise Resource Planning system. The description includes only the control objectives and related controls of the State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services and excludes the control objectives and related controls of Zayo Group, LLC, Microsoft, LLC, BMC Software, Inc., and Virtustream, Inc. Certain control objectives specified by the State of Illinois, Department of Innovation & Technology can be achieved only if complementary subservice organization controls assumed in the design of the State of Illinois, Department of Innovation & Technology's controls are suitably designed and operating effectively, along with related controls at the State of Illinois, Department of Innovation & Technology. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user agency controls assumed in the design of the State of Illinois, Department of Innovation & Technology's controls are suitability designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user agency controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user agency controls.

The information about the corrective action plan, business continuity and disaster recovery, and user agency listings in Section V, "Other Information Provided by the State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services," is presented by management of the State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services to provide additional information and is not part of the State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services description of the Information Technology Shared Services System made available to user agencies during the period July 1, 2017 to June 30, 2018. Information about the State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services corrective action plan, business continuity and disaster recovery, and user agency listings has not been subjected to procedures applied in the examination of the description of the Information Technology Shared Services System and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Information Technology Shared Services System and, accordingly, we express no opinion on it.

Service Organization Responsibilities

In section II, the State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services have provided their assertions about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services are responsible for preparing the description and their assertions, including the completeness, accuracy, and method of presentation of the description and assertions, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertions, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted 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 and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on criteria in management's assertions, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period July 1, 2017, to June 30, 2018. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of control involves:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertions.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization and subservice organization in their assertions.

Inherent Limitations

The description is prepared to meet the common needs of the user agencies and their auditors who audit and report on user agencies' financial statements and may not, therefore, include every aspect of the system that each user agency may consider important in its own particular environment. Because of their nature, controls at a service organization or subservice organizations may not prevent, or detect and correct, all misstatements in processing or reporting transactions. 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 achieve the related control objectives, is subject to the risk that controls at a service organization or a subservice organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in section IV.

Opinion

The accompanying description of the State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System includes the utilization of subservice providers. However, the State of Illinois, Department of Innovation & Technology did not include in their description complementary subservice organization controls. We believe such information should be included in management's description of its system because the information is relevant to user agencies' internal control over financial reporting.

The accompanying description of the State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System did not include information regarding the configuration standards and installation requirements for midrange devices. We believe that such information should be included in management's description of its system because the information is relevant to user agencies' internal control over financial reporting.

The accompanying description of the State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System did not include the secondary mainframe operating system, NOMAD. We believe that such information should be included in management's description of its system because the information is relevant to user agencies' internal control over financial reporting

The accompanying description of the State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System did not include all interfaces and protocols available to user agencies to transmit data. We believe that such information should be included in management's description of its system because the information is relevant to user agencies' internal control over financial reporting.

The accompanying description of the State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System did not include the process for the termination of physical access. We believe that such information should be included in management's description of its system because the information is relevant to user agencies' internal control over financial reporting.

The accompanying description of the State of Illinois, Department Central Management Services' services did not include the process for physical access provisioning for vendor contractors. We believe that such information should be included in management's description of its system because the information is relevant to user agencies' internal control over financial reporting.

The accompanying description of the State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System did not include the mass approval and load process for users transitioning to the ERP. We believe that such information should be included in management's description of its system because the information is relevant to user agencies' internal control over financial reporting.

The accompanying description of the State of Illinois, Department of Innovation & Technology states risks from potential and newly discovered vulnerabilities are assessed through interaction with security experts and vendor subscription services. The Department also contracts with vendors to receive patch vulnerability information at the earliest possible time. The State of Illinois, Department of Innovation & Technology did not provide sufficient appropriate evidence to determine the accuracy of the statement. As a result, we were unable to determine its accuracy.

The accompanying description of the State of Illinois, Department of Innovation & Technology states the IT Risk Assessment Policy is located on the website. Our testing determined the IT Risk Assessment Policy is no longer utilized and is not located on the website.

The accompanying description of the State of Illinois, Department of Innovation & Technology states job descriptions are to be approved by the Department of Central Management Services' Division of Technical Services. Our testing determined the Department of Central Management Services' Division of Technical Services only approves job descriptions for code positions.

The accompanying description of the State of Illinois, Department of Innovation & Technology states ethics training is provided to newly hired contractors. Our testing determined ethics training is not provided to vendor contractors.

The accompanying description of the State of Illinois, Department of Innovation & Technology states newly hired contractors are provided the DCMS Policy Manual and any subsequent changes. Our testing determined the DCMS Policy Manual and subsequent changes are not provided to contractors.

The accompanying description of the State of Illinois, Department of Innovation & Technology states upon completion of a AIS, CIS, CTAS, or CPS change, developers are to obtain user acceptance approvals via email. Our testing determined user acceptance was not obtained.

The accompanying description of the State of Illinois, Department of Innovation & Technology states bi-monthly (every other month) the Security Software Administrator is to receive a separation report. Our testing determined the Security Software Administrator receives the separation report semi-monthly (twice per month).

The accompanying description of the State of Illinois, Department of Innovation & Technology states the Remote Monitoring Facility reports are run weekly and monthly. Our testing determined the Resource Measurement Facility reports are run monthly.

The accompanying description of the State of Illinois, Department of Innovation & Technology states MOVEit File Transfer Protocol and SFTP transmissions are used to transmit data between the Department and user agencies. Our testing determined MOVEit secure file transfer software resides on a SFTP server and the Department utilizes FTPS for mainframe data transmissions.

The accompanying description of the State of Illinois, Department of Innovation & Technology states errors that occur on data file transmission with MOVEit and SFTP systems result in an automated notification being sent to the Production Control Team for resolution. Our testing determined the applicable agency receives notification and the Production Control Team only receives notification for FTPS errors.

The accompanying description of the State of Illinois, Department of Innovation & Technology states MOVEit errors are recorded in the Shift Change Checklist and a Remedy ticket is created. Our testing determined MOVEit errors are not recorded in the Shift Change Checklist and a Remedy ticket is only created if an agency contacts the IT Service Desk for assistance with an FTPS error.

The accompanying description of the State of Illinois, Department of Innovation & Technology states the Isilon has a call home feature that will notify vendor support and the Enterprise Storage and Backup group during any disc or hardware failure. Our testing determined the Isilon call home feature only notifies the vendor.

The accompanying description of the State of Illinois, Department of Central Management Services' services states preventive maintenance agreements for the environmental measures have been entered into. Our testing determined a maintenance agreement had not been entered into for the water detection system; the Department of Central Management Services' staff maintains it.

The accompanying description of the State of Illinois, Department of Innovation & Technology states ERP defect transport requests to the quality region are to be requested and approved. However, the IL ACT (ERP) Change Management Policy & Procedures did not document who was to approve the ERP defect transport request to the quality region. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance that application programs and environment changes are properly authorized, tested, approved and implemented to result in complete, accurate, and timely processing and reporting that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states ERP Change Requests are to be completed, validated, reviewed and approved. However, the IL ACT (ERP) Change Management Policy & Procedures did not document the information which the Project Management Office was to review, who was to validate the requirements, the information the vendor lead is to review, the prioritization for estimates, who was to approve the estimates, and who was to complete the Solution Architect review. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance that application programs and environment changes are properly authorized, tested, approved and implemented to result in complete, accurate, and timely processing and reporting that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states ERP Change Request transport requests to the quality region are to be requested and approved. However, the IL ACT (ERP) Change Management Policy & Procedures did not document who was to approve the ERP Change Request transport request to the quality region. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance that application programs and environment changes are properly authorized, tested, approved and implemented to result in complete, accurate, and timely processing and reporting that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states that in the event of a major outage or infrastructure failure, a MORT was to be activated. However, a complete and accurate population of MORTs was not provided. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance that agency calls that are relevant to user entities' internal control over financial reporting are responded to, tracked and resolved in a timely manner."

The accompanying description of the State of Illinois, Department of Innovation & Technology states for modifications to access rights, an agency IT Coordinator was to submit an approved ESR. However, a complete and accurate population of modifications to access rights was not provided. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states an agency human resource director was to submit an approved ESR for the establishment of an agency eTime Administrator. However, a complete and accurate population of established eTime Administrators was not provided. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states that on an annual basis, the Security Software Coordinator conducts a review of security software IDs with powerful privileges. However, the Department did not document such reviews. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states the Incident Reports are to be reviewed by the Chief Information Security Officer. However, the Department did not document such reviews. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and deviation, problems, and errors are identified, tracked, recorded and resolved in a complete and timely manner that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states System Management Facility records are to be reviewed weekly by the manager of Mainframe Software Support. However, the Department did not document such reviews. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance that the environment is configured as authorized in order to support application controls and to protect data from unauthorized changes that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Central Management Services' services states security guards are to complete incident reports as needed. However, a complete and accurate population of incident reports was not provided. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance that physical access to facilities and resources is restricted to authorized individuals and environmental controls are in place to protected equipment and facilities that are relevant to user entities' internal control over financial reporting."

In our opinion, because of the matters referred to in the preceding paragraphs, in all material respects, based on the criteria described in the State of Illinois, Department of Innovation & Technology's assertion and the State of Illinois, Department of Central Management Services' assertion:

a. the description does not fairly present the State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System and the State of Illinois, Department of Central Management Services' maintenance and facility support, control and management of physical security, and human resource functions used by the State of Illinois, Department of Innovation & Technology that were designed and implemented throughout the period July 1, 2017, to June 30, 2018.

b. the controls of the State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services related to the control objectives stated in the description were not suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2017 to June 30, 2018.

c. the controls of the State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services did not operate effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2017, to June 30, 2018.

Other Reporting Required by Government Auditing Standards

In accordance with *Government Auditing Standards*, we have also issued our report dated August 8, 2018 on our consideration of the State of Illinois, Department of Innovation & Technology's internal control over (1) fairly presenting the State of Illinois, Department of Innovation & Technology's description of its Information Technology Shared Services System throughout the period July 1, 2017 through June 30, 2018, and (2) establishing and maintaining effective internal control over the suitable design and operating effectiveness of the controls related to the control objectives within the State of Illinois, Department of Innovation & Technology's description of its Information Technology Shared Services System throughout the period July 1, 2017 through June 30, 2018 (internal control over reporting) and on our tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, and other matters, limited to the scope of this report. The purpose of that report is solely to describe the scope of our testing of internal control over reporting and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the State of Illinois, Department of Innovation & Technology's internal control over reporting or on compliance. That report is an integral part of an examination performed in accordance with *Government Auditing Standards* in considering the State of Illinois, Department of Innovation & Technology's internal control over reporting and compliance.

In accordance with *Government Auditing Standards*, we have also issued our report dated August 8, 2018 on our consideration of the State of Illinois, Department of Central Management Services' internal control over (1) fairly presenting the State of Illinois, Department of Central Management Services' description of its maintenance and facility support, control and management of physical security, and human resource functions throughout the period July 1, 2017, through June 30, 2018, and (2) establishing and maintaining effective internal control over the suitable design and operating effectiveness of the controls related to the control objectives within the State of Illinois, Department of Central Management Services' description of its maintenance and facility support, control and management of physical security, and human resource functions throughout the period July 1, 2017 through June 30, 2018 (internal control over reporting) and on our tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, and other matters, limited to the scope of this report. The purpose of that report is solely to describe the scope of our testing of internal control over reporting and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the State of Illinois, Department of Central Management Services' internal control over reporting or on compliance. That report is an integral part of an examination performed in accordance with *Government Auditing Standards* in considering the State of Illinois, Department of Central Management Services' internal control over reporting and compliance.

Restricted Use

This report is intended solely for the information and use of the Department of Innovation & Technology, the Department of Central Management Services, user agencies of the Department of Innovation & Technology's the Information Technology Shared Services System during some or all of the period July 1, 2017 to June 30, 2018, and their auditors who audit and report on such user agencies' financial statements or internal controls over financial reporting and have sufficient understanding to consider it, along with other information, including information about controls implemented by user agencies themselves, when assessing the risks of material misstatement of user agencies' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

SIGNED ORIGINAL ON FILE
William J. Sampias, CISA
Director, Information Systems Audits

SIGNED ORIGINAL ON FILE
Mary Kathryn Lovejoy, CPA, CISA
Senior Audit Manager

August 8, 2018
Springfield, Illinois

SECTION II

DEPARTMENT OF INNOVATION & TECHNOLOGY’S ASSERTION REGARDING THE INFORMATION TECHNOLOGY SHARED SERVICES SYSTEM

&

DEPARTMENT OF CENTRAL MANAGEMENT SERVICES’ ASSERTION REGARDING THE INFORMATION TECHNOLOGY SHARED SERVICES SYSTEM

Illinois Department of Innovation & Technology

Bruce Rauner, Governor
Kirk Lonbom, Acting Secretary

Assertion of the Management of the Department of Innovation & Technology

Honorable Frank J. Mautino
Auditor General, State of Illinois

We have prepared the description of State of Illinois, Department of Innovation & Technology's Information Technology Shared Services system entitled "Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services System" for the information technology general controls and application controls throughout the period July 1, 2017, to June 30, 2018 (description) for user agencies of the system during some or all of the period July 1, 2017, to June 30, 2018, and their auditors who audit and report on such user agencies' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user agencies of the system themselves when assessing the risks of material misstatements of user agencies' financial statements.

The State of Illinois, Department of Innovation & Technology uses the State of Illinois, Department of Central Management Services, a subservice organization, to provide maintenance and facility support, control and management of physical security, and human resource functions. The State of Illinois, Department of Innovation & Technology's description includes a description of the State of Illinois, Department of Central Management Services' services used by the Department of Innovation & Technology to provide Information Technology Shared Services system to user agencies, including controls relevant to the control objectives stated in the description. The State of Illinois, Department of Central Management Services' assertion is presented in section II.

The State of Illinois, Department of Innovation & Technology also uses the Zayo Group, LLC, a subservice organization to provide an alternate data center for off-site storage and replication of the production environment, Microsoft, LLC, a subservice organization to provide cloud hosting services, BMC Software, Inc., a subservice organization to provide Software as a Service, and Virtustream, Inc, a subservice organization to provide cloud hosting services for the State's Enterprise Resource Planning system. The description includes only the control objectives and related controls of the State of Illinois, Department of Innovation & Technology and the State of Illinois, Department of Central Management Services and excludes the control objectives and related controls of Zayo Group, LLC, Microsoft, LLC, BMC Software, Inc., and Virtustream, Inc. Certain control objectives specified by the State of Illinois, Department of Innovation & Technology can be achieved only if complementary subservice organization controls assumed in the design of the State of Illinois, Department of Innovation & Technology's controls are suitably designed and operating effectively, along with related controls at the State of Illinois, Department of Innovation & Technology.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user agency controls assumed in the design of the State of Illinois, Department of Innovation & Technology's controls are suitably designed and operating effectively, along with related controls at the State of Illinois, Department of Innovation & Technology. The description does not extend to controls of the user agencies.

We confirm, to the best of our knowledge and belief, that:

1) Except for the matters described in the following paragraphs, the description fairly presents the Information Technology Shared Service System made available to user agencies of the system during some or all of the period July 1, 2017, to June 30, 2018 for the information technology general controls and application controls as it relates to controls that are likely to be relevant to user agencies' internal control over financial reporting. The criteria we used in making our assertion were that the description:

   a) Presents how the system made available to user agencies of the system was designed and implemented to provide the information technology general controls and application controls, including, if applicable:
      i) The types of services provided, including, as appropriate, the information technology general controls and application controls.
      ii) How the system captures and addresses significant events and conditions.
      iii) The services performed by the subservice organizations, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
      iv) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user agency controls assumed in the design of the controls.
      v) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

   b) Includes relevant details of changes to the State of Illinois, Department of Innovation & Technology's system during the period covered by the description.

   c) Does not omit or distort information relevant to the State of Illinois, Department of Innovation & Technology's system, while acknowledging that the description is prepared to meet the common needs of the user agencies of the system and their user auditors, and may not, therefore, include every aspect of the Information Technology Shared Services System that each individual user agency of the system and its auditor may consider important in its own particular environment.

   The accompanying description, of the State of Illinois, Department of Innovation & Technology, of Information Technology Shared Services System includes the utilization of subservice providers. However, we did not include in the description complementary subservice organization controls. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

   The accompanying description, of the State of Illinois, Department of Innovation & Technology, of Information Technology Shared Services System does not include information regarding the configuration standards and installation requirements for midrange devices. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

The accompanying description, of the State of Illinois, Department of Innovation & Technology, of Information Technology Shared Services System does not include the secondary mainframe operating system, NOMAD. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

The accompanying description, of the State of Illinois, Department of Innovation & Technology, of Information Technology Shared Services System does not include all interfaces and protocols available to user agencies to transmit data. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

The accompanying description, of the State of Illinois, Department of Innovation & Technology, of Information Technology Shared Services System does not include the process for termination of physical access. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

The accompanying description, of the State of Illinois, Department of Innovation & Technology, of Information Technology Shared Services System does not include the mass approval and load process for users transitioning to the ERP. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states Risks from potential and newly discovered vulnerabilities are assessed through interaction with security experts and vendor subscription services. The Department also contracts with vendors to receive patch vulnerability information at the earliest possible time. However, we did not provide sufficient appropriate evidence in order for the Service Auditors to determine the accuracy of the statement. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states the IT Risk Assessment Policy is located on the website. However, the IT Risk Assessment Policy is no longer utilized and is not located on our website. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states job descriptions are to be approved by the Department of Central Management Services' Division of Technical Services. However, the Department of Central Management Services' Division of Technical Services only approves job descriptions for code positions. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states ethics training is provided to newly hired contractors. However, ethics training is not provided to vendor contractors. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states newly hired contractors are provided the DCMS Policy Manual and any subsequent changes. However, the DCMS Policy Manual and subsequent changes are not provided to contractors. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states upon completion of AIS, CIS, CTAS, or CPS changes, developers are to obtain user acceptance approvals. However, user acceptance is not obtained. As a result, the description is not fairly presented

The accompanying description of the State of Illinois, Department of Innovation & Technology states bi-monthly, the Security Software Administrator is to receive a separation report. However, the Security Software Administrator receives the separation report semi-monthly. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states Remote Monitoring Facility is run weekly and monthly. However, Resource Measurement Facility Reports are run monthly. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states MOVEit File Transfer Protocol and SFTP transmissions are used to transmit data between the Department and user agencies. However, MOVEit secure file transfer software resides on a SFTP server and the Department utilizes FTPS for mainframe data transmissions. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states errors that occur on data file transmission with MOVEit and SFTP systems result in an automated notification being sent to the Production Control Team for resolution. However, the applicable agency receives notification and the Production Control Team only receive notification for FTPS errors. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states MOVEit errors are recorded in the Shift Change Checklist and a Remedy ticket is created. However, MOVEit errors are not recorded in the Shift Change Checklist and a Remedy ticket is only created if an agency contacts the IT Service Desk for assistance with an FTPS error. As a result, the description is not fairly presented.

The accompanying description of the State of Illinois, Department of Innovation & Technology states the Isilon has a call home feature that will notify vendor support and the Enterprise Storage and Backup group during any disc or hardware failure. However, the Isilon call home feature only notifies the vendor. As a result, the description is not fairly presented.

Except for the matters described in the following paragraphs, the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period July 1, 2017, through June 30, 2018 to achieve those control objectives if user agencies applied the complementary user agency controls assumed in the design of the State of

Illinois, Department of Innovation & Technology's controls throughout the period July 1, 2017, to June 30, 2018. The criteria we used in making this assertion were that:

a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the State of Illinois, Department of Innovation & Technology.

b) The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

c) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

The accompanying description of the State of Illinois, Department of Innovation & Technology states that in the event of a major outage or infrastructure failure, a MORT was to be activated. However, a complete and accurate population of MORTs was not provided to the Service Auditors. As a result, the controls were not suitably designed to achieve the control objective "Controls provide reasonable assurance that agency calls that are relevant to user entities' internal control over financial reporting are responded to, tracked and resolved in a timely manner."

The accompanying description of the State of Illinois, Department of Innovation & Technology states that an agency human resource director was to submit an approved ESR for the establishment of an agency eTime Administrator. However, a complete and accurate population of established eTime Administrators was not provided to the Service Auditors. As a result, the controls were not suitably designed to achieve the control objective "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states for modifications to access rights, an agency IT Coordinator was to submit an approved ESR. However, a complete and accurate population of modifications to access rights was not provided to the Service Auditors. As a result, the controls were not suitably designed to achieve the control objective "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states that ERP defect transport requests to the quality region are to be requested and approved. However, the IL ACT (ERP) Change Management Policy & Procedures does not document who was to approve the ERP defect transport request to the quality region. As a result, the controls were not suitably designed to achieve the control objective "Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and deviation, problems, and errors are identified, tracked, recorded and resolved in a complete and timely manner that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states that ERP Change Requests are to be completed, validated, reviewed and approved. However, the IL ACT (ERP) Change Management Policy & Procedures does not document; the information in which the Project Management Office was to review, who was validate the requirements, the information the vendor lead is to review, the prioritization for estimates, who was to approve the estimates, and who was to complete the Solution Architect review. As a result, the controls were not suitably designed to achieve the control objective "Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and deviation, problems, and errors are identified, tracked, recorded and resolved in a complete and timely manner that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states that ERP Change Request transport requests to the quality region are to be requested and approved. However, the IL ACT (ERP) Change Management Policy & Procedures does not document who was to approve the ERP change request transport request to the quality region. As a result, the controls were not suitably designed to achieve the control objective "Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and deviation, problems, and errors are identified, tracked, recorded and resolved in a complete and timely manner that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states on an annual basis, the Security Software Coordinator conducts a review of security software IDs with powerful privileges. However, we did not document such reviews. As a result, the controls were not suitably designed to achieve the control objective "Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states the Incident Reports are to be reviewed by the Chief Information Security Officer. However, we did not document such reviews. As a result, the controls were not suitably designed to achieve the control objective "Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and deviation, problems, and errors are identified, tracked, recorded and resolved in a complete and timely manner that are relevant to user entities' internal control over financial reporting."

The accompanying description of the State of Illinois, Department of Innovation & Technology states that System Management Facility records are to be reviewed weekly by the manager of

Mainframe Software Support. However, we did not document such reviews. As a result, the controls were not suitably designed to achieve the control objective "Controls provide reasonable assurance that the environment is configured as authorized in order to support application controls and to protect data from unauthorized changes that are relevant to user entities' internal control over financial reporting."

SIGNED ORIGINAL ON FILE

Kirk Lonbom
Secretary, Acting
Department of Innovation & Technology
August 8, 2018

CMS

ILLINOIS Bruce Rauner, Governor
DEPARTMENT OF CENTRAL MANAGEMENT SERVICES
Tim McDevitt, Acting Director

Assertion of the Management of the Department of Central Management Services

Honorable Frank J. Mautino
Auditor General, State of Illinois

The State of Illinois, Department of Central Management Services provides maintenance and facility support, control and management of physical security, and human resource function services to the State of Illinois, Department of Innovation & Technology. The services provided by the State of Illinois, Department of Central Management Services are a part of the State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System. We are responsible for the description of the State of Illinois, Department of Central Management Services' maintenance and facility support, control and management of physical security, and human resource function services provided to the State of Illinois, Department of Innovation & Technology and user agencies of the State of Illinois, Department of Innovation & Technology's Information Technology Shared Service System, which is included in the "State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System entitled "Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services System" for the information technology general controls and application controls throughout the period July 1, 2017, to June 30, 2018 (description) for user agencies of the system during some or all of the period July 1, 2017, to June 30, 2018, and their auditors who audit and report on such user agencies' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, when assessing the risks of material misstatement of user agencies' financial statements.

We confirm, to the best of our knowledge and belief, that:

1) Except for the matter described in the following paragraph, the description fairly presents the State of Illinois, Department of Central Management Services' maintenance and facility support, control and management of physical security, and human resource functions services made available to the State of Illinois, Department of Innovation & Technology and user agencies of the State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System during some or all of the period July 1, 2017, to June 30, 2018 for the information technology general controls and application controls, as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making our assertion were that the description:

   a) Presents how the maintenance and facility support, control and management of physical security, and human resource function made available to State of Illinois, Department of Innovation & Technology and user agencies of the State of Illinois, Department of Innovation & Technology's Information Technology Shared Services System were designed and implemented to provide the information technology general controls and application controls, including, if applicable:

i) The types of services provided by the State of Illinois, Department of Central Management Services, including, as appropriate.
ii) How the maintenance and facility support, control and management of physical security, and human resource function services capture and address significant events and conditions, other than transactions.
iii) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user agency controls assumed in the design of the State of Illinois, Department of Innovation & Technology's controls.
iv) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b) Includes relevant details of changes to the State of Illinois, Department of Central Management Services' services during the period covered by the description.

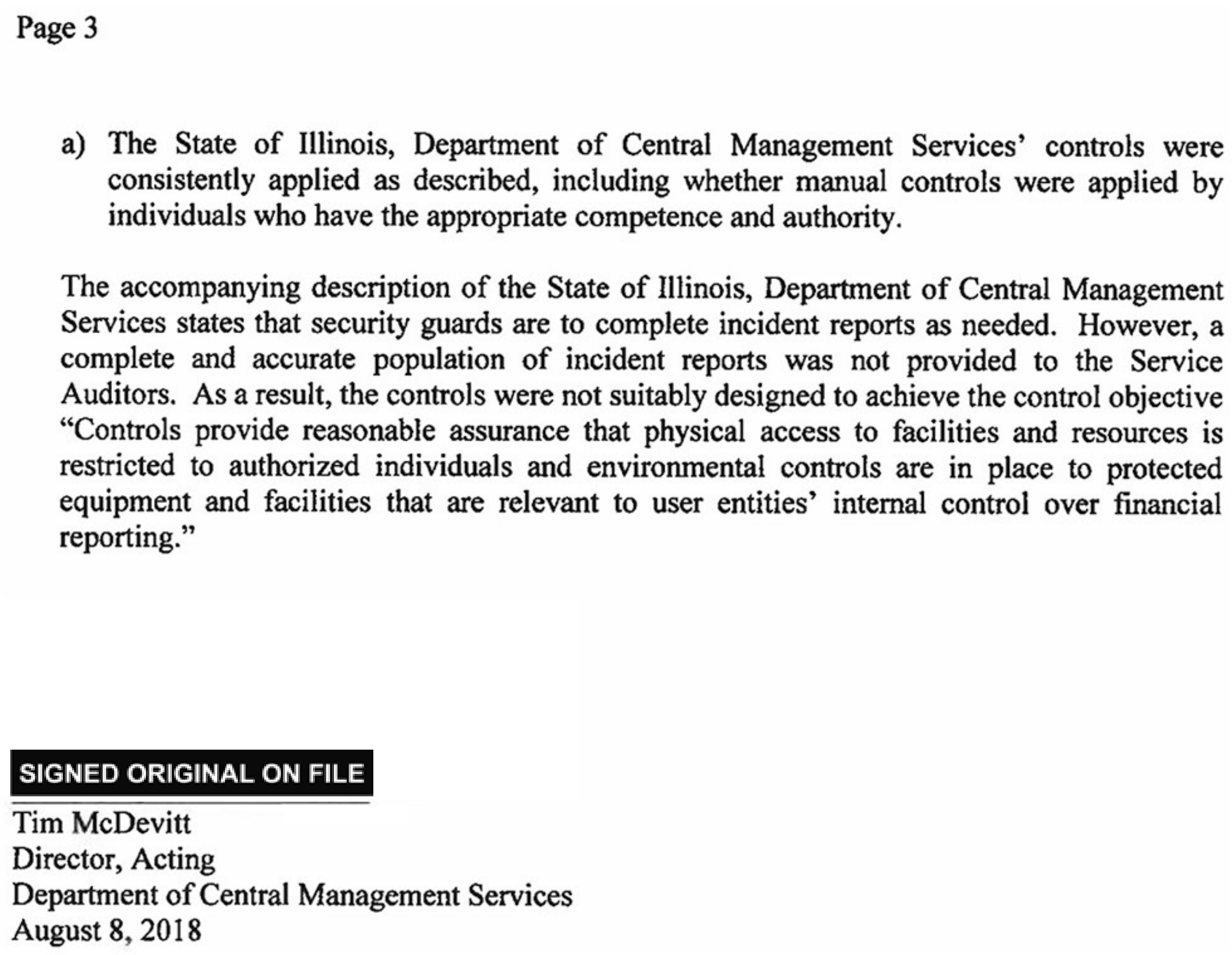
c) Does not omit or distort information relevant to State of Illinois, Department of Central Management Services' services, while acknowledging that the description is prepared to meet the common needs of the user agencies of the system and their user auditors, and may not, therefore, include every aspect of the maintenance and facility support, control and management of physical security, and human resource function services that each individual user agency of the system and its auditor may consider important in its own particular environment.

The description of the State of Illinois, Department Central Management Services' services did not include the process for physical access provisioning for vendor contractors. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

The description of the State of Illinois, Department Central Management Services' services states preventive maintenance agreements for the environmental measures have been entered into. However, maintenance agreements had not been entered into for the water detection system. As a result, the description is not fairly presented.

2) Except for the matter described in the following paragraph, the State of Illinois, Department of Central Management Services' controls related to the control objectives stated in the description were operating as described throughout the period July 1, 2017, to June 30, 2018.

The criteria we used in making this assertion were that:



Page 3

a) The State of Illinois, Department of Central Management Services' controls were consistently applied as described, including whether manual controls were applied by individuals who have the appropriate competence and authority.

The accompanying description of the State of Illinois, Department of Central Management Services states that security guards are to complete incident reports as needed. However, a complete and accurate population of incident reports was not provided to the Service Auditors. As a result, the controls were not suitably designed to achieve the control objective "Controls provide reasonable assurance that physical access to facilities and resources is restricted to authorized individuals and environmental controls are in place to protected equipment and facilities that are relevant to user entities' internal control over financial reporting."

SIGNED ORIGINAL ON FILE

Tim McDevitt
Director, Acting
Department of Central Management Services
August 8, 2018

SECTION III

DESCRIPTION OF THE DEPARTMENT OF INNOVATION & TECHNOLOGY'S INFORMATION TECHNOLOGY SHARED SERVICES SYSTEM

Description of the IT General Controls and Application Controls for the Department of Innovation & Technology's Information Technology Shared Services System

Overview of the Department of Innovation & Technology

According to Executive Order 2016-001, the Department of Innovation & Technology (Department) is to deliver "innovation and technology to client agencies to foster collaboration among client agencies, to empower client agencies to provide better services to residents of Illinois, and to maximize the value of taxpayer resources." The Department is responsible for the information technology and specific applications to State agencies.

Subservice Organizations

The Department utilizes the following subservice providers:

- The Department of Central Management Services to provide maintenance and facility support, control and management of physical security, and human resource functions.
- Zayo Group, LLC to provide an alternate data center for off-site storage and replication of the production environment.
- Virtustream, Inc. to provide cloud hosting services for the State's Enterprise Resource Planning system.
- Microsoft, LLC to provide cloud hosting services.
- BMC Software, Inc. provides Software as a Service (SaaS) by hosting Remedy on Demand.

Overview of Services Provided

The Department is responsible for:

- Managing and planning, procurement, maintenance and delivery of voice, data, wireless, video, internet and telecommunication services to all State-government agencies, boards, commissions and State-supported institutions of higher education in Illinois, as well as other governmental and some nongovernmental entities.
- Operating the central computer facility, as well as other facilities that provide complete IT environment systems and support for most State agencies, boards and commissions.
- Maintaining applications and the related infrastructure that State agencies, boards and commissions may utilize to meet their financial requirements.

Scope of the Description

In accordance with the criteria in management's assertion, this Description includes a description of the Department's Information Technology (IT) General Controls and Application Controls provided to agencies and the Department of Central Management Services' maintenance and facility support, control and management of physical security, and human resource functions utilized by the Department. The Description excludes the control objectives and related controls of Zayo Group, LLC, BMC Software, Inc, Microsoft, LLC and Virtustream, Inc.

The Description is intended to provide information for the agencies and their independent auditors to obtain an understanding of the system and controls in place of the Department's IT General Controls and Application Controls that are likely to be relevant to an agency's internal control over financial reporting.

The Description of the System includes information technology general controls and specific application controls:

- Accounting Information System;
- Central Inventory System;
- Central Payroll System;
- Central Time & Attendance System;
- eTime; and
- Enterprise Resource Planning System.

Internal Control Framework

This section provides information about the five interrelated components of internal control at the Department, including the Department's:

- Control environment;
- Risk Assessment;
- Information and Communication;
- Control Activities; and
- Monitoring.

Control Environment

Elements that support the Department's control environment include management's commitment to cybersecurity; management's philosophy of an engaged, informed, and ethical workforce; an organizational hierarchy with clearly assigned roles and responsibilities; and human resource policies and procedures that promote qualified workforce participants.

The Department's organizational hierarchy supports internal control starting with the Department's Secretary. The Secretary is a member of the Governor's Cabinet and is the "the chief information officer for the State and the steward of State data, with respect to those agencies under the jurisdiction of the Governor", per Section II of Executive Order 2016-01.

The Secretary is responsible for carrying out the objectives of the Department as defined within the Executive Order which includes to "develop and implement data security and interoperability policies and procedures that ensure the security and interoperability of State data … [and] ensure compliance with applicable federal and State laws pertaining to information technology, data, and records of DoIT and the client agencies …".

The Department's organizational hierarchy promotes separation of duties, monitoring of controls, and customer support through staff positions of: Affirmative Action/Equal Employment Opportunity Officer, Chief Administrative Officer, Chief Internal Auditor, Chief Information Security Officer, Chief Service Officer, Chief of Staff, Chief Strategy Officer, Chief

Technology Officer, ERP Program Director, and seven Cluster Chief Information Officers (CIO).

The Affirmative Action/Equal Employment Opportunity Officer serves as an advisor and consultant to the Department on issues, policies, guidelines, and standards related to affirmative action and equal employment opportunity activities. The position also participates in recruitment, investigates discrimination, and serves as the Department's coordinator for the Americans with Disabilities Act.

The Chief Administrative Officer consults with the Secretary and senior management to facilitate functional compatibility and alignment of Department objectives. Subordinate managers oversee the Department's legal, procurement, and human resource services.

The Chief Internal Auditor directs and manages the Department's internal audit program which validates compliance to the Fiscal Control and Internal Audit Act and verifies consistency with the Department's mission, program objectives, and regulatory statutes. In addition, internal audit operations identify and evaluate significant risk exposures and contribute to the improvement of the Department's overall control environment.

The Chief Information Security Officer (CISO) is responsible for strategies, policies, standards, processes, and assessments that promote protection over the Department's assets and reduce cyber risks. This includes development of a cybersecurity program that provides risk identification, mitigation, analysis, and resolution advice to the Department and to agencies. The CISO manages protective services such as encryption, recovery, and monitoring controls such as incident detection and response. The CISO is also the sponsor of the Department's workgroup that meets weekly to develop and recommend enterprise policies for further review and signature by the Chief Legal Counsel and the Secretary.

The Chief Service Officer plans, coordinates, reviews, and directs long and short term strategic goals, policies, and procedures based on the Department's mission and initiatives with the ultimate goal of understanding, satisfying, and exceeding, if possible, customer expectations. This position is responsible for the delivery of customer-facing IT services, end user support, and change control.

The Chief of Staff advises the Secretary on the transformation status of legacy agency resources (personnel and equipment) to meet the requirements of Executive Order 2016-01 which created the Department and provides the authority for transferring State resources into the Department. The Chief of Staff also supervises functional areas of the Department's fiscal officer, budget director, legislative liaison, and communications/public information manager. In addition to supervisory and managerial roles, the Chief of Staff is the primary champion for the "DoIT Daily" conferences lending top level support and decision-making resolutions to deliver quality service to agencies.

The Chief Strategy Officer directs implementation of strategies, plans, procedures, and guidelines reflecting organizational requirements and the Department's mission. The Chief Strategy Officer also oversees the Department's Enterprise Program Management Office and IT

Governance program. Both of these units address change control methodologies as it relates to financial application functional requirements.

The Chief Technology Officer is responsible for building the Department's strategy for future technology innovations as well as for managing business functions covering data, infrastructure, applications, network, and software distribution. Each of these business functions have been assigned separate managers. Enterprise Infrastructure includes data center and midrange server operations, enterprise production operations, and personal information management.

The Enterprise Resource Planning (ERP) Program Director is responsible for directing, planning, developing, administrating, and implementing the Statewide ERP program. For participating agencies, the ERP provides consolidated management over financial services.

The seven Cluster CIOs promote quality of service and enhance the effectiveness of the Department's internal control environment through information exchange, general oversight of agency information processing, and strategic planning participation. The Cluster CIOs enhance agency awareness of Department policies, procedures, objectives, and new initiatives as well as providing a channel to communicate agency concerns and recommendations. These responsibilities have been categorized into seven (7) groups reflecting Statewide agency services. Categories are (1) family, children, elderly, and veterans; (2) government and public employees; (3) business and workforce; (4) natural and cultural resources; (5) public safety; (6) students; and (7) transportation.

Human Resources

The Department's hiring practices adhere to legal requirements as published in the State Personnel Code, Personnel Rules, union contracts, Rutan decisions, court orders and applicable state/federal laws. Workforce members are categorized into employees (collective bargaining and non-union) and contractual (personal services contracts).

For each employee position, a formal, written, published job description is maintained which documents the duties and qualifications consistent with established class specifications for the position title. Minimum acceptable competency education requirements and experience levels are identified in each job description to ensure a quality and qualified workforce. Newly-developed as well as clarified job descriptions require final approval from the Department of Central Management Services' Division of Technical Services within the Bureau of Personnel.

Effective August 15, 2017, the Department took responsibility for the posting of vacant positions. Prior to August 15, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department.

Upon verification between the Department's Human Resources and the appropriate supervisor/manager of the accuracy of the job description, the Department's Human Resources prepares a Personnel Action Request (PAR) form; the Department's Chief Fiscal Officer and the Secretary (or designee) are required to approve the PAR form prior to posting of the position.

Effective September 18, 2017, the Department took responsibility for the creation of bid records. Prior to September 18, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department.

The Department's Human Resources identifies individuals who have bid on the position and have been deemed qualified and eligible through the Department of Central Management Services' examining process and forwards the information to the interview panel to commence the interview and selection process. Required forms and interview procedures differ depending on whether or not the position is covered by collective bargaining. For collective bargaining positions, Human Resources compiles a bid record that meets the "Filling of Vacancies" language outlined in the position's collective bargaining agreement that dictates who has rights to the position. Bid record information is forwarded to the interview panel and interviews are conducted that follow the Rutan guidelines as appropriate for the position. For other Personnel Code-covered non-bargaining unit positions or bargaining unit positions that have no contractual bidders with rights, the selection of a qualified candidate is made by the work area management after the Rutan interview and the completion of the Employment Decision Form.

For a Personal Service Contractual (PSC/contractor) position, the description of services (i.e. required duties and qualifications) is prepared by the supervisor and approved by Human Resources; upon approval of the PSC description of services, Human Resources prepares a PAR form used to post the employment opportunity. Human Resources forwards candidate information to the hiring unit to schedule interviews. Based on answers to questions, the most qualified candidate is selected, documented on a PSC Decision Form, and continues through the hiring process which includes the Department's legal staff writing a contract outlining the terms and conditions of the services to be provided.

Effective October 13, 2017, the Department took responsibility for the submission of background checks. Prior to October 13, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department.

Any new employee or contractor must pass a background check before being offered employment. Demographic information is submitted to and results are received from the Illinois State Police's Criminal History Information Response Process system. Once cleared, the hiring process continues with offering employment to the prospective candidate. However, if an offense is revealed, the Department considers the date, nature and level of the offense to determine if there is a relationship to the duties of the vacancy for which the candidate has been selected. Dependent upon the outcome of that review, the candidate is either offered the vacancy or bypassed.

Effective October 16, 2017, the Department took responsibility for conducting new employee orientation. Prior to October 16, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department.

As the need arises, Human Resources provide New Employee Orientation on the first work day of each pay period for employees and on the contract start dates for contractors. During orientation, newly-hired employees and contractors are provided the Department of Central

Management Services' (DCMS) Policy Manual and are required to sign a Policy Manual Acknowledgement form which documents receipt of the Policy Manual and acknowledges responsibility to abide by the policies contained therein. Department employees are emailed the Security Awareness Training and Ethics Orientation for State Employees. Contractors are provided hard copies of Security Awareness Training and Ethics Orientation for State Employees on their start date. All new hires (employees and contractors) are required to sign the acknowledgement included in the Security Awareness Training and Ethics Orientation and return to Human Resources. The signed acknowledgement form documents that the employee or contractor has reviewed the material and recognizes the responsibility to abide by Security Awareness Training and Ethics Orientation for State Employees. Employees and contractors are notified via email of any changes to the DCMS Policy Manual and are required to sign and return acknowledgement of receipt of any changes to the policies contained therein.

Effective November 16, 2017, the Department took responsibility for processing personnel transactions. Prior to November 16, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department.

For an employee leaving the Department (transferring, resigning, or retiring), once Human Resources receives signed confirmation from the employee, Human Resources initiates a PAR Form, obtains appropriate Department authorizations from the Chief Fiscal Officer and the Secretary (or designee), and begins the separation process. For a contractor, the separation process begins upon expiration or termination of the contract. At separation of either employee or PSC contractor, Human Resources initiates an Employee Exit Form for completion by the supervisor. Once the Form is reviewed by the appropriate supervisor (either of the employee or contractor), it is forwarded to the Department's IT Coordinator group which then creates a Remedy Enterprise Service Request (ESR) based on its content. The Remedy ESR is then submitted to the Department's IT Service Desk for the removal of access and retrieval of equipment.

Effective November 16, 2017, the Department took responsibility for employee evaluations reporting. Prior to November 16, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department.

Employees serving an original six-month probationary period are expected to be evaluated twice - one performance appraisal at the end of three months and another two weeks prior to the end of the probationary period (end of six months). Employees serving a four-month probationary period are expected to have an evaluation completed two weeks prior to the end of the probationary period (end of four months).

Each month, Human Resources prepares a report of annual employee performance evaluations that are due in the current month, in the upcoming next two months, and any that are overdue. Human Resources distribute the report to respective managers with instructions to return completed evaluations to Human Resources for processing. As Human Resources receives completed performance evaluations from the managers, they are marked off the list; the Secretary's signature is affixed, with final copies of the evaluations bearing the Secretary's signature being provided to the employee and supervisor. The evaluations are maintained in the employees' file. When the next month's report is prepared, Human Resources reviews it to verify all evaluations previously submitted have been removed from the list and follows up on any discrepancies.

Requirement for a contractual performance appraisal is dependent upon contract language. Performance appraisals may or may not be detailed within a personal services contract. The characteristic that ensures quality work is that contractual workers are 'at will' and may be terminated at the discretion of the Department for poor performance.

On February 26, 2018, the Department took full control/responsibility related to the Department's personnel functions.

For employee training and continuing education, managers contact the Human Resources' Training Manager to assist with identifying available classes to meet the training needs of the employee, register the employee for approved training when appropriate, and track the employee's training history via completion of a Training Request Form.

Annual ethics training for Department employees is a requirement of the State Officials and Employees Ethics Act (5 ILCS 430). A certificate is issued upon successful completion of the online course.

In addition to ethics training, Public Act 100-0040, effective January 1, 2018 tasks the Department to provide mandatory, annual cybersecurity training to all State employees and contractors by amending the State's Data Security on State Computers Act. Compliance is tracked via the Learning Management System.

Prior to January 2018, annual security awareness training was provided to all employees and contractors. The training was tracked by the Division of Information Security.

As part of the annual security awareness training and the ethics training, employees and contractors acknowledge their compliance with security policies.

Risk Assessment Process

The Department's commitment to security, risk reduction and mitigation, and quality of service is stated as part of the vision statement published in the 2017-2019 State of Illinois Cybersecurity Strategy.

The Department's Risk Management Program states that risks be categorized into criticality levels of high, medium, and low based on data classification, impact level (severity), likelihood (probability), and strength of existing controls. The Risk Management Program also classifies data as Public, Official Use Only, or Confidential. Risk categorization assists in the degree of effort and cost applied to mitigation efforts that reduce Department risk.

During March and April 2018, the Department conducted an organizational risk assessment based on federal NIST standards. The assessment collected data via a series of questions based on the NIST Risk Management Framework Methodology. The data was utilized to calculate a risk maturity score based on the assessed strength and effectiveness of existing controls.

The Department receives threat, vulnerability, and incident intelligence from multiple sources, including the FBI, MS-ISAC, the Illinois Statewide Terrorism Information Center, and Twitter feeds. Risks from potential and newly discovered vulnerabilities are assessed through interaction with security experts and vendor subscription services. The Department also contracts with vendors to receive patch vulnerability information at the earliest possible time. A vulnerability scanning protocol is employed to assess identified servers monthly. The Department shares information obtained from the vulnerability scanning process with senior management to help eliminate vulnerabilities on information systems.

The Department has partnered with the Department of Homeland Security's National Cybersecurity Assessments and Technical Services to conduct a proactive phishing campaign assessment. This exercise assessed the risk and the susceptibility of Department and agency email phishing attacks.

Information and Communication

Maintaining communication with Department staff and agencies is a key element to effective operations. Agencies and employees may request and receive information via the Department's website www2.illinois.gov/sites/doit/. The website also provides a method to report problems.

In addition, the "News" section informs agencies on major initiatives and accomplishments of the Department. Links on the website provide operational details to the Department's Service Catalog and guidelines for ordering services. The Department's Service Catalog was updated March 7, 2018 to include additional services and updates to rates, including the ERP.

The weekly DoIT Digest digital newsletter is archived on the website to enhance transparency. Agencies also are notified via email on a variety of communication topics.

Agency communication is also accomplished through the website, Cluster CIOs, group meetings, and Department policies. Cluster CIOs provide an exchange of information between the Department and agencies and keeps both the Department and agencies informed regarding significant events, service issues, improvements, processes, and strategic goals. Cluster CIOs meet with agency CIOs when business need requires or when instructed by Department management. Group meetings are held to update and gather information from agencies.

The Department coordinates an annual Strategy Summit where all State agencies, as well as other taxing authorities are invited to attend a conference covering topics of interest to Illinois governmental entities. Additionally, CIO Council meetings are held at the Secretary's request to update and inform agency CIOs of news and information. Information and presentation slides from these ad hoc meetings are available to the Cluster CIOs and agency CIO's.

Policies, along with application user manuals, communicate the process to report system problems and security issues.

Department workforce communication is provided through the website, the employee portal/intranet, DoIT Digest, Town Hall meetings, and emails. The intranet contains content that defines the role employees play in meeting the Department's mission. The intranet provides information covering topics such as pensions and retirement, insurance, training opportunities, payroll information, as well as a link to the DCMS' Policy Manual, which details the rules of conduct, attendance, employee evaluations, and related employee responsibilities. DoIT Digest email publications and Town Hall meetings keep Department workforce members informed on topics such as Department strategic priorities, personnel updates, and new Department initiatives. Technical, security, and emergency notifications are sent directly via email alerting the workforce to conditions including outages, phishing attempts, and scheduled upgrades.

The Department policies available on the Department's website include, but are not limited to:

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.

ERP Communication

The Department communicates ERP information to the agencies through its Production Support team. Production Support initiates all communications, including incidents, from the stilerpsupport@deloitte.com email address. Production Support also communicates with agencies via phone, or in person, depending on the nature of the incident and the level of coordination and communication needed.

Release Management, including descriptions of any releases is sent to the agencies from the stilerpsupport@deloitte.com email address.

Agencies are encouraged to contact the ERP Team:

- IT Service Desk via Remedy ticket for all problems experienced with the ERP.
- Individual ERP team members via email or phone for any business process questions.
- Statewide.ERP@illinois.gov for any general questions about the ERP Program.

In addition, policies and procedures are maintained on SharePoint.

Monitoring

The Department's philosophy of an engaged and informed workforce is reflected through the "DoIT Daily" conference attended by senior leadership, operational management, Cluster CIO's, and agency CIOs. Attendees participate in an hour-long meeting scheduled each Monday through Thursday for the purpose of improving communication, increasing the successful resolution of issues impacting customer service and internal operations, providing transparency to Department staff as well as to agencies, and demonstrating continued commitment to maintaining a quality control environment. The "DoIT Daily" also supports monitoring and assessment of Department activities by sharing of operational issues and receiving recommendations from a cross-section of Department functional managers.

Monitoring of Subservice Providers

Monitoring of the Department of Central Management Services activities in regards to Physical security is conducted informally via email and phone.

The Department's Compliance Officer receives and reviews the type 2 SOC 1 report of Zayo Group, LLC, subservice organization, on an annual basis. In addition, Zayo Group, LLC's performance is monitored at various event occurrences such as vendor account manager change, contract renewal, billing reconciliation, etc.

Annually, the Department's ERP Team receives and reviews the type 2 SOC 1 report from Virtustream, Inc. These reports are reviewed and the review process is managed within the ERP SharePoint site.

In addition, the Department conducts weekly meetings with Virtustream to ensure compliance with contractual requirements. Project status documents and any notes are discussed and saved within the ERP SharePoint site.

Environment

Midrange

The Department's midrange configuration consists of several multi-core processors. The midrange systems are configured into logical partitions or virtual servers consisting of production, test, and continuous service. The midrange primary operating systems software includes:

- Microsoft Windows Servers operating system (OS) is a series of enterprise-class servers

operating systems designed to share services with multiple users and provide extensive administrative control of data storage, applications and corporate networks.
- VMWare ESXi is an enterprise class type-1 bare-metal Hyperivsor. It installs onto a physical server with direct access to and control of underlying resources. ESXi can effectively partition hardware to increase virtual servers' ratios.
- Advanced Interactive eXecutive (AIX) is an enterprise-class UNIX operating system (OS) for the POWER processor architecture found in the IBM Power Systems.
- LINUX is a family of free and open-source software operating systems built around the Linux kernel, typically packaged in a form known as a Linux distribution (distro) for both desktop and server use.

Mainframe

The Department's mainframe configuration consists of several CMOS processors. The mainframe is partitioned into logical partitions consisting of production, test, and continuous service. Several partitions are configured in a SYSPLEX (coupling facility). The mainframe primary operating system software includes:
- 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.
- z/Virtual Machine (z/VM) is a time-sharing, interactive, multi-programming operating system.

The primary subsystems include:
- 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.
- 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".

Information Systems Overview-Applications

The Department provides several applications in which agencies may utilize. The agencies are responsible for the entry and maintenance of the data, while the Department is responsible for the maintenance of the applications.
- Accounting Information System (AIS);
- Central Inventory System (CIS);
- Central Payroll System (CPS);
- Central Time and Attendance (CTAS);
- eTime; and
- ERP.

AIS, CIS, CPS, and CTAS resides on the Department's mainframe environment, while eTime resides on the Department's midrange environment. The Department has contracted with Virtustream, Inc to host the ERP.

AIS

AIS is a mainframe application which addresses accounts payable, manages appropriations, fund transfers and adjustments, vendors, contracts and contract amendments; tracks expenditures from the initial receipt of the invoice throughout the production of vouchers; and provides both project and cost center accounting. Transactions allocate financial information into sub accounts according to the Office of the Comptroller's Statewide Accounting Management System (SAMS) procedures, which allows agencies to track cost centers.

AIS supports segregation of responsibilities and functions by limiting the ability of data manipulation to accounting and bureau administration. The bureau level allows for the initial entry and maintenance functions, where the accounting level is the audit function and final approval process.

Upon passage of a State budget, agencies are to enter their applicable appropriations. After entry of the appropriations, agencies are required to enter their obligation data (contracts) against the applicable expenditure account. A contract must be entered before the corresponding obligation is recognized.

Upon receipt of a vendor's invoice, the agencies enter the invoice information. The agencies must indicate the fund, account, and line item in which the invoice is being charged to in order to ensure sufficient appropriations are available.

Upon proper approval within AIS, the agencies print the AIS 13 for review. Upon approval, the voucher is printed for the agencies' head approval and submission to the Office of the Comptroller.

Additionally, upon approval, the voucher is released, and the Agency Tape Balancing Report is printed, signed by the applicable agency head, and submitted to the Office of the Comptroller for processing.

AIS allows agencies to issue refunds/credits and to make adjustments to invoices. The type is dependent on the circumstance. The refund/credit allows funds to be added back to the voucher and the appropriation/obligation line.

AIS has edit features designed to reject erroneous or invalid data entered. When erroneous or invalid data is entered, an error message will appear at the top of the screen and the field that is in error will be highlighted. AIS will not accept the entry until the error has been corrected or deleted. In addition, AIS will not allow a transaction to be processed without sufficient funds. AIS assigns a unique identification number to each inputted transaction. Additionally, the Department has developed the AIS User Manual to assist agencies.

AIS provides various reports to assist agencies in process and reconciling their transactions.

AIS interfaces and interacts with other applications by either forwarding specific data or by sharing access to the AIS database.

- ALS - Auto Liability System;
- ARPS - Accounts Receivable Posting System;
- CPS - Central Payroll System;
- CRIS - Comprehensive Rate Information System;
- FLEET - Vehicle System;
- IGPS - Inter-Governmental Procurement System; and
- Office of the Comptroller.

CIS

CIS is a mainframe application which manages inventory, and creates, updates, and tracks property records for equipment, furniture, real property, and vehicles.

Upon receipt of an asset, agencies are to enter the asset's information into CIS; tag, location, description, voucher information, etc. Additionally, in the event information regarding the asset needs to be revised, i.e. asset location change, the agencies are to make the applicable corrections.

In the event, an asset requires deleting, the agency is to contact the Department of Central Management Services' Property Control Division in order to obtain approval, prior to deletion.

Additionally, CIS allows an agency the ability to depreciate an asset, via straight-line depreciation. Depreciation is calculated and updated on a monthly basis.

To help ensure the accuracy of the data, CIS is equipped with online edit checks and range checks which provide the agency with immediate notification if errors are encountered during data entry and processing edit checks which report processing errors online. Additionally, CIS will not allow duplicative tag numbers.

The Department has developed the CIS User Manual to assist agencies. CIS can produce various reports to assist agencies in processing their inventory; locations, reconciliations, tag by location, vehicle and transaction summaries, etc.

CIS interfaces with three external systems to provide asset update files that are processed nightly:

- EMS - Telecommunication Asset Tracking;
- FLEET – Vehicle System; and
- Remedy - EDP Asset Tracking.

CPS

CPS is a mainframe application that enables agencies to process and manage payroll information for their employees. CPS generates payrolls for agencies providing for appropriation coding, base pay and overtime computation, updating of relevant tax tables, processing of supplemental and anticipated payrolls, net pay determination, and direct deposit. CPS also provides for warrant reversals to correct warrants issued in error.

CPS has a ten day working pay schedule, which allows agencies to enter their payroll in order for the payroll vouchers to be processed timely. Every pay period is assigned a close date, which is the date that all payroll data entry must be completed. On the night of the close, CPS freezes the data for that pay period and runs the Gross-to-Net process. The Gross-to-Net processes uses the data for the pay period, along with tax tables and withholding information to calculate and generate vouchers for all employees that are to be paid. Error reports are generated if the Gross-to-Net process fails or problems are identified.

As part of the Gross-to-Net process, the payroll vouchers are produces as series of reports for each agency. Each agency is to print the payroll voucher, approve, and submit to the Office of the Comptroller for warrant generation. In addition, CPS sends an electronic file of the vouchers to the Office of the Comptroller.

In the event the payroll is rejected by the Office of the Comptroller, or the Gross-to-Net process, or if the agency identifies problems when they review the voucher reports, the data must be corrected and re-generated. In order to correct the data, the agency is to submit a Remedy Help Desk ticket to the Enterprise Application & Architecture (EAA) Personnel Payroll support group, specifying the needed changes. The EAA Personnel Payroll staff will run special ad-hoc programs to correct the specific problem and will then re-run the Gross-to-Net process.

Annually, the Department reviews and updates the applicable federal and states' tax rates.

CPS has edit features designed to reject erroneous or invalid information entered. When erroneous or invalid data is entered, an error message will appear at the top of the screen and the field that is in error will be highlighted. CPS will not accept the entry until the error has been corrected or deleted. In addition, CPS assigns a unique identification number to each inputted transaction.

The Department has provided agencies with the CPS User Manual to assist in the preparation of payroll records. As outlined in the CPS User Manual, CPS can produce various reports to assist in the reconciliation and integrity of payroll.

CPS interfaces and interacts with other applications by either forwarding specific data or by sharing access to the CPS database:

- AIS,
- ERP, and
- Office of the Comptroller.

CTAS

CTAS is a mainframe application that provides a system for recording and managing employee time. CTAS calculates and reports overtime, compensatory time, accumulated leave and benefits based on continuous service dates, accumulated leave and compensatory time, and monitors maximum vacation carryover. CTAS provides for attendance information to be recorded using either the positive or exception method. The positive method of recording daily attendance requires the timekeeper to enter or confirm an employee's general attendance information. The exception method assumes that an employee's scheduled work time is the correct attendance unless the timekeeper enters something different. CTAS also maintains historical records of employee time data and can generate audit trails pertaining to adjustments when requested.

The agency Timekeeper is responsible for entry and maintenance of the agencies employee's time and attendance; vacation, sick, personal, etc.

In order to reconcile all the time entered for a time period, CTAS performs a "close" process. The "close" process checks for consistency and completeness and performs necessary calculations for overtime and compensatory time. Additionally, the "close" process utilizes the work schedule to create the attendance entries for "exception-entry" employees who did not have their attendance entered for a particular day.

Upon completion of the "close" process, an employee's record cannot be altered. Therefore, agencies are to complete a "pre-close" process and review all information to ensure its accuracy.

Once the "close" process has been run, CTAS generates an error report, a reconciliation report, and a file maintenance activity report. All discrepancies noted need to be reconciled before a "close" can be finalized.

Upon entry of information, CTAS runs various edits to ensure the completeness and accuracy of the data. When erroneous or invalid data is entered, an error message will appear at the top of the screen and the field that is in error will be highlighted. CTAS will not allow transactions to be processed until all errors are rectified. CTAS assigns a unique identification number to each inputted transaction. The Department has also developed the CTAS User Manual to assist agencies.

In addition, CTAS produces other reports that assist in data integrity and processing including lists of pending pre-close transactions (which identifies potential warnings and errors that may occur during the close process), supplemental requests (lists information other than found in the close process report such as work schedules, job positions, vacation time, overtime, sick time, GAAP report, etc.), and listing of employee historical information. Per an agency request, ad hoc, non-standard reports may be generated based on extracts from the CTAS database.

CTAS interfaces and interacts with e-Time; sharing a back-end database where e-Time is the front-end GUI interface.

<u>eTime</u>

eTime is a web-based application which allows agencies the ability to manage work time and attendance. eTime provides for the ability for employees to electronically report hours worked and to submit leave, overtime pre-approvals, and overtime requests.

The process begins by the employee entering exceptions to standard, scheduled work hours which have been established in CTAS. This is accomplished by requesting overtime pre-approvals and leave requests, submitting overtime worked hours, or canceling or modifying previously entered information. Conditions requiring approvals are automatically routed to the appropriate supervisor or designee. Approved leave and overtime requests are processed nightly via the CTAS batch process. For contractual workers, the process begins by entering actual hours worked. Once completed for a pay period, eTime routes hours entered to the appropriate supervisor or designee for approval. For a given pay period, the timekeeper searches eTime to retrieve approved contractual hour amounts and then manually posts them into CTAS.

Error messages are displayed on the screen as inconsistencies are encountered. Sample message topics include exceeding comp time; duplicate record or request, no preapproval, overtime exceeds pre-approved hours, and others. Supervisor roles are prohibited from correcting errors or changing employee entered information. Quick reference guides and context sensitive error messages are available to assist users when using the application.

eTime is the front-end, GUI interface to CTAS users who use the exception method of attendance reporting.

ERP

The Department implemented SAP's Enterprise Resource Planning (ERP) system on October 1, 2016. The ERP integrates the finance, human resource, procurement, and other financial related areas into a single system. The ERP Central Component (ECC) is comprised of the following modules:

- Financial Accounting
    - General Ledger
    - Accounts Payable
    - Asset Accounting/Management
- Material Management
- Public Sector Collections & Disbursements
- Funds Management
- Grants Management

In addition, the Department has implemented SAP's Supplier Relationship Management which facilitates the procurement of goods.

General Ledger

The General Ledger records the financial transactions of the agencies. The General Ledger and chart of accounts master data elements govern the manner in which budgets, revenues/receipts, transfers, bonds, federal funds, or expenditures of the agency are recorded. The maintenance of the General Ledger chart of accounts is maintained by the General Ledger Functional Expert.

The Department has implemented three ledgers in order to account for the multiple bases of accounting utilized by agencies; full accrual, modified accrual and cash basis. The ERP is configured to automatically post to all three ledgers, unless the agency specifically indicates otherwise.

Each "transaction" is posted to the General Ledger with the associated history and documentation. Each transaction is created when a document is created and assigned a document number. In addition, Journal Entries (JE) can be made to record adjustments and month/year end adjustments.

When making an entry, the entry must balance; debits must equal credits. The system will not allow a user to process a transaction or a JE without it balancing. Prior to being posted, JEs are required to be reviewed and approved.

Period End Closing

The fiscal year variant is the periods utilized in posting transactions. The Department is utilizing 12 regular months (July through June) with the 13th month being utilized for lapse period transactions.

In order to close a period, each agency must have completed recording all transactions. In addition, the agency is required to complete the various reconciliations; IOC, general ledger, etc. and ensure all transactions are accurately reflected in the General Ledger. The close process cannot be conducted until all agencies have completed all monthly, quarterly or year-end activities/reconciliations.

On the last day of the month, the General Ledger Functional Expert will open the next accounting period (next month) in order for agencies to post to the next month. In addition, the General Ledger Functional Expert will close the prior period. Closing of a period is to be conducted:

- Monthly-last day of the month,
- Quarterly-March, September, and December,
- Year end-June, and
- Lapse-after lapse activities are completed.

The quarterly and year-end closing also include tasks for required reporting requirements; C-15, C-97, etc.

Fiscal year 2017 lapse period (period 13) and all periods for fiscal year 18 remain open.

In the event an agency needs to make a correction or post to a closed period, the agency will need to submit an incident ticket to the ERP Production Support. The General Ledger Functional Expert will work with the agency to make the needed corrections.

As part of the closing activities at fiscal year-end, specific account balances are carried forward; assets and liabilities. In addition, all vendor balances will be carried forward to the next fiscal year.

Accounts Payable

Accounts Payable records and manages accounting data for all vendors. Upon receipt of a vendor invoice, the Accounts Payable Processer enters the basic invoice data. Upon entry, there are specific data fields that are automatically populated, along with specific data fields that are required to be manually entered. Upon completion of entry, all hardcopy documentation is attached to the invoice record.

Once entered, the Accounts Payable Processer is to save the document and the Oversight Approver is notified of the invoice waiting approval. The Oversight Approver is to review and approve the invoice.   At that time the invoice is posted to the General Ledger. In the event the Oversight Approver rejects the invoice, it is returned to the Accounts Payable Processer.   Within the invoice, the Oversight Approver is to document what the issues are.

A nightly batch is ran which generates the Balance Report documenting all approved invoices. The Balance Report is emailed to the Oversight Approver for review and approval to release to the Office of the Comptroller.   After the Oversight Approver approves, the file and voucher are released. If needed, the Accounts Payable Processer has the ability to manually generate the Balance Report.

In addition, there is a nightly batch that is run which brings in voucher payment details from the Statewide Accounting Management System (SAMS).

Asset Accounting

Asset Accounting allows agencies to maintain, transact and report on their fixed assets. Transaction codes allow agencies to process asset transactions; additions, transfers and retirements.

During asset acquisition, the asset shell records the detailed information; description, acquisition date, value, fund information, depreciation details, and location. In order for the location to be entered into the asset shell, the agency must have entered the location information (addresses) associated with their agency.

An asset acquisition is entered into the asset shell record in order to be added to the Supplier Relationship Management Module (SRM). Once the asset has been "receipted" from the Purchase Order, the capitalization date and value are added to the asset shell. At this time the asset number (tag number) is created; assigned by the agency.

In the event an asset is acquired through a transfer, donation, etc., the asset shell is completed; however, the asset shell is not added to the SRM; as a Purchase Order is not required.

During the construction of an asset, the costs are posted to an Asset under Construction account. Upon completion, the accumulated cost in the Asset under Construction account is transferred to the Asset account and capitalized as appropriate.

The capitalization threshold is determined based on the asset type; land, equipment, etc. Depreciation is calculated utilizing the straight-line method over the estimated useful life of the asset.

On the first day of each month, batch job is run which calculates the monthly depreciation for that month. In addition, a second batch job is run for the monthly depreciation on new, disposedof and transferred assets. At the completion of each batch job, the calculated depreciation is recorded against the asset and the general ledger depreciation account.

In the event a correction needs to occur after a period has been closed, the agency must contact the Assets Functional Expert in order to make the needed correction.

Inventory reports are available to be downloaded and used alongside bar-code scanners in order to conduct inventory activities. Upon completion, results from scanning are uploaded. At that time, the information is reviewed and a discrepancy report is available documenting asset information that differs between the asset record and the information uploaded. Agencies are responsible for reviewing and rectifying the errors noted on the discrepancy report.

There are several inventory reports available to the agencies; asset location, asset depreciation, asset transactions, etc. In addition, the Agency Report of State Property (C-15) which is to be submitted to the Office of the Comptroller is available.

Material Management

Material Management records transactions related to purchase and utilization of goods/services and materials. In order to obtain goods/services a Purchase Requisition (Shopping Cart) is to be created, documenting the details of the goods/services to be purchased. Upon approval of the Shopping Cart, a Purchase Order is created and a check for funds availability is conducted. If funds are available a commitment (encumbrance) is posted to the applicable Funds Center.

The value of the Shopping Cart directs the required approvals; supervisor, manager, and fiscal.

Upon receipt of the goods/services, the receipt of goods/services is completed; thus allowing the posting of invoices. An invoice cannot be posted to the Purchase Order until a receipt of goods/services is completed.

If requesting inventory from stock, a Purchase Requisition (Shopping Cart) is created and approved. At that time a check is made to determine if stock is available. If there is available stock, a reservation is created and subsequently delivered. In the event stock is not available, a Purchase Order is created.

Public Sector Collection & Disbursements (PSC&D)

PSC&D provides for the activities associated with billings, payments, and Accounts Receivable (AR). The posting of AR is through a document against the Customer’s Contract Object. The Customer’s Master Data is comprised of a three tier hierarchy:

- Business Partner (Customer) – the central level of all data associated with the customer. Customer number is based on SSN, FEIN or a unique agency ID. All agencies have access to this level.
- Contract Account – this level is associated with a specific agency’s activities; posting of agency payment methods, interest calculations, conditions or dunning procedures, billing methods, etc.

- Contract Object – the third level, defines the Customer's account with additional detail, specific licenses, taxes, claims, etc.

When activity is conducted by the Customer or the agency, the activity is posted at the Contract Object level; ie; application for a license (DNR), filing of taxes (IDOR), etc. Additionally, in the event the Customer conducts activity, but does not submit payment immediately, the AR is established at the Contract Object level.

The posting of payments may be completed in one of two ways:

- Cash Desk, or
- Check Lot.

The Cash Desk requires the agency to enter each payment one at a time; whereas Check Lot allows an agency to post multiple payments at a time. When utilizing Check Lot, the total of the individual payment posting must agree with the total of Check Lot.

Once the Treasurer's draft is received, the RDT is created. From July 1, 2017 until December 31, 2017, a RDT was generated for each cash receipt for agency signature and submission to the Comptroller. As of January 1, 2018, a RDT is created which can contain multiple cash receipts. Upon creation, the RDT is signed and sent to the Office of the Comptroller, along with a batch file of the RDTs.

Upon receipt of the payment, the posting is made against the AR at the Customers Contract Object level by the applicable agency. In the event a one-time payment is received, the payment is posted as a miscellaneous receipt and the Business Partner is provided for reference.

Monthly, agencies are to utilize the General Ledger Balance Report in order to balance with the Comptroller's SB04; monthly revenue status report. In addition, the agencies are to create their Quarterly Summary of Accounts Receivable (C-97), Quarterly Summary of Accounts Receivable-Aging of Total Gross Receivables (C-98), and Quarterly Summary of Accounts Receivable-External Collection Activity for Accounts Over 180 Days Past Due (C-99) for submission to the Office of the Comptroller.

Funds Management

Funds Management records, tracks and report on revenues, expenditures, commitments, obligations and transfers. Upon the passage of a budget, approved budget numbers (appropriations) are established at the Fund level by the Office of the Comptroller. Then via an interface, the budget numbers are entered. After entry, agencies may maintain the budget numbers at the upper level (superior Funds Center) or can distribute to lower levels based on the agency's specific needs; specific Funds Center, Commitment Items, Funded Programs.

In the event a new fund needs to be established, a request from the Office of the Comptroller or an agency is received, via a Help Desk Ticket. The Functional Expert with Firefighter ID access completes the creation of the new fund.

Grants Management

Grants Management is utilized to maintain the details (terms and conditions) of the grant awards between the granting (federal, other state agencies, private, etc) and the agency. The Grants Management module maintains the budget, obligations, actual expenditures, revenues, etc associated with each specific grant. The grant budget can be maintained on an accrual basis or cash basis of accounting.

Upon receipt of an award, the agencies are required to enter the grant master data. The grant master data maintains the administrative details (name, billing, funds, term, etc) and the fiscal details (budget, expenditures, indirect cost, revenues, etc). The budgeting function allows the agency to establish appropriations, allowable expenditures, and the period of the grant. The grant expenditure categories (sponsor class), establishes the specific allowable expenditures under the grant.

Prior to the expenditure of any funds, the Grant Budget Workflow requires the grant budget to be approved.

The Grants Management module provides agencies with various reports for required grant reporting.

The ERP has edit features designed to reject erroneous or invalid data entered. When erroneous or invalid data is entered, an error message will appear. The ERP will not accept the entry until the error has been corrected or deleted.

Information Technology General Controls

Change Control

Change Control – Other Than Applications

Control over changes to the network, mainframe, and midrange infrastructures as well as to data storage devices are achieved through the change management processes as documented in the Remedy Change Management Guide and the Change Management Policy. Changes are documented, tracked, and authorized through Remedy. Each change is required to be entered into Remedy as a Request For Change (RFC), categorized, prioritized, and approved as required.

Emergency changes are processed differently than non-emergency changes. In the event of an emergency change, the Support Group Manager (supervisor) is notified to obtain verbal approval before the change is implemented. Previous week's emergency changes are reviewed at the weekly Change Advisory Committee meeting.

Emergency changes and scheduled changes that cause a major outage, requires a Post Implementation Review (PIR) to be conducted. The Enterprise Change Manager reviews relevant documentation for customer confirmation of resolution and lessons learned, if applicable.

All changes are classified by impact values of high, medium, low, and transparent. High and medium impact changes require approvals from the Support Group Manager, the Enterprise Change Manager, and the Change Advisory Committee. High impact changes are also required to include testing, implementation, and back-out plans. Low impact changes require approvals only from the Support Group Manager and the Enterprise Change Manager. Transparent changes require no approvals and are to be reviewed by the Enterprise Change Manager on a monthly basis as required by the Remedy Guide.

The Change Advisory Committee consists of individuals from the Department as well as from multiple agencies and is chaired by the Enterprise Change Manager. Minutes along with reports, are posted to the Change Management SharePoint site, accessible by agency personnel.

Once a low, medium, or high impact change is approved, the Enterprise Change Manager sets the Remedy status to “Scheduled” and Remedy then generates email correspondence to the originator of the change request and to Department Subject Matter Experts required to implement the change. Transparent changes are set to “Scheduled” by the Shared Service Technician.

Change Control – Applications (AIS, CIS, CTAS, CPS and eTime)

EAA staff follow processes outlined in the Application Lifecycle Management Manual and the EAA Project Development Web Methodology when conducting change control.

The Department’s application change management process begins with the submission of a Help Desk Ticket or Change Ticket via Remedy. A single request may be a body of work containing multiple tasks, some of which necessitate a change to application code, application database, or generating new report.

A Help Desk ticket or Change Ticket originate from agency IT Coordinators based on requirements identified by a business owner. The agency IT Coordinators enter change requirements into Remedy and assign an EAA group to the Help Desk ticket or Change Ticket. The EAA group assignments may also be assigned by the Department’s Help Desk staff.

When a Help Desk ticket or Change Ticket is entered into Remedy, classification and priority codes may be assigned indicating emergency or normal classification and low, medium, high, or critical priority.

In addition to Remedy's internal classification and priority settings, the web application development group, which is responsible for changes to eTime, maintains a separate spreadsheet classifying tasks into "break/fixes” or "enhancements" and prioritizing them into high, medium, or low.

Once a Help Desk ticket or Change Ticket has been assigned to an EAA group, appropriate EAA staff (e.g. developers) becomes responsible for completing the tasks necessary to implement the change.

Developers complete the necessary coding, conduct tests to validate change correctness and appropriateness, and obtain user acceptance approval. User acceptance approvals are documented by email correspondence.

For mainframe application changes, a revision control and code management system permits a developer to 'checkout' program code; however, prohibits modified code from being placed back into the production area without proper authorization. The developer sends a move sheet (which links program changes to the Remedy Help Desk ticket or Change Ticket) to a secure email account shared by the EAA supervisor. The EAA supervisor then reviews the move sheet and after approving it, forwards appropriate documentation to a different secure email account shared by Library Services. Library Services then carries out the move sheet instructions following directives within the Department of Central Management Services Bureau of Communication and Computer Services Library Control Standards publication. Library Services sends an email back to the originating EAA supervisor and developer indicating the status of the move activity. The Remedy Help Desk ticket or Change Ticket is closed after a period of time, depending on attributes such as impact (minor/major significance) or complexity (simplistic or complicated).

For web application changes, once a user emails acceptance of the modification, the developer requests permission for production deployment from the EAA Web Group supervisor via email. Once the EAA Group supervisor approves the request for deployment, the developer creates a task on the Remedy Help Desk ticket or Change Ticket requesting deployment to production. Separation of duties is accomplished through the practice of assigning the move-to-production task to a different developer than who coded and tested the change. In addition, there are a limited number of staff authorized to deploy to production. The Remedy Help Desk ticket or Change Ticket order is considered resolved after all tasks on the ticket have been closed.

Change Control-ERP

The Department has a documented change management process in place to ensure changes to the ERP are properly initiated, authorized, planned, tested and approved prior to being placed into production.

An agency submits a request for assistance with an issue to the IT Service Desk, The IT Service Desk will log the incident into Remedy and assign to Production Support for resolution. Production Support will review the Remedy ticket to determine if the issue is an incident, defect or a change request. If the issue is deemed an incident (questions from the agency), it will be resolved per the ERP Help Desk process and tracked in Remedy.

Defect

The Department defines a defect as an instance where the ERP is configured incorrectly or improperly coded. There are two types of defects:

- Configuration
- Transport

If configuration is required, then Production Support applies the configuration in development and it's subsequently tested and approved by Production Support. Next the configuration is applied and tested in the quality region and tested by Production Support. These results are reviewed and approved by the State Functional Expert. A State Project Manager (or their designee) must approve a Governance, Risk Management, and Compliance Management (GRC) emergency access request so that the State Functional Expert or Production Support can perform the configuration in Production. Finally, the same State Project Manager (or their designee) must review and approve a GRC activity log detailing the configuration activity.

For transport related requests, there are two paths: one for ERP functionality and security changes, and one for technical changes, which are managed by our hosting provider. If functional or security related, then Production Support tests and approves the change in the development region. Next, the changes are transported to the quality region and tested by Production Support. The State Functional Expert reviews and approves the results from the quality region. Finally, a State Project Manager (or their designee) approves the results, which are stored in Hewitt Packard Quality Control (HPQC), which authorizes Production Support to transport to Production. If technical, then the hosting provider applies the transport to the Production based upon an agreed upon schedule with the State or alignment with the State Technical and Quality Project manager.

Once successful completion and approval of testing is completed, the defect is eligible for release. Releases are conducted weekly and must be approved by the Project Manager or designee.

After release, the agency who submitted the defect is notified of the resolution and the associated Remedy ticket is closed. Documentation of testing, approvals and release related to the defect is maintained either in HPQC and aligned to the appropriate defect or change request numbers (for transports) or externally by the Production Support team (for configuration).

Change requests

Change Requests (CR) are defined as instances where the requested functionality is not part of the approved design. If the incident is determined to be a change request, the incident is closed in Remedy and the agency is to complete a CR, via the ERP SharePoint.

All change requests are evaluated for requirements validation, then level of effort is added, and subsequently, a State Project Manager makes a recommendation for disposition. Finally, the State Program Director determines a disposition of approval or rejection. If a CR is rejected, the requestor is automatically notified. If the CR is approved, the agency is notified and then the CR will be scheduled by the ERP team for release based upon priority, complexity and capacity.

There are four main phases for approved CR: design, build/configure, test, and release. In the design phase, the Production Support team works with the appropriate Functional Expert(s), and if needed agency Subject Matter Expert(s) to align on the exact business requirements. Once that alignment occurs, the Production Support team will draft a functional specification design (FSD) document and submit it to the appropriate Functional Experts(s) for review and approval. If needed, the Functional Experts(s) may choose to include agency Subject Matter Expert(s) in the review process. Ultimately, the Functional Expert(s) must approve the FSD before technical design will commence. The technical specification design (TSD) is drafted by the Production

Support development team, which is subject to approval by the Production Support technical lead(s).

Once the FSD is approved and the TSD is completed, the build/configure phase starts. Configuration is handled by the Production Support team and/or the appropriate Functional Experts(s), depending on the specific nature of the configuration.

After the build/configuration phase is completed, the testing phase starts. The Production Support team completes Technical Unit Testing (TUT) and obtains approval. The Production Support team requests that the Production Support basis team transport changes to the quality region. Next, the Production Support team aligns with the Functional Experts(s) on the required Functional Unit Testing (FUT) test steps and test data. The Production Support team executes the FUT, with assistance from the Functional Experts(s), if needed. The Production Support team then formally presents the FUT steps and results to the Functional Experts(s), who are responsible for review and approval. The Functional Experts(s) will request assistance from agency Subject Matter Experts(s), if needed. If the FUT results are not acceptable, the Functional Experts(s) work with the Production Support team to return to the appropriate phase, which could be design, build/configure, or testing. If the FUT results are acceptable, the Functional Experts(s) provide approval. All TUT and FUT test steps, results, and approvals are stored either in HPQC and aligned to the appropriate defect or change request numbers (for transports) or externally by the Production Support team (for configuration). Once the test results are approved, the CR or defect is eligible for the release management process. CR releases normally occur on the third Thursday of each month.

Move to Production (Release)

The process by which changes are moved to other environments is called transporting. All transport requests are tracked in HPQC, and associated with the defect or CR number. Transport approvals are also captured in HPQC, through status change from “Pending State Approval” to “Ready for Transport”. A transport is only eligible when a Project Manager, or their designee updates HPQC with the “Ready to Transport” status.

Transports are moved through the regions by the Production Support basis team members; these are not the same individuals that perform the design, build/configure, or test phases.

The ERP Manager – Work Management reviews a weekly report which details all change management activities completed by the Production Support team, including incidents, defects, and CRs. Additionally, the Program Manager – Work Management and Program Director receive and review a monthly report detailing multiple reports highlighting ticket trends and analysis, as well as service level agreement (SLA) acknowledgement and incident resolution details, and finally a reporting of hours consumed.

Emergency releases

The Program Managers or their designated have the authority to allow emergency releases for defects or CRs, based upon a subjective analysis on the impact to the users. Emergency releases occur on-demand, after proper authorization and approvals are documented in HPQC (for transports) or GRC (for configuration).

Network

Network infrastructure modifications are categorized into two groups with differing change control procedures. For common infrastructure devices, the Department maintains detailed technical specifications identifying mandatory configuration parameters. Devices supplied by a vendor that meet those exact specifications are attached to the network when received within operational workload constraints. Devices for which the Department has no detailed technical specification defined or for which the Department has determined may cause a significant impact, undergo a two-step change management process. The first step is a Network Operations internal peer review where the network modification is reviewed by subject matter experts and approved by Department network architects. The second step is to submit the network modification through the change management process for approval by the Change Advisory Committee. The Department change management procedures are then followed to implement the network modification. Emergency or break/fix network changes are implemented as soon as operationally possible and are followed-up, after-the-fact, with documentation as required by the change management procedures.

IT Service Desk

The IT Service Desk serves as a central point of contact for requesting new services and to report problems encountered with existing support services. The IT Service Desk processes and manages information technology service requests, incident reporting, major outage notification, account maintenance, and password resets.

Incident Management

Unplanned interruptions to IT services, reduction in the quality of IT services or the failure of a configured item defines an incident. Such incidents are to be reported to the IT Service Desk by staff and agencies, via phone, email or a report via the Department's website. When the IT Service Desk receives a report of an incident, a Remedy ticket is to be opened, documenting the user's name, agency, and contact information along with a detailed description of the incident. Each incident will be categorized based on the service, system or application impacted by the incident. Tickets are also prioritized based on the impact (the number of affected users) and urgency (how quickly the resolution is needed) of the incident. The IT Service Desk then assigns the Remedy ticket to the applicable service group for remediation.

The applicable service group receives notification of the Remedy ticket, conducts remediation efforts and marks the Remedy ticket as resolved once rectified.

The Department has developed the Incident Management Process Guide to document the remediation process of reported incidents.

Major Incident (MORTS)

In the event of a major outage or infrastructure failure, a MORT (Major Outage Response Team) is activated. A MORT is initially reported as an incident to the IT Service Desk and evaluated by the IT Service Desk to determine if the incident should be elevated to a MORT. Upon determination of a MORT, the Remedy ticket is assigned to the Major Outage Response Team.

In addition, the IT Service Desk will initiate a MORT email notification across the call centers and the MORT members. The email notification will indicate a time and number for a conference bridge in order to discuss the remediation efforts when there is a question as to the cause of the outage.

Based on the event, a specific team/division will be notified in order to conduct the remediation efforts. During the remediation efforts, the Department will communicate with the affected agencies as to the progress. Upon completion of the remediation, the agencies will be notified and the Remedy ticket will be closed.

The Department has documented their procedures in the MORT Initiation Procedure.

Lost or Stolen Equipment

The Mobile Device Security Policy and the Enterprise Desktop/Laptop Policy requires users to report to the IT Service Desk any lost or stolen equipment. Upon notification, the IT Service Desk creates a Remedy ticket. In the event the item is stolen, the IT Service Desk attaches a copy of the police report to the Remedy ticket and contacts End User Computing for verification of encryption. Upon confirmation of encryption, the Remedy ticket is updated to reflect such.

In the event the equipment was not encrypted, an analysis will be conducted to determine what type of information was maintained. If it is determined sensitive/confidential information was maintained, the Security Operation Center will enact the breach investigation and response process.

Additionally, Asset Management will forward a copy of the police report to the Illinois State Police for further investigation and will complete a request for deletion of the asset from Remedy.

The Department's Missing IT Equipment Procedures provide guidance on missing and stolen equipment.

ERP- Helpdesk Monitoring Process

Upon receipt of a Remedy ticket, the IT Service Desk will assign the Remedy ticket related to the ERP to the ERP Help Desk ("Production Support"). Production Support will perform a series of actions to confirm and resolve an incident.

The process flow details the actions taken once an incident (i.e. ticket) is assigned to the Production Support. Upon receipt of a Remedy ticket, Production Support will leverage the Remedy system in order to track the incident until resolution. Production Support then sends an acknowledgement of the ticket to the submitter/user.

At this point, Production Support triages the Remedy ticket to first determine if it can be resolved without a change to the ERP. Production Support interacts with the user to address the incident. If it can be resolved without a change, Production Support sets the status of the

Remedy ticket to “Resolved”, which in turn automatically notifies the user of resolution via email.

If the Remedy ticket is determined to be a defect that requires a change, the Remedy ticket is replicated to the Production Support SharePoint and assigned to the appropriate Production Support team member(s). The status of the ticket is set to “Work in Progress” in the Production Support SharePoint, an analysis is completed by Production Support and the defect follows the defect process flow.

If Production Support determines that a Change Request is required, then the user is notified that they have an opportunity to enter a CR in SharePoint. At this point Production Support will change the status of the SharePoint ticket to “Resolved”, as well in Remedy, which in turn automatically notifies the user of resolution via email. This “Resolved” status is because the path forward requires the user to submit a CR and follow the change management process flow.

Production Support hosts a weekly meeting with ERP management to provide status updates. Additionally, Production Support provides ERP management with written weekly updates and monthly reports.

Logical Security

Access Provisioning

The Department has developed several policies and procedures governing logical security over access to the environment.

Upon receipt of an approved ESR from an agency IT Coordinator for a new employee/contractor, the IT Service Desk will assign “tasks” to the applicable groups/divisions for completions. The group/division is then required to create the applicable accounts as noted in the ESR and provide the applicable equipment. As the group/division completes the task, the task is to be closed. Once all tasks are completed, Remedy will automatically close the ESR.

Until December 12, 2017, if an individual required a security software account, an approved Mainframe Security Request Form had to be completed. After December 12, 2017, the Mainframe Security Request Form is no longer required; the applicable information is included in the ESR.

In the event an employee/contractor requires modification to their access rights or equipment, the agency IT Coordinator is to submit an approved ESR, documenting the modifications. Once received, the IT Service Desk will assign “tasks” to the applicable group/division for completions. The group/division is then required to modify the applicable accounts as noted in the ESR or provide the applicable equipment. As the group/division completes the task, they are to close the task. Once all tasks are completed, Remedy will automatically close the ESR.

Upon notification of an employee/contractor terminating, the agency IT Coordinator is to submit an ESR noting the employee/contractor accounts and equipment. Once received, the IT Service Desk will assign “tasks” to the applicable group/division for deactivation of accounts and the collection of equipment. As the group/division completes the task, the task is to be closed. Once all tasks are completed, Remedy will automatically close the ESR.

Access Provisioning - Applications

The security over the mainframe applications is a three – layer approach; network ID, mainframe ID, and an application specific ID. In order to obtain application access, the agencies are required to establish an agency Application Administrator. To request the establishment of the agency Application Administrator, the agency's IT Coordinator is to submit an approved ESR.

The agency Application Administrator is then responsible for the management of their agencies' accounts; assignment of individual rights, modification of rights and deactivation of rights. The agencies are responsible for ensuring the proper assignment of rights (segregation of duties); as each application ID may be assigned multiple rights; entry, approval, edits, etc. In addition, it is the responsibility of the agencies to review the access rights to their data.

The agency Application Administrator is also responsible for resetting of their agency user's passwords. In the event of an issue, the Department will assist the agency Application Administrator with resets; however, a request is to be submitted via an ESR.

When requested, the Department will provide instructions and training to agency Application Administrators on a one-on-one basis.

eTime security is tied to Active Directory. In order to obtain access to eTime, agencies are required to establish an eTime Administrator. To request the establishment of an eTime Administrator, the agency's Human Resource Director submits an approved ESR. The agencies are responsible for informing the Department of a change in the agency's eTime Administrator.

The eTime Administrator is responsible for the assignment of eTime roles for their applicable agency. eTime has defined functional roles, which specific actions are allowed and by whom; timekeepers, supervisors, or employee (subordinate). The timekeeper role makes adjustments in eTime to release the time report resulting from employee error so that an employee can then resubmit their time report. The supervisor role can approve employee time, overtime, and leave requests. The employee role permits employees to make adjustments that ultimately affect their paychecks. In addition, it is the responsibility of the agency to review the access rights to their data.

When requested, the Department will provide instructions and training to agency eTime Administrators on a one-on-one basis.

The ERP utilizes the Governance, Risk and Compliance (GRC) tool to automate user access provisioning, provide enhanced management of roles, including emergency access, and enable proactive Segregation of Duties ("SOD") monitoring.

There are four types of users: dialog, system, service and communication. End users are assigned dialog type. The dialog type logs in interactively and the password expires according to the defined profile parameter. For interfaces, System and Communication user types are assigned.

These two types of users cannot be used to log in interactively. Firefighters are service user types. The principle of least privilege access is followed, which prescribes that every user should have access only to the information and resources that are necessary for a legitimate purpose.

Access Provisioning-ERP

When a new user needs added, the agency enters the access request into GRC and applies the first level of approval. The request is then sent to ERP security for segregation of duties conflicts. If no conflicts are noted, the request is approved. In the event a conflict is noted, the ERP security and the agency work to resolve by applying mitigating controls. No access is granted when segregation of duties conflict exists and a mitigating control is not applied.

Upon approval, an email is sent to the new user with their user ID and a temporary password. Upon login, the user will be required to create a new password.

To change a user’s access, the same process is followed.

Access De-provisioning

When a user no longer requires access, the agency enters a request into GRC and approves. The user access is then automatically disabled.

Reviews

Annually, the ERP security team sends User Access Reports to the agencies documenting their users and the associated rights, which are to be reviewed. Required changes are to be processed via the GRC process. Upon completion of the review and any required changes, the agencies are to document such review and return to the ERP security team.

Password Resets-Mainframe

In the event a user requires a reset of their mainframe password, they are required to either submit the request via email to the IT Service Desk or use DIM (DoIT Id Management); the Department’s self-service option. Email reset requests are to include the user’s name, mainframe ID and a contact phone number. The IT Service Desk staff will contact the user at the number provided and reset the mainframe ID password. If the IT Service Desk staff are not able to reach the user, a message is left for the user that includes the Remedy ticket number instructing them to contact the IT Service Desk, at which time the password will be reset.

When the individual returns the IT Service Desk call, the individual’s id is verified with the information within the Remedy ticket prior to resetting the password.

In the event the IT Service Desk staff does not have the appropriate rights to reset a mainframe password, a Help Desk ticket is opened in Remedy and assigned to the Security Software Coordinator or the Security Software Administrator for the Department. Upon assignment, the Security Software Coordinator or the Security Software Administrator will contact the individual, verify their id, and reset the password.

Password Resets (Active Directory)

Active Directory accounts are reset by calling the IT Service Desk or by using one of the Department's self-service options – Forefront Id Management (FIM) or DIM. When a call is received by the IT Service Desk for an Active Directory password reset, IT Service Desk staff will determine if the caller is eligible to use FIM / DIM and if they have previously registered. If registered, users will be directed to reset via this method. If they are unsuccessful, have not previously registered or are not eligible to use FIM / DIM, IT Service Desk staff will proceed with the reset after verification of two of three pieces of information. Once a successful reset has taken place, users will be instructed to either register or re-register for FIM, if they are eligible.

Password Resets (Novell)

Novell password resets are performed by calling the IT Service Desk. IT Service Desk staff will perform a verification of two of three pieces of information before resetting the password.

ERP Password Resets

Agency end users are required to submit a request through the IT Service Desk, which is then assigned to Production Support. Password reset requests must include the user's name, agency, user ID, and a contact phone number. If any information is unclear, Production Support will contact the user at the number provided. Regardless of what information is provided in the request, a temporary password is only emailed to the approved email address that is on record.

System Security-Mainframe

The Department utilizes security software as a method of controlling and monitoring access to the mainframe resources.

The security software requires an established ID and password in order to verify the id of the individual. The primary means of defining an individual's access is the security software profile. The security software profile defines the level of access a user has.

Password security parameters have been established and configured to ensure access to mainframe resources is appropriate:

- Minimum password length;
- Password complexity;
- Password history;
- Minimum password age; and
- Number of invalid login attempts.

Additionally, the security software passwords are maintained in an encrypted database.

For agencies which do not have a Security Software Coordinator, the Department conducts the Security Software Coordinator activities on their behalf (proxy agencies). Agencies with a Security Software Coordinator are responsible for monitoring/reviewing the security software accounts assigned to their agency.

On an annual basis, the Security Software Administrator sends proxy agencies a listing of security software IDs assigned to their agency for review. The agencies are to review the listing and provide a response back to the Security Software Administrator stating the IDs are appropriate or indication which IDs are to be revoked. Additionally, on a monthly basis, the Security Software Administrator runs a report documenting IDs which have not been utilized in the past 90-days; upon review, the IDs are disabled.

The Security Software Administrator runs a weekly violation report which is reviewed for invalid and unauthorized access attempts of proxy agencies security software IDs. The Security Software Administrator contacts the individual or their supervisor to determine the reason for the violation.

Bi-monthly, the Security Software Administrator receives a separation report from Human Resources. The Security Software Administrator reviews the separation report, noting separation of individuals from proxy agencies. If a separation is noted, the Security Administrator will revoke the individual's security software ID.

System Security-Midrange

The Department utilizes Active Directory as its method for controlling and monitoring access to the midrange resources.

In order to access the midrange environment, an ID and password are required. Password security parameters have been established and configured to ensure access to midrange resources is appropriate:

- Minimum password length;
- Password complexity;
- Password history;
- Minimum password age; and
- Number of invalid login attempts.

Beginning in January 2018, the Department performs a monthly review of all Illinois.gov Active Directory accounts and disable accounts which have been dormant for 90 days or more. Agencies are provided a listing of the disabled accounts instructing them to review and to provide an explanation in the event the account needs to be reactivated or kept for a valid business need. In the event the agency determines the account is no longer needed, they are instructed to submit an ESR for removal of the account. If the agency does not provide a response to the Department, after 90 days the account will be eligible for the auto-delete process.

System Administrators-Mainframe

Access to the operating system configurations is limited to system support staff; system programmers and security software personnel. Access with powerful privileges, high-level access and access to sensitive system functions is restricted to authorized personnel.

On an annual basis, the Security Software Coordinator conducts a review of security software IDs with powerful privileges.

System Administrators-Midrange

Access to administer the midrange environment is limited to authorized technical support personnel.

On an annual basis, the Department's Wintel Admin Team conducts a review of the technical accounts to ensure appropriateness. The supervisor of the technical account owner is requested to provide an explanation for the account. In the event the technical account is no longer required, an ESR is completed in order to deactivate the account.

Application Administrators/Programmers

Access to application source code, Job Control Language (JCL) streams, data files and sensitive application functions are restricted to authorized personnel. To request access, the access provisioning process is to be followed.

Firefighter IDs-ERP

The Firefighter ID provides access to administrative rights; limited to ERP functional experts and authorized production staff. In order to obtain Firefighter access, the user enters a request into GRC, providing a specific reason for the access and a statement if production data is going to be altered or not. If the user is going to alter production data, approval from the applicable agency must be attached; or the request will be denied.

If approved by the ERP security, the user will receive an email stating the request has been approved.

Network Operations

The Department manages firewalls, routers, switches, cabling, servers, and software that are the components to the backbone, wide area network, local area network, and virtual private network infrastructures. Infrastructure component equipment may be physically located at Department facilities or on agency premises. Mandatory backbone design and configuration standards and guides are defined and maintained. The Department has implemented redundancy between pop-sites where technically, fiscally, and operationally feasible and has also installed fiber optic wave transmission technologies to selected sections of the managed backbone. Network diagrams depict common connectivity configurations.

Virtual Private Networks (VPN) provide controlled and trusted connections between devices when data travels over public networks including the Internet. The Department's Enterprise VPN Standard provides guidance when establishing a VPN connection. When data travels across a public network, it is encrypted at the access router and while in transit across the public network until it reaches the distribution router and enters the private network.

As a security awareness mechanism, a security banner is displayed at initial network connection warning of prosecution for unauthorized access.

Modification to the network is restricted to Department authorized technicians and authorized vendors. Authorization and access rights to a network-attached device by either a Department technician or vendor specialist requires assignment of an Active Directory account, inclusion in a specific access-rights group, and use of a Department issued token. All are required before network access is granted. Active Directory accounts are assigned and issued through access provisioning procedures. Department staff with a business need to access or modify network devices are added to a designated Active Directory access group and setup with a two-factor authentication token. A token is issued to only authorized staff which requires supervisor approval. Tokens remain inactive until a challenge/response procedure is successfully completed. This procedure requires the Department's Two-Factor Authentication Administrator communicate certain information to the technician in real time in order to activate the token.

Additional security measures are applied through use of Access Control Lists and Authentication Servers. Access Control Lists reside on the network device itself and restrict communication to only certain IP addresses or address ranges. Authentication Servers control access through assignment of access right privileges (read only or update) based on Department-defined group profiles. Authentication Servers record failed login attempts to the network equipment which are processed by the Network Operations Center.

The Department conducts a backbone health-check assessment by evaluating availability statistics (percent of time network was operational) and reviewing threshold metrics (how effective did the network operate). The statistics and threshold metrics are reviewed and recorded monthly.

The Department applies self-monitoring hardware and software, redundant backbone construction, scheduled backups, and vendor-based services in order to maintain network availability. Self-monitoring network hardware devices are encoded with filters that automatically generate system entries when an industry or Department defined parameter or condition occurs. Network Operation Center staff reviews each occurrence and engage operation teams for resolution. Network software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. Network hardware and software generates an email or console display alert when a predefined event occurs or a threshold is reached. The Network Operations Center follows-up on these alerts. Backups are scheduled based on device type; daily or weekly. Firewall, router, and switch configurations are backed up and stored at the CCF and/or the Alternate Data Center (ADC).

The Security Operations Center utilizes a myriad of tools to continuously monitor the network for the detection and analysis of potential intrusions, cybersecurity threats, and incidents.

Depending on the threat, the Security Operation Center has established Standard Operating Procedures to assist with the detection, analysis and resolution.

Upon notification of a threat, an Incident Report is completed for incidents that are classified as medium or high. The Incident Report contains details of the threat and its resolution. The Incident Reports are reviewed by the Chief Information Security Officer.

Additionally, various reports are provided to management for review:

- Daily the Shift Change Report is completed at the end of each shift documenting information regarding incidents the next shift should be aware of.

- Weekly Activity Report documents a summary of the incidents noted during the week and a summary of the incident and resolution.
- Monthly, quarterly, bi-annually, and annually Metric Reports are completed documenting the statistics on incidents.

Patches/Antivirus
The Department receives Microsoft Windows patches monthly. The patches are first tested with the technical staff, then a pilot group, and then pushed out to the general population. The patch process follows the Department's change management process. The Department utilizes Microsoft's System Center Configuration Manager (SCCM) to push and monitor Windows patches.

The Anti-Virus Group is responsible for pushing daily definitions and other antivirus software updates out. The definitions are delayed six hours before being pushed to users. This allows the staff to review and ensure no issues are encountered. The pushes follow the change management process. The Anti-Virus Group has tools available to monitor the enterprise computing equipment that are out of compliance regarding antivirus definitions.

Computer Operations

The Operation Center continuously monitors the operation of the computing resources to ensure availability, performance, and response necessary to sustain agency demands. The Operation Center operates 24 hours a day, 7 days a week, 365 days a year.

The Operations Center utilizes software and the Automated Operations Console in order to continuously monitor the environment. Problems, issues, and incidents are recorded via the Daily Shift Reports and a Remedy ticket is created. In the event the Operations Center cannot resolve the issue, the Remedy ticket is assigned to the applicable group/division for resolution.

The Daily Shift Report documents the activity conducted on all mainframe production systems and incident calls received at the Operations Center. The Report contains the date, time, system involved in the incident, along with a narrative providing any necessary information regarding the incident. The Report is reviewed by ISD management and supervisors.

In the event division staff or management needs to be notified, contact information is maintained within the FOCAL database.

The Operator Shift Change Checklist is completed at the beginning of each shift to ensure the production systems are operating appropriately and any open items are passed on to the next shift and to identify any changes which need to be made. The Checklists are reviewed by the Operations Center supervisor.

Mainframe
The mainframe environment is monitored through the z/OS systems console for errors and issues. Operations Center continuously monitors the system console.

Mainframe system performance and capacity is monitored by System Software programming personnel, via Remote Monitoring Facility (RMF) reports. RMF reports are run weekly and monthly. Performance and capacity monitoring is documented via internal memorandum distributed to ISD management, monthly.

The Department has implemented system options to protect resources and data. The System Management Facility (SMF) records the operating system activities. The manager of Mainframe Software Support reviews the SMF records corresponding to the Department's profiles on a weekly basis.

Midrange

The midrange environment availability and performance is monitored via What's Up Gold. Proactive performance and capacity monitoring is performed for the midrange environment utilizing What's Up Gold and Microsoft's System Center. Alerts are sent to the Operations Center when certain performance and capacity loads meet or exceed set thresholds. Email notifications are also sent to responsible team/group technicians, who review the alerts and take corrective action.

SQL Database servers/software performance is monitored using What's Up Gold, Microsoft SQL utilities, and Idera tools. The Command Center follows their outage procedures if WUG alarms on a SQL server, by contacting the staff assigned to the server experiencing the outage. The Wintel SQL support staff monitor the Idera and Microsoft SQL Utilities during normal working hours. These tools also provide email alerts to the Wintel SQL support staff 24/7 if any alarms occur. They will review and take appropriate actions as necessary.

Data Storage

Data Storage performance and capacity are monitored using EMC Toolsets. When there is an equipment outage or performance issues, Data Storage Technicians contact the equipment or software vendor.

Automated alerts are sent via email to Data Storage Technicians and management when capacity is reached or exceeds 80%. Mid-Range System Data Backups are monitored by EMC tools and IBM Spectrum Protect.

The MOVEit File Transfer Protocol software and standard Secure File Transfer Protocol (SFTP) are both used to transmit data between the Department and the agencies. Errors that occur on data file transmission with MOVEit and SFTP systems result in an automated notification being sent to the Production Control Team for resolution. The errors are recorded in the Shift Change Checklist and a Remedy ticket is created in order to track the error to resolution.

Access to MOVEit and SFTP systems are reviewed on an annual basis by the Department.

The Department has developed the Data Processing Guide in order to provide staff with instruction related to their various tasks.

Backups

Mainframe

The Department is responsible for monitoring the backup process, while the agencies are responsible for the scheduling of mainframe backups. Data on mainframe systems are backed up daily and weekly utilizing Virtual Tape Technology (Disk Library Management (DLM)). The Department utilizes CA Scheduler to schedule and verify the completion of the backups.

The Department has implemented backup policies to assist staff in the event of failures.

Daily, Storage staff review the output of the daily backup jobs for any failures. In the event of a mainframe daily backup job failure, the Operations Center staff records the incident in the Shift Report. The next working day, Storage staff review the Shift Report to identify the problem, correct and resubmit the failed portion of the backup job.

The Storage personnel review the output of the weekly backup jobs for success or failure. The failure is researched and corrected, and then the failed portion of the backup job is resubmitted for completion.

Data replication is performed between the CCF and the ADC. Mainframe data replication occurs every 10 minutes between the CCF and the ADC DLM. The monitoring software sends the Enterprise Storage and Backup group an alert if the data is out of sync for more than 8 hours. If there is an issue, a Remedy ticket is opened in order to track the Enterprise Storage and Backup group's progress on resolution of the issue.

The DLM Replicated Status log keeps a log of replication between the two DLMs and tracks library replication outcomes for DLM replication activity. These logs document the status of the replicated libraries and the time of the last sync and are maintained for seven days.

Midrange

Spectrum Protect and Avamar are used to back up the midrange environment. Data Protection Advisor is used to monitor and report on Midrange backups. Midrange server backups are performed daily or weekly and are either incremental or full. On a daily basis, Spectrum Protect and Data Protection Advisor automatically generate reports indicating the backup status of all scheduled jobs from the prior day. These reports are emailed to the Enterprise Storage and Backup group. Enterprise Storage and Backup group investigates the cause of the failure and works to resolve the problem.

Backed up server data is written to a Data Domain storage system and then replicated to another Data Domain storage system at the ADC. The Data Domain storage systems generate a daily status report which is emailed to the Enterprise Storage and Backup group. The Data Domain storage systems also send email alerts to the Enterprise Storage and Backup group when issues arise that may need additional attention. Enterprise Storage and Backup group investigate the issue until a satisfactory conclusion is reached. The Data Domain systems automatically alert vendor support in the event of hardware or system failures.

The Data Domain storage systems are also a target for SQL, DB2, and Oracle backups. The database backups are written to the Data Domain storage systems via Common Internet File System or Network File System and then replicated to the ADC. It is the responsibility of the SQL team to perform and monitor the success of the database backups.

A powershell script goes through the production SQL servers and creates a report with the latest backup date and it is sent to the SQL team daily. The SQL team reviews it for any failures. The SQL team also gets alerts from the SQL servers when backup jobs fail. Additionally, the SQL team receives alerts from the Idera monitoring software if a database has missed a backup on consecutive nights.

Any data, including, but not limited to SQL, Access, DB2 databases, user shared documents and user profiles are located on the Isilon storage device via the Network File System or the Service Message Block shares. The Enterprise Storage and Backup group has policies on the Isilon that take daily snapshots of all shares which are then retained for 60 days. The Isilon also has daily synchronization with the ADC to another Isilon storage system. The Isilon generates a daily report showing all successful and failed synchronization attempts with the ADC. Enterprise Storage and Backup group investigate failed synchronization attempts until a satisfactory conclusion is reached. The Isilon has a call home feature that will notify vendor support and the Enterprise Storage and Backup group during any disc or hardware failure.

Physical Security

To gain access to the CCF and the Communications Building, an individual must obtain an ID Badge. Prior to April 1, 2018, in order to obtain an ID Badge:

Communication Building-Employees and Contractors

The Human Resources submits an approved ID Badge Request Form or an email to the Department of Central Management Services' Property Management for the creation of the ID Badge.

CCF-Employees and Contractors

The Infrastructure Services Management Team submits an approved ID Badge Request Form or an email to the Department of Central Management Services' Property Management for the creation of the ID Badge.

Effective April 1, 2018, the Department took responsibility for physical access provisioning. Below are the Department's controls:

Communication Building-Employees and Contractors

Human Resources obtain approval from the employee or contractor's supervisor for the creation of the ID Badge. Upon approval, Human Resources create the ID Badge with the applicable access rights.

CCF-Employees and Contractors

The Assistant Chief of Enterprise Infrastructure and Manager of Enterprise Production Operations submits an approved ID Badge Request Form or an email to the Department' Human

Resources for the creation of the ID Badge. Human Resources will then create the ID Badge with the applicable access rights.

Access Reviews

Monthly, the Infrastructure Services Management Team conducts informal reviews of individuals who have access to the CCF data center to ensure proper access is being granted. The review consists of monthly meetings to review the most current access list for the CCF data center. The access list is informally reviewed to verify completeness and accuracy.

Internal Control Framework-Department of Central Management Services

This section provides information about the five interrelated components of internal control at the Department of Central Management Services, including the Department of Central Management Services':

- Control environment;
- Risk Assessment;
- Information and Communication;
- Control Activities; and
- Monitoring.

Control Environment

The organizational structure of the Department of Central Management Services provides a stream-lined management, accountability, and efficiency in delivery of services to other State agencies.

The Department of Central Management Services is organized into functional areas and organizational and reporting management structures are established. The Director is the leader and reports to the Governor's Office. There are two Deputy Directors who report to the Director that manage the Bureau of Personnel and the Bureau of Property Management. The Bureau of Personnel manages Internal Personnel and the Bureau of Property Management manages physical security. This organizational structure allows for proper segregation of duties.

The Department of Central Management Services has formal policies and procedures related to human resources, administration and operations which define roles and responsibilities of its employees.

Human Resources

Effective August 15, 2017, the Department of Innovation & Technology took responsibility for the posting of vacant positions. Prior to August 15, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department of Central Management Services.

The Department of Central Management Services adheres to the State's hiring procedures, Personnel Code, union contracts, *Rutan* decisions, and all other applicable laws, regulations and court-orders for the hiring of staff members. Newly developed and changes to established job descriptions require approval from Department Central Management Services' Technical Services. Once a job description is in place, the Department's Human Resources initiates a personnel action request (PAR) to request to fill a vacancy. The PAR must be approved by the Department's Chief Financial Officer and the Secretary, and the hiring process begins when DCMS posts the vacant position.

Effective September 18, 2017, the Department of Innovation & Technology took responsibility for the creation of the bid records. Prior to September 18, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department of Central Management Services.

Once the posting has closed, if the position is a bargaining unit position, the Department of Central Management Services compiles a bid record in accordance with the language outlined in the position's collective bargaining agreement. This dictates, based on contractual language, who has rights to the position. Once the Department of Central Management Services compiles all information received during the bidding process, the bid record is forwarded to the Department's Human Resources to commence the candidate selection and security process.

If the position is non-bargaining unit, after the posting notice has closed, all applicable applications are turned over to the Department's Human Resources. The Department's Human Resources is responsible for ensuring the completion of all Rutan covered interviews. Once the interviews are completed, the Department's Human Resources completes the Candidate Evaluation Forms and an Employment Decision Form. The file is then turned back over to DCMS and an official offer is made by the Department of Central Management Services based on the Department's selection. The Department of Central Management Services then finalizes the offer to the candidate and sends a notice to the appropriate staff within the Department's Human Resources and Budget Office and the Department of Central Management Services' Budget, Payroll, New Employee Orientation Coordinators, EEO Officer and Internal Personnel.

Effective October 13, 2017, the Department of Innovation & Technology took responsibility for submitting background clearances. Prior to October 13, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department of Central Management Services.

The Department of Central Management Services conducts and completes the background check and reports the corresponding findings to the Department's Human Resources for review prior to the employee's hire date. The Department's Human Resources then returns the worked bid record and file back to the Department of Central Management Services for the finalization of making the final offer to the candidate and sends a notice out to the appropriate staff within the Department's Human Resources and Budget and the Department of Central Management Services' Budget, Payroll, New Employee Orientation Coordinators, EEO Officer and Internal Personnel.

Effective October 16, 2017, the Department of Innovation & Technology took responsibility for conducting new employee orientation. Prior to October 16, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department of Central Management Services.

The Department of Central Management Services then administers new employee orientation and newly hired staff are given a packet of applicable forms for completion as well as Ethics and Security Awareness training and the Department of Central Management Services' Policy Manual. New Department staff and contractors are required to sign a statement signifying they will comply with security policies contained within the Policy Manual. The forms include the Security Awareness Training Acknowledgement form the new employee must sign to acknowledge receipt of the Department of Central Management Services' Policy Manual and indicate the new employee understands their responsibility to read and act in accordance with the State of Illinois Security Policies.

Effective November 16, 2017, the Department of Innovation & Technology took responsibility for employee evaluation reporting. Prior to November 16, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department of Central Management Services.

For performance evaluations, the Department of Central Management Services' Internal Personnel provides the Department's Human Resources a monthly report of annual employee performance evaluations (separated by division) that are due in the current month, upcoming in the next 2 months and any that are overdue.

Effective November 16, 2017, the Department of Innovation & Technology took responsibility for processing personnel transactions. Prior to November 16, 2017, the Department of Central Management Services was responsible. Below are the controls of the Department of Central Management Services.

Upon notification of separation, the Department's Human Resources submits a PAR form to the Department of Central Management Services for processing to facilitate employee separation from the Department and to discontinue time keeping and payroll.

Risk Assessment Process

The Department of Central Management Services identifies and manages risks related to the human resources and facility management services provided.

The Department of Central Management Services Internal Personnel Division receives and reviews payroll discrepancy reports twice monthly from the CMS Transactions to determine if there are any risks identified in the discrepancies noted. The Department of Central Management Services Internal Personnel Timekeeper reviews timekeeping discrepancy reports prior to payroll and timekeeping close dates looking for errors related to employees who are paid hourly and daily, employee temporary assignments, overtime and dockage, attendance and adjustment errors, sick advance, workers' compensation days off, maternity/paternity, military leaves, shift differential, holidays worked, other authorized time away from work, time owed, comp time and FMLA usage-accumulation to see if there are any risks identified in the discrepancies noted.

The Department of Central Management Services Bureau of Property Management has utilized vendors to perform inspections on facility systems to assess weaknesses in each facility.

Monitoring Controls

The Department of Central Management Services Internal Personnel monitors activities through the use of a Personnel Action Request Form (PAR). Bureaus submit PARS to the Department of Central Management Services' Internal Personnel for signature and routing to the Fiscal Office for budget approval. These are used to monitor any vacancy additions or changes, employee removals and employee changes. All hiring packets are reviewed by the Internal Personnel

Transactions staff and then sent to Transactions for a second review prior to them stamping the Director's signature to the hiring paperwork.

The Department of Central Management Services Bureau of Property Management maintains staff on-site to monitor the facilities' mechanical systems and facilitate any maintenance and repairs needed.

In addition, Internal Audit conducts audits of financial and operational controls. Internal Audit reports are provided to the Director.

Information and Communications

The Department of Central Management Services Internal Personnel staff communicates to employees and the Department via email, teleconference, personal meetings, telephone and face to face with walk-ins.

The Department of Central Management Services Bureau of Property Management has specific personnel assigned to handle various facility management duties at the Central Computer Facility (CCF) and the Communications Building. The selected Department personnel will contact the Department of Central Management Services' facility personnel with any facility questions or comments. In addition, the Bureau of Property Management uses a web based work order system that allows authorized Department staff to report facility issues.

Physical Security

Physical access to the CCF and the Communications Building are controlled and managed by the Department of Central Management Services Property Management. The CCF, as well as the Communications Building, are monitored 24 hours per day, seven days per week, 365 days per year by on-site security guards, proximity badge readers and security alarms. In addition, digital cameras are in place throughout both buildings and footage is retained for 14 days.

To control access to the CCF and the Communications Building, the Department of Central Management Services has installed proximity readers throughout the buildings. In order to gain access, an individual must have established physical access right within the Velocity Access Control system (Velocity) and have an ID Badge. Velocity will document/log the date, time and doors in which an individual entered.

Until April 1, 2018, the Department of Central Management Services was responsible for physical security access provisioning. Prior to April 1, 2018, in order to obtain an ID Badge;

Communication Building-Employees and Contractors

The Department of Central Management Services' Property Management must receive an approved ID Badge Request Form or an email from the Department's Human Resources documenting the physical access rights the Department of Central Management Services' Property Management is to establish for the individual. Upon receipt, the individual is to present a valid driver's license or State ID Card to the Department of Central Management Services Property Management in order to obtain the ID Badge. The Department of Central Management

Services' Property Management will then enter the individual's applicable information and take a picture which is loaded into Velocity for verification purposes.

CCF-Employees

The Department of Central Management Services' Property Management must receive an approved ID Badge Request Form or an email from the Department's Infrastructure Services Management Team documenting the physical access rights the Department of Central Management Services' Property Management is to establish for the individual. Upon receipt, the individual is to present a valid driver's license or State ID Card to the Department of Central Management Services Property Management in order to obtain the ID Badge. The Department of Central Management Services' Property Management will then enter the individual's applicable information and take a picture which is loaded into Velocity for verification purposes.

CCF-Contractors

The Department of Central Management Services' Property Management must receive an approved ID Badge Request Form or an email from the Department's Infrastructure Services Management Team documenting the physical access rights the Department of Central Management Services' Property Management is to establish for the individual. Upon receipt, the Department of Central Management Services' Property Management will then enter the individual's applicable information into Velocity. However, the individuals are not provided an ID Badge; rather, upon entry into the CCF, they are provided a temporary badge with the access documented within Velocity by the security guards.

When the individual enters the CCF they are to provide the guards a driver's license or State ID card in order for the security guard to verify their id. Once verified, the security guard will provide them a temporary badge with the access rights noted within Velocity. In addition, the individual is required to sign in on the register.

Change of Access Rights

In the event an individual's access requires modification, the process noted above would be followed.

Separation

The Department of Innovation & Technology's Human Resources emails the Department of Central Management Services' Property Management noting the individual's termination date. The Department of Central Management Services' Property Management will deactivate the individual's access effective the date of termination.

CCF and Communications Building-Visitors

Upon entry, the individual is to provide the security guards a driver's license or State ID card. The security guards then enter the applicable information into Velocity and provide a Visitor ID Badge; which provide no access rights. In addition, the individual is required to sign the Visitor Register and be escorted at all times by an employee.

Security Guards

The Department of Central Management Services' Property Management provides security guards 24x7x365 at the CCF and the Communications Building, who are responsible for patrolling and monitoring. There are specific post orders (standard operating procedures) for the individual sites. The post orders are developed in conjunction with the Department of Central Management Services and the Department. These orders outline specific reporting requirements along with the duties for the post. However, the guards use daily activity reports and incident reports in the course of their duties. On a monthly basis, the Department of Central Management Services receives a summary of this information.

The Department of Central Management Services has installed security alarms in various locations at the CCF and the Communications Building. The alarms are monitored by the security guards.

In addition, the Department of Central Management Services has installed digital cameras throughout the CCF and the Communications Building, which are also monitored by the security guards.

The Department of Central Management Services has installed preventive environmental measurers at the CCF and/or the Communications Building; fire extinguishers, fire suppression, sprinkler system, water detection, cooling/heating systems, UPS, and generators. The Department of Central Management Services has entered into preventive maintenance agreements for the environmental measures.

Objectives and Related Controls

The Department of Innovation and Technology and the Department of Central Management Services has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives, related controls, and the complementary user agency controls are presented in section IV, "Description of the Department of Innovation & Technology's and the Department of Central Management Services' Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results", and are an integral component of the Department of Innovation & Technology's and the Department of Central Management Services' description of Information Technology Shared Services System for the information technology general controls and application controls.

Complementary User Agency Controls

The Department of Innovation & Technology's and the Department of Central Management Services' controls related to the Information Technology Shared Services System for the information technology general controls and application controls cover only a portion of the overall internal control structure for each user agency of the Department of Innovation & Technology and the Department of Central Management Services. It is not feasible for the control objectives related to Information Technology Shared Services System for the information technology general controls and application controls to be achieved solely by the Department of Innovation & Technology and the Department of Central Management Services. Therefore, each agency's internal control over financial reporting must be evaluated in conjunction with the Department of Innovation & Technology's and the Department of Central Management Services' controls and the related tests and results described in section IV of this report, taking into account the related complementary user agency controls identified under each control objective, where applicable. In order for agencies to rely on the control reported on herein, each user agency must evaluate its own internal control structure to determine if the identified complementary user agency controls are in place.

SECTION IV

Description of the Department of Innovation & Technology’s and the Department of Central Management Services’ Control Objectives and Related Controls, and the Independent Service Auditor’s Description of Tests of Controls and Results

Description of the Department of Innovation & Technology’s and the Department of Central Management Services’ Control Objectives and Related Controls, and the Independent Service Auditor’s Description of Tests of Controls and Results

Information Provided by the Independent Service Auditor

This report, when combined with an understanding of the controls at the user agencies, is intended to assist auditors in planning the audit of user agencies’ financial statements or user agencies’ internal control over financial reporting and in assessing control risk for assertions in user agencies’ financial statements that may be affected by controls at the Department of Innovation & Technology and the Department of Central Management Services.

Our examination was limited to the control objectives and related controls specified by the Department of Innovation & Technology and the Department of Central Management Services in Sections III and IV of the report, and did not extend to controls in effect at the user agencies.

It is the responsibility of each user agency and its independent auditor to evaluate this information in conjunction with the evaluation on internal control over financial reporting at the user agencies in order to assess total internal control. If internal control is not effective at the user agencies, the Department of Innovation & Technology’s and the Department of Central Management Services’ controls may not compensate for such weaknesses.

The Department of Innovation & Technology’s and the Department of Central Management Services’ internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of controls specified by the Department of Innovation & Technology and the Department of Central Management Services. In planning the nature, timing, and the extent of our testing of the controls to achieve the control objectives specified by the Department of Innovation & Technology and the Department of Central Management Services, we considered aspects of the Department of Innovation & Technology’s and the Department of Central Management Services’ control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature to tests performed:

Test	Description
Inquiry	Inquiry of personnel and management.
Observation	Observation, performance, or existence of the control.
Inspection/Reviewed	Inspection/review of documents and reports indicating performance of the control.

In addition, as required by paragraph .35 of AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*), and paragraph .30 of AT-C section 320, when using information produced or provided by the Department of Innovation & Technology and the Department of Central Management Services, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Control Environment Objective: CE 1: Controls provide reasonable assurance that policies and procedures related to employee responsibilities and hiring have been established, new employees and contractors are screened and on-boarded, and that a defined organizational structure exist, that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY	TESTS OF CONTROLS	RESULTS OF TESTS
CE1.1	The organizational hierarchy promotes segregation of duties, monitoring of controls and customer support.	Reviewed the organizational chart to determine if appropriate segregation of duties, monitoring and customer support were promoted.	No deviation noted.
CE1.2	Each employee position has an approved formal written job description which documents the duties, qualifications, minimum acceptable competency education requirements, and experience levels.	Selected a sample of employee positions to determine if a job description had been completed and approved.	Job descriptions for non-code positions did not require the Department of Central Management Services' Division of Technical Services approval.
		Selected a sample of job descriptions to determine if they outlined duties and qualifications.	No deviation noted.
	For the period August 15, 2017 to June 30, 2018		
CE1.3	The hiring practices adhere to legal requirements as published in the State Personnel Code, Personnel Rules, Union contracts, Rutan decisions, court orders and applicable state/federal laws.	Reviewed the hiring procedures, Personnel Code, Union Contract, and Rutan decisions to determine hiring process.	No deviation noted.
	For the period October 13, 2017 to June 30, 2018		
CE1.4	New employee and contractors must pass a background check prior to being offered employment.	Selected a sample of new employees and contractors to determine if background checks were completed prior to being offered employment.	No deviation noted.

	For the period October 15, 2017 to June 30, 2018		
CE1.5	Newly-hired employees and contractors are provided the DCMS Policy Manual and are required to sign an acknowledgment form acknowledging responsibility to abide by the policies contained within the DCMS Policy Manual.	Selected a sample of new employees determine if the DCMS Policy Manual Acknowledgement had been completed.	No deviation noted.
		Contractors were not provided the DCMS Policy Manual or signed an acknowledgment.	Contractors were not provided the DCMS Policy Manual or signed an acknowledgement. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
CE1.6	Newly-hired employees and contractors are required to sign the acknowledgement included in the Security Awareness Training and Ethics Orientation acknowledging they have reviewed the materials and recognizes the responsibility to abide by the Security Awareness Training and Ethics Orientation for State Employees requirements.	Selected a sample of new employees to determine if acknowledgment of Security Awareness Training and Ethics Orientation had been completed.	No deviation noted.
		Selected a sample of new contractors to determine if acknowledgment of Security Awareness Training had been completed.	2 of 39 contractors selected had not completed security awareness training.
		Collaboratively inquired with human resource staff that ethics training was not provided to vendor contractors.	Ethics training was not provided to vendor contractors. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
CE1.7	Employees and contractors are notified of any changes to the DCMS Policy Manual and are required to acknowledgment of receipt.	Selected a sample of employees to determine if acknowledgment of receipt of DCMS' Policy Manual changes had been completed.	No deviation noted.

		Contractors were not provided changes to the DCMS Policy Manual.	Contractors were not provided changes to the DCMS Policy Manual. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
CE1.8	An Employee Exit form and an ESR are completed to ensure remove of access and retrieval of equipment for employees and contractors.	Selected a sample of terminated employees to determine if an Exit form and ESR had been completed.	2 of 13 employees selected did not have an ESR completed.
		Selected a sample of terminated contractors to determine if an Exit form and ESR had been completed.	1 of 8 contractors selected did not have an Exit Form completed.
CE1.9	Performance evaluations are completed at the end of three months and the six months for employees serving a six months probationary period	Selected a sample of new employees to determine if applicable probationary evaluations had been completed.	7 of 25 employees selected did not have a probationary evaluation completed. 7 of 25 employees selected had probationary evaluations completed 16 to 82 days late.
CE1.10	Annually, employee evaluations are completed.	Selected a sample of employees to determine if an annual evaluation had been completed.	3 of 60 employees selected did not have an annual evaluation completed. 39 of 60 employees had an annual evaluation completed 1to 246 days late.
CE1.11	Annually, ethic training is provided to employees and contractors.	Selected a sample of employees to determine if annual ethics training had been completed.	No deviation noted.
		Collaboratively inquired with human resource staff that ethics training was not provided to vendor contractors.	Ethics training was not provided to vendor contractors. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

CE1.12	Effective January 1, 2018, annual cybersecurity training is provided to all State employees and contractors.	Selected a sample of employees to determine if annual cybersecurity training had been provided.	No deviation noted.
		Selected a sample of contractors to determine if annual cybersecurity training had been provided.	1 of 60 contractors selected had not completed cybersecurity training.
CE1.13	Prior to December 31, 2017, annual security awareness and ethics training was provided to all employees and contractors.	Selected a sample of employees to determine if security awareness and ethics training was provided.	No deviation noted.
		Selected a sample of employees and contractors to determine if security awareness and ethics training was provided.	1 of 60 contractors selected had not completed security awareness training.
CE1.14	Annually, employees and contractors acknowledge compliance with security policies.	Selected a sample of employees to determine if the annual acknowledgment of compliance with security policies was completed.	No deviation noted.
		Selected a sample of contractors to determine if the annual acknowledgment of compliance with security policies was completed.	2 of 39 contractors selected had not completed the annual acknowledgement of compliance with security policies.

Control Environment Objective: CE 1: Controls provide reasonable assurance that policies and procedures related to employee responsibilities and hiring have been established, new employees and contractors are screened and on-boarded, and that a defined organizational structure exist, that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF CENTRAL MANAGEMENT SERVICES	TESTS OF CONTROLS	RESULTS OF TESTS
	For the period July 1, 2017 to August 14, 2017		
CE1.15	The hiring practices adhere to legal requirements as published in the State Personnel Code, Personnel Rules, Union contracts, Rutan decisions, court orders and applicable state/federal laws.	Reviewed the hiring procedures, Personnel Code, Union Contract, and Rutan decisions to determine if a hiring process had been established .	No deviation noted.
	For the period July 1, 2017 to October 12, 2017		
CE1.16	New employee and contractors must pass a background check prior to being offered employment.	Selected a sample of new employees and contractors to determine if background checks were completed prior to being offered employment.	No deviation noted.
	For the period July 1, 2017 to October 16, 2017		
CE1.17	Newly-hired employees and contractors are provided the DCMS Policy Manual and are required to sign an acknowledgment form acknowledging responsibility to abide by the policies contained within the DCMS Policy Manual.	Selected a sample of new employees to determine if the Policy Manual Acknowledgement had been completed.	No deviation noted.
		Collaboratively inquired with human resource staff that contractors were not provided the DCMS Policy Manual and had not signed the acknowledgment form.	Contractors were not provided the DCMS Policy Manual and had not signed the acknowledgment form. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

CE1.18	Newly-hired employees and contractors are required to sign the acknowledgement included in the Security Awareness Training and Ethics Orientation acknowledging they have reviewed the materials and recognizes the responsibility to abide by the Security Awareness Training and Ethics Orientation for State Employees requirements.	Selected a sample of employees to determine if acknowledgment of receipt of DCMS Policy Manual changes had been completed.	No deviation noted.
		Collaboratively inquired with human resource staff that contractors were not provided changes to the DCMS Policy Manual.	Contractors were not provided changes to the DCMS Policy Manual. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
CE1.19	Department of Central Management Services provides the Department monthly reports documenting annual evaluations whish are due in the current month, upcoming in the next 2 months, and those that are overdue.	Selected a sample of monthly reports to determine if the reports provided documented the annual evaluations which were due in the current month, upcoming 2 months and overdue.	No deviation noted.

Control Objective: 1: Controls provide reasonable assurance that invalid transactions and errors that are relevant to user agencies internal control over financial reporting are identified, rejected, and correctly reentered into the application in a timely manner.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY	**TESTS OF CONTROLS**	**RESULTS OF TESTS**
	AIS, CIS, CPS, CTAS, eTime		
C1.1	The applications have edit features designed to reject erroneous or invalid data. When erroneous or invalid data is entered, an error message will appear on the screen and the field will be highlighted.	Selected a sample of field edits to determine if they were functioning appropriately and were providing error notifications.	No deviation noted.
	AIS, CIS, CPS, CTAS, eTime		
C1.2	Application user manuals are provided to user which provides guidance to assist users.	Reviewed user manuals to determine if they provided guidance to users.	No deviation noted.
	ERP		
C1.3	The ERP has edit features designed to reject erroneous or invalid data entered. When erroneous or invalid data is entered, an error message will appear.	Selected a sample of edits to determine if incorrect information was rejected and if a message appeared.	12 of 47 transactions codes selected were no longer utilized by the Department; however, they had not been deactivated. 1 of 13 logical edits selected allowed for duplicate asset tag numbers to be entered.
Complementary User Agency Controls			
1. Agencies are responsible for the complete and accurate entry and maintenance of data into the applications.			

Control Objective: 2: Controls provide reasonable assurance that appropriate federal, state and local specifications are used for tax calculations during processing, that are relevant to user entities’ internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY	TESTS OF CONTROLS	RESULTS OF TESTS
C2.1	Annually, the applicable federal tax rates are reviewed and updated within CPS.	Reviewed the federal tax rates to determine if the rates had been updated within CPS.	No deviation noted.
	Annually, the applicable states’ tax rates are reviewed and updated within CPS.	Reviewed the states' tax rates to determine if the rates had been updated within CPS.	19 of 43 States with income tax requirements were not included in the CPS tax tables. 3 of 24 States' (including Washington DC) tax rates were incorrect in the CPS tax tables. The State of Illinois tax rate was correct.
Complementary User Agency Controls			
1. Agencies are responsible for the reviewing the payroll voucher to ensure the accurate calculation of dedications.			

Control Objective: 3: Controls provide reasonable assurance that application programs and environment changes are properly authorized, tested, approved and implemented to result in complete, accurate, and timely processing and reporting that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY	TESTS OF CONTROLS	RESULTS OF TESTS
	Changes other than applications		
C3.1	The Department has established the Remedy Change Management Guide and the Change Management Policy over the change management process.	Reviewed the Change Management Policy and the Remedy Change Management Guide to determine if procedures were documented.	The Remedy Change Management Guide did not document the details that were to be included in Post Implementation Reviews. The Remedy Change Management Guide did not document the details to be included in the implementation, testing and backout plans. The Change Management Policy did not document the requirements for testing, evaluating and authorization prior to implementation.
C3.2	Changes are tracked, documented and approved in Remedy	Selected a sample of changes to determine if they were tracked, documented and approved in Remedy.	No deviation noted.
C3.3	Changes are approved based on their classification; high, medium and low.	Selected a sample of changes to determine if they were properly approved based on their classification.	No deviation noted.
C3.4	Test, backout and implement plans are required for high-impact changes prior to implementation.	Selected a sample of high impact changes to determine if test, backout and implementation plans were attached prior to implementation.	No deviation noted.

C3.5	Emergency Changes are reviewed at the weekly CAC meetings.	Selected a sample of emergency changes to determine if they were reviewed at the CAC meeting.	1 of 21 emergency changes selected was not reviewed and discussed at the weekly CAC meetings.
C3.6	Transparent Changes are reviewed monthly by the Enterprise Change Manager.	Inquired with the Department to determine if transparent changes are reviewed monthly by the Enterprise Change Manager.	The Enterprise Change Manager did not review transparent changes monthly.
	Application changes-AIS, CIS, CTAS, CPS, eTime		
C3.7	The Application Lifecycle Management Manual and the EAA Project Development Web Methodology document application change management procedures.	Reviewed the Manual and Methodology to determine if they documented the change management process.	The Manual did not provide guidance related to: -required approvals, testing and documentation requirements, -requirements for post implementation reviews, -emergency change requirements. The Methodology did not provide guidance related to: -prioritization of requests, -required approvals, testing and documentation requirements, -requirements for post implementation reviews.
C3.8	Application changes are tracked, documented and approved in Remedy.	Selected a sample of changes to determine if they were tracked and documented in Remedy.	No deviation noted.
C3.9	Upon completion of coding, user acceptance approval is obtained via email.	Collaboratively inquired with application staff that user acceptance approvals were not obtained for AIS, CIS, CTAS, and CPS changes.	User acceptance approvals were not obtained for AIS, CIS, CTAS, and CPS changes. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

		Selected a sample of eTime changes to determine if user acceptance approval was obtained.	No deviation noted.
C3.10	Prior to implementation into the mainframe production environment, a move sheet is approved by the EAA supervisor.	Selected a sample of changes to determine if the move sheet was completed and approved by the EAA supervisor prior to implementation.	No deviation noted.
C3.11	Moves to the mainframe production environment are completed by Library Services, based on instruction within the move sheet.	Selected a sample of changes to determine if Library Services completed the moves to the production environment.	No deviation noted.
C3.12	Library Services sends an email to the originating EAA supervisor and developer indicating the status of the move.	Selected a sample of changes to determine if Library Services sent an email documenting the status of the move.	No deviation noted.
C3.13	Prior to implementation for web applications, the EAA group supervisor approves the request for deployment into the production environment.	Selected a sample of change to determine if the EAA group supervisor approved the request for deployment.	No deviation noted.
C3.14	A developer, who did not code the change, moves the change into the production environment.	Selected a sample of changes to determine if a developer, who did not code the change, completed the move to the production environment.	No deviation noted.
	Application Changes - ERP		
C3.15	The Department has established the Illinois ACTS (ERP) Change Management Policy & Procedures to control changes to the ERP.	Reviewed the IL ACTS (ERP) Change Management Policy & Procedures to determine the change management process.	The IL ACTS (ERP) Change Management Policy & Procedures did not document or provide guidance for: -who was to approve transports to the quality region for the various types of defects, -the process for requesting access to

			transport to the production region and the associated review of the transport. The IL ACTS (ERP) Change Management Policy & Procedures did not document or provide guidance for: -who was to review the various requirements, -who was to approve the manpower estimates, -documentation and approvals related to the transport to the various regions.
	Defects		
C3.16	Technical Unit Testing is to be completed and reviewed by Production Support and maintained on Production Support's SharePoint.	Selected a sample of defects to determine if Technical Unit Testing had been completed, reviewed by Production Support and was maintained on Production Supports' SharePoint.	No deviation noted.
C3.17	Transport requests to the Quality Regions are to be requested and approved via HPQC.	Reviewed the IL ACTS (ERP) Change Management Policy & Procedures and inquired with ERP staff.	The IL ACTS (ERP) Change Management Policy & Procedures did not document who was to approve the defect transport to the Quality Regions. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
C3.18	Functional Unit testing is to be completed by Production Support and approved by the State's Functional Expert and maintained in HPQC.	Selected a sample of defects to determine if Functional Unit Testing had been completed, reviewed by the State's Functional Expert, and maintained in HPQC.	No deviation noted.
C3.19	Functional and security defect transports to the Production Region are to be requested and approved by a State Project Manager, via HPQC.	Selected a sample of defects to determine if transport to the Production Region were requested via HPQC and approved by a State Project Manager.	No deviation noted.

C3.20	Configuration defect transports are to be approved by a State Project Manager and review the Activity Log, via GRC.	Selected a sample of defects to determine if transports were approved by a State Project Manager and the associated activity log was reviewed, via GRC.	No deviation noted.
	Change Requests		
C3.21	A Change Request is to be completed, validated, reviewed and approved via the Department's SharePoint.	Reviewed the IL ACTS (ERP) Change Management Policy & Procedures and inquired with ERP staff.	The IL ACTS (ERP) Change Management Policy & Procedures did not document: -the information which was to be review reviewed by the Project Office, -who was to review the various requirements, -the information that was to be reviewed by the various parties. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
C3.22	Functional Specification Design document is to be developed by Production Support and approved by the State's Functional Expert.	Selected a sample of Change Requests to determine if the Functional Specification Design document was developed by Production Support and approved by the State's Functional Expert.	No deviation noted.
C3.23	Technical Specification Design document is to be developed and approved by Production Support.	Selected a sample of Change Requests to determine if the Technical Specification Design document was developed and approved by Production Support.	1 of 9 Change Requests selected did not have the Technical Specification Design document completed and approved.
C3.24	Technical Unit Testing is to be completed and reviewed by Production Support and maintained on Production Support's SharePoint.	Selected a sample of Change Requests to determine if Technical Unit Testing was completed and reviewed by Production Support and maintained on Production Support's SharePoint.	1 of 9 Change Requests selected did not have Technical Unit Testing completed and approved.

C3.25	Transport requests to the Quality Regions are to be requested and approved via HPQC.	Reviewed the IL ACTS (ERP) Change Management Policy & Procedures and inquired with ERP staff.	The IL ACTS (ERP) Change Management Policy & Procedures did not document who was to approve the transport to the quality region. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
C3.26	Functional Unit testing is to be completed by Production Support and approved by the State's Functional Expert and maintained in HPQC.	Selected a sample of Change Requests to determine if Functional Unit testing was completed by Production Support, approved by the State's Functional Expert and maintained in HPQC.	1 of 11 Change Requests selected did not have documentation of Functional Testing completed. 2 of 11 Change Requests selected did not have documentation of approval by the State’s Functional Expert.
C3.27	Change Request transports to the Production Region are to be requested and approved by a State Program Manager or the State's Project Manager, via HPQC.	Selected a sample of Change Requests to determine if transports to the Production were requested and approved by a State Program Manager or the State's Project Manager, via HPQC.	1 of 12 Change Requests did not contain approval for transport to the Production Region. 2 of 12 Change Requests did not have transport requests to the Production Region completed via HPQC; rather they were completed via email.
C3.28	The State Program Manager-Work Management receives and reviews weekly reports from Production Support detailing all the change activity for the week.	Selected a sample of weekly reports to determine if the State Project Manager-Work Management had received and reviewed them.	No deviation noted.
C3.29	The State Program Manager-Work Management and the Program Director receives and reviews monthly reports from Production Support documenting change activities, incident resolution, and SLA targets.	Selected a sample of monthly reports to determine if the State Program Manager-Work Management and the Program Director had received and reviewed them.	No deviation noted.

Complementary User Agency Controls
1. Agencies are responsible for submission of a Remedy ticket documenting issues and needs of the environment and applications.
2. Agencies are responsible for submission of a Change Request documenting issues and needs of the ERP.

Control Objective: 4: Controls provide reasonable assurance that agency calls that are relevant to user agencies' internal control over financial reporting are responded to, tracked and resolved in a timely manner.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY	TESTS OF CONTROLS	RESULTS OF TESTS
C4.1	The Incident Management Process Guide documents the remediation process of reported incidents.	Reviewed the Incident Management Process Guide to determine if it documented the remediation process of reported incidents.	No deviation noted.
C4.2	Reported incidents are tracked via a Remedy ticket until appropriate remediation efforts are completed.	Reviewed Remedy to determine if incidents are tracked until remediation efforts are completed.	No deviation noted.
C4.3	The MORT Initiation Procedures document the procedures for MORTS.	Reviewed the MORT Initiation Procedures to determine if it documented the MORT process.	The Procedures did not address the after-hours processes.
C4.4	Reported MORTS are tracked via a Remedy ticket until appropriate remediation efforts are completed.	Selected a sample of MORTS to determine if they are tracked in Remedy until remediation efforts are completed.	The Department did not provide a complete and accurate population of MORTS. However, for the MORTS we were able to identify no deviation was noted.
C4.5	The Missing IT Equipment Procedures provide guidance on missing and stolen equipment.	Reviewed the Missing IT Equipment Procedures to determine if it documented guidance on missing and stolen equipment.	The Procedures did not address the process in the event encryption was not installed.
C4.6	Missing or stolen equipment is tracked via a Remedy ticket.	Selected a sample of missing/stolen equipment to determine if a Remedy ticket had been created.	No deviation noted.
C4.7	A police report is attached to the Remedy ticket for stolen equipment.	Selected a sample of stolen equipment to determine if a police report was attached to the Remedy ticket.	No deviation noted.

C4.8	Verification is completed to ensure encryption had been installed on stolen equipment.	Selected a sample of stolen equipment to determine if encryption had been installed.	No deviation noted.
C4.9	If encryption was not installed on stolen equipment, the Security Operations Center will enact a breach investigation.	Collaboratively inquired with the IT Service Desk staff.	The Department did not report any unencrypted equipment stolen or missing. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
Complementary User Agency Controls			
1. Agencies are responsible for reporting unplanned interruptions to the IT Service Desk.			
2. Agencies are responsible for reporting lost or stolen equipment to the IT Service Desk.			

Control Objective: 5: Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY	**TESTS OF CONTROLS**	**RESULTS OF TESTS**
	Access Provisioning-Environment		
C5.1	The Department has developed several policies and procedures governing logical security over access to the environment.	Reviewed the policies and procedures to determine if they addressed logical security controls.	The policies did not address: -the requirements for requesting, obtaining and modifying access rights, -periodic review of access rights, -revocation of access rights.
C5.2	Access to the environment requires an ESR authorized by the agency IT Coordinator.	Selected a sample of new hires to determine if an ESR was authorized by an agency IT Coordinator.	3 of 74 new hires selected did not have an ESR completed authorizing access to the environment.
C5.3	Prior to December 12, 2017, to obtain a mainframe security software ID, an approved Mainframe Security Request Form was required.	Selected a sample of new hires to determine if an approved Mainframe Security Request Form was completed.	1 of 74 new hires selected did not have a Mainframe Access Request Form completed.
	After December 12, 2017, to obtain a mainframe security software ID, an ESR is required.	Selected a sample of new hires to determine if an ESR was completed.	3 of 74 new hires selected did not have an ESR completed.
C5.4	For modifications to access rights or equipment, an agency IT Coordinator is to submit an approved ESR.	The Department was unable to provide a universe of modification to access rights.	The Department was unable to provide a universe of modification to access rights. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

C5.5	Upon termination, an agency IT Coordinator is to submit an ESR documenting the access rights to be terminated and the equipment to be collected.	Selected a sample of terminated employees/contractors to determine if access was timely terminated and equipment collected.	13 of 28 terminated employees/contractors selected had ESRs submitted between 2 and 248 days after their termination date.
			17 of 54 terminated employees/contractors selected did not have an ESR completed.
	Access Provisioning-Applications		
C5.6	Agency IT Coordinators are to submit an approved ESR for the establishment of an agency Application Administrator (AIS, CIS, CPS, CTAS).	Collaboratively inquired with application staff.	The Department did not receive a request (ESR) to establish an AIS and CIS agency Application Administrator. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
		Reviewed the CPS and CTAS agencies Application Administrators established to determine if an ESR was approved by the agencies IT Coordinator.	No deviation noted.
C5.7	Agency Human Resource Directors are to submit an approved ESR for the establishment of an agency eTime Administrator.	Reviewed the agencies eTime Administrators established to determine if an ESR was approved by the agencies HR Director.	The Department did not provide a complete and accurate population of eTime Administrator requests (ESR). The one request (ESR) we were able to identify was not properly approved by the agency's Human Resource Director.
C5.8	ERP security reviews access request to ensure no segregation of duties conflict exist prior to approving.	Selected a sample of ERP access request to ensure segregation of duties conflicts were reviewed.	The Department did not document the security review process for agencies that are transitioning to the ERP for the first time.
C5.9	Annually, the ERP security team provides agencies with the User Access Report for review of their users and associated rights.	Reviewed documentation to determine if the User Access Report was reviewed annually.	No deviation noted.

	Password Resets		
C5.10	To reset AD accounts a user may use the self service options; FIM or DIM, or contact the IT Service Desk. Users who contact the IT Service Desk are required to provide three pieces of information in order to verify their ID.	Reviewed the ID Management Website to determine solutions to reset passwords.	No deviation noted.
		Observed the IT Service Desk staff to determine if an individual's ID was verified.	No deviation noted.
C5.11	To reset a security software account, a user is to utilize the self-service option; DIM, or contact the IT Service Desk. Users who contact the IT Service Desk are required to provide three pieces of information in order to verify their ID.	Reviewed the ID Management Website to determine solutions to reset passwords.	No deviation noted.
		Observed the IT Service Desk staff to determine if an individual's ID was verified.	No deviation noted.
C5.12	To reset Novell accounts, a user is to contact the IT Service Desk. Users are required to provide the IT Service Desk information in order to verify their ID.	Observed the IT Service Desk staff to determine if an individual's ID was verified.	No deviation noted.
C5.13	To reset a SAP password, users are to contact Production Support, via the IT Service Desk, and provide their name, agency, ID and contact phone number.	Observed Production Support staff to determine if the user provided their name, agency, contact number in order to reset their password.	No deviation noted.
C5.14	Once the SAP password is reset, a temporary password is emailed to the email addressed associated with the user ID.	Observed an email was sent with a temporary password.	No deviation noted.

	Mainframe Security		
C5.15	To access the mainframe environment, the security software requires an established ID and password.	Observed a security software ID and password was required to access the mainframe environment.	No deviation noted.
C5.16	Security software profiles define the level of access.	Selected a sample of security software profiles to determine if the profile defined the level of access.	No deviation noted.
C5.17	Security software passwords are maintained in an encrypted database.	Reviewed the systems options to determine if security software passwords were maintained in an encrypted database.	No deviation noted.
C5.18	Password security parameters have been established and configured to ensure access to mainframe resources is appropriate: - Minimum password length; - Password complexity; - Password history; - Minimum password age; and - Number of invalid login attempts.	Reviewed system options to determine if password standards had been established.	No deviation noted.
C5.19	Annually, the Security Software Administrator sends the proxy agencies a listing of security software IDs assigned to their agency for review.	Reviewed annual report to the proxy agencies to determine if the report had been sent to the proxy agencies.	No deviation noted.
C5.20	Monthly, the Security Software Administrator runs a report documenting IDs that have not been utilized in the past 90-days upon which are disabled.	Selected a sample of monthly reports to determine if the IDs had been disabled.	No deviation noted.
C5.21	The Security Software Administrator runs a weekly violation report which is reviewed for invalid and unauthorized access attempts. The Security Software	Selected a sample of weekly reports to determine if the Security Software Administrator had reviewed and followed up on violations.	No deviation noted.

	Administrator contacts the individual or their supervisor to determine the reason for the violation.		
C5.22	Bi-monthly (every other month), the Security Software Administrator receives a separation report. If a separation is noted, the Security Software Administrator will revoke the individual's security software ID.	Inquired with the Security Software Administrator and selected a sample of semi-monthly (twice per month) reports to determine if the Security Software Administrator had reviewed and revoked individual accounts which had separated.	The Security Software Administrator received the separation report on a semi-monthly basis; instead of bi-monthly. 1of 8 semi-monthly separation reports selected had not been reviewed.
	Midrange Security		
C5.23	To access the midrange environment a user requires an ID and password.	Observed that an Active Directory ID and password was required to access the environment.	No deviation noted.
C5.24	Password security parameters have been established and configured to ensure access to midrange resources is appropriate: - Minimum password length; - Password complexity; - Password history; - Minimum password age; and - Number of invalid login attempts.	Reviewed password parameters to determine if parameters had been established and configured.	No deviation noted.
C5.25	Beginning in January 2018, the Department performs a monthly review of all Illinois.gov Active Directory accounts and disable accounts which have been dormant for 90 days or more.	Selected a sample of monthly reviews to determine if dormant accounts were reviewed.	No deviation noted.
	System Administrators-Mainframe		
C5.26	Access to the mainframe operating system configurations is limited to system support	Reviewed access rights to the mainframe operating system configurations to determine if	No deviation noted.

	staff; system programmers and security software personnel.	access was limited to system support staff.	
C5.27	Access with powerful privileges, high-level access and access to sensitive system functions is restricted to authorized personnel.	Reviewed access with powerful privileges, high-level access and sensitive system function to determine they were restricted to authorized personnel.	No deviation noted.
C5.28	On an annual basis the Security Software Coordinator conducts a review of security software IDs with powerful privileges.	Inquired with the Security Software Coordinator.	The Department was unable to provide documentation that the annual review of security software IDs was conducted. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
	System Administrators-Midrange		
C5.29	Access to administer the midrange environment is limited to authorized technical support personnel.	Reviewed the midrange environment administrators to determine if their access was appropriate.	No deviation noted.
C5.30	Annually, the Wintel Admin Team conducts a review of the technical accounts to ensure appropriateness.	Reviewed documentation of the annual review to determine if technical accounts were reviewed.	No deviation noted.
	Application Administrators/Programmers-AIS, CIS, CTAS, CPS, eTime		
C5.31	Access to application source code, JCL streams, data files and sensitive application functions are restricted to authorized personnel.	Reviewed administrator access to source code, JCL streams, data files and sensitive application functions to determine if appropriate.	No deviation noted.
	Firefighter IDs-ERP		
C5.32	Access to a Firefighter ID requires a request via GRC and a need statement. The ERP security team will review, approve and	Observed ERP security team receive a request for Firefighter ID to determine if it was reviewed, approved, and an email was submitted.	No deviation noted.

	submit an email to the requestor stating access has been approved.		
	Network		
C5.33	Mandatory backbone design and configuration standards and guides are defined and maintained.	Reviewed backbone design, configuration standards, and guides to determine if they were defined and maintained.	No deviation noted.
C5.34	Redundancy between pop-sites where technically, fiscally, and operationally feasible and has also installed fiber optic wave transmission technologies to selected sections of the managed backbone.	Reviewed pop-site configurations to determine if they have been configured for redundancy.	No deviation noted.
C5.35	Network diagrams depict common connectivity configurations.	Reviewed network diagrams to determine connectivity configurations.	No deviation noted.
C5.36	VPNs provide controlled and trusted connections between devices.	Reviewed VPN configurations to determine if security settings were configured to allow for secure remote connections.	No deviation noted.
C5.37	The Department’s Enterprise VPN Standard provides guidance when establishing a virtual private network connection.	Reviewed Enterprise VPN Standards to determine if they provide guidance on VPN connections.	No deviation noted.
C5.38	When data travels across a public network, it is encrypted at the access router and while in transit across the public network until it reaches the distribution router and enters the private network.	Reviewed configurations to determine if data traversing the network is encrypted.	No deviation noted.
C5.39	A security banner is displayed at the initial network connection warning of prosecution for unauthorized access.	Selected a sample of configurations to determine if a security banner is displayed upon initial connection to the network.	2 of 138 devices selected were not configured to display a security banner.

C5.40	Modification to the network is restricted to Department authorized technicians and authorized vendors.	Selected a sample of individuals with the authority to modify the network to determine if they were authorized.	No deviation noted.
C5.41	Access Control Lists reside on the network device itself and restricts communication to only certain IP addresses or address ranges.	Selected a sample of configurations to determine if ACLs restricted communications.	No deviation noted.
C5.42	Authentication Servers control access through assignment of access right privileges based on defined group profiles.	Selected a sample of configurations to determine if Authentication Servers controlled access.	No deviation noted.
C5.43	Authentication Servers record failed login attempts to the network equipment which are processed by the Network Operations Center.	Selected a sample of configurations to determine if failed login attempts are logged and processed by Network Operations Center.	No deviation noted.
C5.44	A backbone health-check assessment is conducted monthly by reviewing statistics and threshold metrics.	Reviewed the monthly statistics and metric records spreadsheet to determine if the statistics and metrics are recorded and reviewed monthly.	No deviation noted.
C5.45	Self-monitoring network hardware devices are encoded with filters that automatically generate system entries when an industry or Department defined parameter or condition occurs. Network Operation Center staff review and engage operation teams for resolution.	Selected a sample of hardware devices to determine if they are encoded with filters and if Network Operations Center are reviewing and resolving occurring issues.	No deviation noted.
C5.46	Network software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization and generates an email or console display alert when a predefined event occurs or a threshold is reached. Network Operations Center follows-up on these alerts.	Reviewed software configurations to determine if emails and alerts were sent when predefined events or thresholds were reached and that Network Operations followup on the alerts.	No deviation noted.

Complementary User Agency Controls

Access Provisioning-Environment

1. Agency IT Coordinators are responsible for the submission of an approved ESR for the creation of a user access.
2. Agency IT Coordinators are responsible for the submission of an approved ESR for modification of user access.
3. Agency IT Coordinators are responsible for the submission of an approved ESR for the termination of user access.
4. Agencies are responsible for the submission of an approved ESR for the creation of a security software account.

Access Provisioning-Applications (AIS, CIS, CTAS, CPS, eTime)

5. Agency IT Coordinators are responsible for the submission of an approved ESR for the establishment of the agency Application Administrator.
6. Agency Human Resources Director is responsible for the submission of an approved ESR for the establishment of an eTime Administrator.
7. Agency Application Administrator is responsible for the management of their agencies application accounts; assignment, modification and deactivation of rights.
8. Agencies are responsible for ensuring proper segregation of duties in the assignment of application user access rights.
9. Agencies are responsible for reviewing their user’s access rights.
10. Agencies are responsible for notifying the Department in changes to Agency Application Administrators.

Access Provisioning-ERP

11. Authorized agency staff are responsible for entry of an access request into GRC and first level of approval.
12. Agencies are responsible for ensuring proper segregation of duties.

13. Agencies are responsible for notifying the Department in changes to Agency Application Administrators.

Password Resets

14. Agency Application Administrators are responsible for resetting their user accounts.
15. Agencies are responsible for notifying the Department in changes to Agency Application Administrators.
16. Agencies are responsible for contacting the IT Service Desk or the utilization of FIM or DIM in order to reset the AD, Novell, or ERP accounts.

Mainframe

17. Proxy agencies are responsible for reviewing the appropriateness of their agencies security software accounts and responding to the Security Software Coordinator.
18. Agencies are responsible for monitoring and reviewing their security software accounts assigned to them.

Midrange

19. Agencies are responsible for reviewing AD accounts that have been dormant for 90 or more days and determining their need.

Control Objective: 6: Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and deviation, problems, and errors are identified, tracked, recorded and resolved in a complete and timely manner that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY	TESTS OF CONTROLS	RESULTS OF TESTS
C6.1	The Operations Center utilizes software and the Automated Operations Console in order to continuously monitor the environment.	Observed the Automated Operations Console to determine if it monitored the environment.	No deviation noted.
C6.2	Problems, issues, and incidents are recorded via the Daily Shift Reports and a Remedy ticket is created.	Selected a sample of Daily Shift Reports to determine if problems, issues and incidents were recorded and if a Remedy ticket was created.	No deviation noted.
C6.3	The Daily Shift Report documents the activity conducted on all mainframe production systems and incident calls received at the Operations Center and reviewed by ISD management and supervisors.	Selected a sample of Daily Shift Reports to determine if they documented activity conducted on the mainframe production environment and recorded incident calls received.	No deviation noted.
C6.4	The Operator Shift Change Checklist is completed at the beginning of each shift and reviewed by the Operations Center supervisor.	Selected a sample of the Operator Shift Change Checklist to determine if they were completed at the beginning of each shift and reviewed by the Operations Center supervisor.	No deviation noted.
C6.5	The Data Processing Guide has been established in order to provide staff with instruction related to their various tasks.	Reviewed the Data Processing Guide to determine if it provided instructions.	No deviation noted.
	Mainframe Environment		
C6.6	The mainframe environment is continuously monitored via z/OS systems console by the Operation Center staff.	Observed the z/OS system console to determine if the Operations Center staff were continuously monitoring.	No deviation noted.

C6.7	Remote Monitoring Facility is run weekly and monthly.	Interviewed staff and selected a sample of Resource Measurement Facility Reports to determine if they were ran monthly.	The Department did not run Remote Monitoring Facility is run weekly and monthly. The Department only runs Resource Measurement Facility Reports on a monthly basis. No deviation noted with the review of monthly Resource Measurement Facility Reports.
C6.8	Mainframe performance and capacity monitoring is documented via internal memorandum distributed monthly to management.	Interviewed staff regarding the memorandums to determine if they documented performance and capacity monitoring.	No deviation noted.
	Midrange Environment		
C6.9	The midrange environment availability and performance is monitored via What's Up Gold (WUG).	Observed WUG to determine if availability and performance was monitored.	No deviation noted.
C6.10	Proactive performance and capacity monitoring is performed for the midrange environment utilizing What's Up Gold and Microsoft's System Center, which sends alerts to the Operations Center when certain performance and capacity loads meet or exceed set thresholds. Email notifications are also sent to the responsible team group technician who reviews and takes corrective action.	Observed WUG and Microsoft's System Center to determine if performance and monitoring was performed and if email alerts were sent to the Operations Center.	No deviation noted.
C6.11	The Command Center monitors SQL Database servers/software via WUG, Microsoft SQL Utilities, and Idera tools. The Command Center contacts the staff assigned to the server experiencing the	Observed WUG, Microsoft SQL Utilities and Idera tool to determine if SQL servers were monitored and if the Command Center contacts the applicable staff for remediation.	No deviation noted.

	outages for remediation.		
C6.12	The WinTel SQL support staff receives alerts via Idera and Microsoft SQL if outages are noted on the SQL Database servers/software.	Observed Idera and Microsoft SQL to determine if email alerts were sent if an outage on the SQL Database servers or software occurred.	No deviation noted.
	Data Storage		
C6.13	The Data Storage Technicians monitor data storage performance and capacity via EMC Toolsets.	Observed EMC Toolsets to determine if data storage performance and capacity was monitored.	No deviation noted.
C6.14	Automated alerts are sent to the Data Storage Technicians and management when capacity is reached or exceeds 80%.	Observed EMC Toolsets to determine if email alerts were sent when capacity reached 80%.	No deviation noted.
	Security Operations Center		
C6.15	A myriad of tools are utilized by the Security Operations Center to continuously monitor the network.	Observed tools utilized by the Security Operations Center to continuously monitor the network.	No deviation noted.
C6.16	The Security Operations Center has established Standard Operating Procedures.	Reviewed the Standard Operating Procedures to determine if they provided guidance on detection, analysis and resolution.	No deviation noted.
C6.17	An Incident Report is completed for incidents that are classified as medium or high and are reviewed by the Chief Information Security Officer.	Selected a sample of medium and high incidents to determine if an Incident Report was completed.	No deviation noted.
		Inquired with the Chief Information Security Officer.	The Department did not maintain documentation of the Chief Information Security Officer review of the Incident Reports. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

C6.18	The daily Shift Change Report is completed at the end of each shift documenting information regarding incidents the next shift should be aware of.	Selected a sample of daily Shift Change Reports to determine if incidents were recorded.	From July 2017 to February 2018, daily Shift Change Reports were not completed. After February 2018, no deviation noted.
C6.19	The weekly Activity Report, summarizing the week’s incidents and resolution, is provided to management for review.	Selected a sample of weekly Activity Reports to determine if incidents and their resolutions were recorded and reviewed by management.	No deviation noted.
C6.20	Monthly, quarterly, bi-annually and annually Metric Reports, documenting statistics on incidents, are provided to management for review.	Selected a sample of monthly Metrics Reports to determine if incident statistics were documented and reviewed by management.	No deviation noted.
		Selected a sample of quarterly Metric Reports to determine if incident statistics were documented and reviewed by management.	No deviation noted.
		Selected a sample of bi-annual Metric Reports to determine if incident statistics were documented and reviewed by management.	No deviation noted.
		Inquired with the Security Operations staff.	The annual Metric Report had not been completed. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

<u>Control Objective: 7:</u> Controls provide reasonable assurance that the transmission of data between the Department and agencies are from authorized sources and are complete, accurate, secure and timely that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION AND& TECHNOLOGY	**TESTS OF CONTROLS**	**RESULTS OF TESTS**
C7.1	MOVEit File Transfer Protocol and SFTP transmissions are used to transmit data between the Department and the agencies.	Interviewed staff to determine file transfer protocols.	The Department utilized MOVEit secure file transfer software which resided on a SFTP server. The Department utilized FTPS for mainframe data transmissions.
C7.2	Errors that occur on data file transmission with MOVEit and SFTP systems result in an automated notification being sent to the Production Control Team for resolution.	Interviewed staff to determine the process for reporting and recording of errors.	In the event of a MOVEit error, the applicable agency was notified; not the Production Control Team.
C7.3	The errors are recorded in the Shift Change Checklist and a Remedy ticket is created in order to track the error to resolution.	Interviewed staff to determine the process for reporting and recording of errors.	MOVEit errors were not recorded in the Shift Change Checklist. A Remedy ticket was opened when an agency contacted the IT Service Desk for assistance.
C7.4	Access to MOVEit and SFTP systems are reviewed on an annual basis by the Department.	Interviewed staff to determine if an annual review of access to MOVEit and SFTP was conducted.	The Department had not conducted an annual review.

<u>Control Objective: 8:</u> Controls provide reasonable assurance that the environment is configured as authorized in order to support application controls and to protect data from unauthorized changes that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY	**TESTS OF CONTROLS**	**RESULTS OF TESTS**
	Mainframe		
C 8.1	System options have been implemented in order to protect resources and data.	Reviewed system options report to determine if security options were implemented.	No deviation noted.
C8.2	System Management Facility records the operating system activity, which are reviewed weekly by the manager of Mainframe Software Support.	Inquired with the Mainframe Software Support manager.	The Department could not provide documentation of the weekly reviews of System Management Facility records. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
	Midrange		
C 8.3	Anti-virus definitions and updates are pushed out daily.	Reviewed antivirus compliance report to determine if definitions and updates were up to date.	Of the 37,088 laptops and desktops connected to services on May 24, 2018, 551 were not up-to-date with the latest anti-virus product.
C8.4	Tools monitor the equipment to determine what equipment is out of compliance regarding antivirus definitions.	Observed tools utilized for antivirus protection.	No deviation noted.
		Reviewed antivirus compliance reports to determine if devices were monitored.	Of the 37,088 laptops and desktops connected to services on May 24, 2018, 3,692 were not up-to-date with the latest anti-virus definitions.
C8.5	Windows patches are pushed out and monitored through SCCM.	Reviewed SCCM report to determine if Window patches were pushed out and being monitored.	No deviation noted.

Control Objective: 9: Controls provide reasonable assurance that applications, data and the environment is backed up and stored offsite that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY	TESTS OF CONTROLS	RESULTS OF TESTS
	Mainframe		
C 9.1	Data on mainframe systems are backed up daily and weekly utilizing Virtual Tape Technology (Disk Library Management (DLM)).	Selected a sample of daily and weekly mainframe backup schedules to determine if backups were performed daily and weekly.	No deviation noted.
C 9.2	The Department utilizes CA Scheduler to schedule and verify the completion of the backups.	Selected a sample of CA Scheduler Reports to determine if mainframe backups were scheduled and the completion was verified.	No deviation noted.
C 9.3	The Department has implemented backup policies to that assist staff in the event of failed backups.	Reviewed policies to determine if they provided guidance in the event of failed backups.	No deviation noted.
C 9.4	Daily, Storage staff review the output of the daily backup jobs for any failures, correct the issues and resubmits the backup job.	Selected a sample of daily backup job output to determine if the failed backup jobs were reviewed and resubmitted.	No deviation noted.
C 9.5	In the event of a mainframe daily backup failure, Operations Center staff records the incident in the Shift Report.	Collaboratively inquired with the Operations Center staff.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
C 9.6	The Storage personnel review the output of the weekly backup jobs for success or	Selected a sample of weekly backup job reports to determine if there were reviewed and failed backup	No deviation noted.

	failure. The failure is researched and corrected, and then the failed portion of the backup job is resubmitted for completion.	jobs were resubmitted.	
C 9.7	Mainframe data replication occurs every 10 minutes between the CCF and the ADC DLM. The monitoring software sends the Enterprise Storage and Backup group an alert if the data is out of sync for more than 8 hours.	Observed the DLM configurations to determine if replication occurred every 10 minutes and that an alert was sent if the data was out of sync for more than 8 hours.	No deviation noted.
C 9.8	If there is an issue, a Remedy ticket is opened in order to track the Enterprise Storage and Backup group’s progress on resolution of the issue.	Collaboratively inquired with the Storage and Backup staff.	The Department did not encounter any issues during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
C 9.9	The DLM Replicated Status log keeps a log of replication between the two DLMs and tracks library replication outcomes for DLM replication activity.	Observed the DLM replication log to determine if the replication activity was recorded and tracked the replication outcomes.	No deviation noted.
	Midrange		
C9.10	Spectrun Protect and Avamar are used to backup the midrange environment.	Observed the Spectrun Protect and Avamar to determine if they were used to backup the midrange environment.	No deviation noted.
C 9.11	Data Protection Advisor is used to monitor and report on midrange backups.	Observed Data Protection Advisor to determine if it monitored and reported on midrange backups.	No deviation noted.
C 9.12	Midrange server backups are performed daily or weekly and are either incremental or full.	Observed server backup schedules to determine if they were performed daily or weekly and were either incremental or full backups.	No deviation noted.

C 9.13	Spectrum Protect and Data Protection Advisor generate daily reports indicating the backup status of all scheduled jobs from the prior day and emails to the Enterprise Storage and Backup group for resolution.	Observed Spectrum Protect and Data Protection Advisor to determine if they were configured to send daily reports of the backup status for all scheduled jobs.	No deviation noted.
C 9.14	Backed up server data is written to a Data Domain storage system and then replicated to another Data Domain storage system at the ADC.	Observed the replication of the Data Domain storage system to determine if it was replicated to the ADC.	No deviation noted.
C 9.15	The Data Domain storage system generates a daily status report and alerts which are emailed to the Enterprise Storage and Backup groups for review and resolution.	Observed the Data Domain to determine if it was configured to send daily reports of the replication status for all scheduled jobs.	No deviation noted.
C 9.16	The Data Domain storage system alerts the support vendor in the event of hardware to system failures.	Observed the configuration of the Data Domain storage system to determine if alerts were sent to the support vendor.	No deviation noted.
C 9.17	Database backups are written to the Data Domain storage system and then replicated to the ADC.	Observed the replication of the Data Domain storage system to determine if it was replicated to the ADC.	No deviation noted.
C9.18	The SQL team receives a daily report documenting the latest backups and their status.	Selected a sample of daily reports to determine if the status of backups was documented.	No deviation noted.
C9.19	SQL servers send alerts to the SQL team when a backup job fails.	Observed the SQL servers to determine if alerts were enabled.	No deviation noted.
C9.20	The Idera monitoring software sends automatic alerts to the SQL team when a database backup has been missed.	Observed the Idera monitoring software to determine if automatic alerts were enabled.	No deviation noted.

C 9.21	Any data, including, but not limited to SQL, Access, DB2 databases, user shared documents and user profiles are located on the Isilon storage device.	Observed the configuration of the Isilon storage device to determine the data stored.	No deviation noted.
C 9.22	The Enterprise Storage and Backup group has policies on the Isilon that take daily snapshots of all shares which are then retained for 60 days.	Observed the Isilon storage device configurations to determine if daily snapshots were taken and maintained for 60 days.	No deviation noted.
C 9.23	The Isilon also has daily synchronization with the ADC to another Isilon storage system.	Observed the Isilon storage device configurations to determine if it was replicated to the ADC.	No deviation noted.
C 9.24	The Isilon generates a daily report showing all successful and failed synchronization attempts with the ADC.	Observed the Isilon storage device to determine if it was configured to send daily reports with the status of replication jobs to the Storage group.	No deviation noted.
C 9.25	Enterprise Storage and Backup group investigate failed synchronization attempts until a satisfactory conclusion is reached.	Reviewed process documentation to determine if the Storage group investigated failed synchronization attempts.	No deviation noted.
C 9.26	The Isilon has a call home feature that will notify vendor support and the Enterprise Storage and Backup group during any disc or hardware failure.	Observed the Isilon configurations to determine if the call home feature was active.	The Isilon call home feature notified the vendor, not the Enterprise Storage and Backup group.
Complementary User Agency Controls			
1. Agencies are responsible for scheduling of their mainframe backups.			

<u>Control Objective: 10:</u> Controls provide reasonable assurance that physical access to facilities and resources is restricted to authorized individuals and environmental controls are in place to protected equipment and facilities that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY	**TESTS OF CONTROLS**	**RESULTS OF TESTS**
	Prior to April 1, 2018		
	Communication Building		
C 10.1	Human Resources submit an approved ID Badge Request Form or an email to DCMS for the creation of an ID Badge.	Selected a sample of new employees and contractors to determine if an approved ID Badge Request Form or an email was received prior to the creation of an ID Badge.	1 of 60 new employees and contractors selected access was not properly approved.
	CCF		
C 10.2	Infrastructure Service Management team submits an approved ID Badge Request Form or an email to DCMS for the creation of the ID Badge.	Selected a sample of new employees and contractors to determine if an approved ID Badge Request Form or an email was received prior to the creation of an ID Badge.	No deviation noted.
	April 1, 2018 through June 30, 2018		
	Communication Building		
C10.3	Human Resources obtain approval from the employee or contractors supervisor for the creation of the ID Badge.	Selected a sample of new employees and contractors to determine if approval was received prior to the creation of an ID Badge.	No deviation noted.
	CCF		
C10.4	The Assistant Chief of Enterprise Infrastructure and Manager of Enterprise Production Operations submits an approved ID Badge Request Form or an email to the Department's Human Resources for the creation of the ID Badge.	Selected a sample of new employees and contractors to determine if an approved ID Badge Request Form or an email was received prior to the creation of an ID Badge.	No deviation noted.

Control Objective: 10: Controls provide reasonable assurance that physical access to facilities and resources is restricted to authorized individuals and environmental controls are in place to protected equipment and facilities that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT OF CENTRAL MANAGEMENT SERVICES	TESTS OF CONTROLS	RESULTS OF TESTS
C10.5	In order to gain access to the facilities, an individual must have and ID Badge with associated rights.	Observed an ID Badge, with associated rights, was required to gain access to the CCF and the Communication Building.	No deviation noted.
C10.6	The Velocity Access Control system documents/logs the date, time and doors in which an individual enters.	Observed the Velocity Access Control system to determine if it documented the date, time and door an individual enters.	No deviation noted.
	Prior to April 1, 2018		
	Communication Building		
C10.7	An approved ID Badge Request Form or an email from the Department's Human Resources must be received documenting the rights to be provided prior to the creation of an ID Badge.	Selected a sample of new employees and contractors to determine if an approved ID Badge Request Form or an email was received from the Department's Human Resources prior to the creation of an ID Badge.	1 of 60 new employees and contractors selected access was not properly approved.
C10.8	An individual must present a valid driver's license or State ID Card in order to obtain the ID Badge.	Observed an individual was to present a valid driver's license or State ID Card in order to obtain an ID Badge.	A current State employee may present their State employment ID, instead of their driver's license or State ID Card.
	CCF-Employees		
C10.9	An approved ID Badge Request Form or an email from the Department's Infrastructure Services must be received documenting the rights to be provided prior to the creation of an ID Badge.	Selected a sample of new employees to determine if an approved ID Badge Request Form or an email was received from the Department's Infrastructure Services prior to the creation of an ID Badge.	No deviation noted.

C10.10	An individual must present a valid driver’s license or State ID Card in order to obtain the ID Badge.	Observed an individual was to present a valid driver's license or State ID Card in order to obtain an ID Badge.	A current State employee may present their State employment ID, instead of their driver's license or State ID Card.
	CCF-Contractor		
C10.11	An approved ID Badge Request Form or an email from the Department’s Infrastructure Services must be received documenting the rights to be provided prior to the creation of an access right within Velocity.	Selected a sample of new contractors to determine if an approved ID Badge Request Form or an email was received from the Department's Infrastructure Services prior to the creation of access rights within Velocity.	No deviation noted.
C10.12	Contractors are provided a temporary access badge with access rights based on access documented within Velocity.	Observed contractors were provided temporary badges with rights as documented in Velocity.	No deviation noted.
C10.13	Upon entry into the CCF, contactors are to present their driver’s license or State ID and sign-in in order to receive a temporary badge.	Observed contractors were to present their driver's license or State ID and sign-in in order to receive a temporary badge.	Contractors were provided badges with access rights, except contractors under the Department of Central Management Services control. These contractors were to present their driver's license or State ID and sign-in in order to receive a temporary badge.
	Separations		
C10.14	Upon receipt of notification from the Department’s Human Resources, access rights will be terminated effective their date of termination.	Selected a sample of terminated employees and contractors to determine if their access had been terminated on their date of termination.	9 of 50 terminated employees and contractors selected did not have their access terminated on their date of termination.
	CCF and Communication Building-Visitors		
C10.15	At entry, a visitor must present a driver’s license or State ID card and sign the	Observed visitors were to present a driver's license or a State ID and sign the Visitor Register in order	No deviation noted.

	Visitor Register in order to a Visitor ID Badge.	to obtain a Visitors Badge.	
C10.16	The security guard will enter the visitor's information into Velocity and provide a Visitor Badge, which does not have access rights.	Observed the entry of visitor information into Velocity.	No deviation noted.
		Observed the operation of the visitor badge to determine if access to the CCF and Communication Building was not permitted.	No deviation noted.
C10.17	Visitors are required to be escorted at all times by an employee.	Observed visitors being escorted by employees.	No deviation noted.
	Security Guards		
C10.18	The CCF and the Communication Building are monitored 24x7x365 by security guards.	Reviewed security guard contract to determine their duties at the CCF and Communication Building.	No deviation noted.
		Observed security guards at the CCF and Communication Building.	No deviation noted.
C10.19	The security guards have post order (operating procedures) for each facility.	Reviewed the post orders for each facility to determine if they provided guidance.	No deviation noted.
C10.20	The security guards complete daily activity reports and incident reports as needed.	Selected a sample of daily activity reports to determine if they had been completed.	7 of 40 daily activity reports selected could not be located.
		The Department could not provide a population of incident reports.	The Department could not provide a population of incident reports. Therefore, the Service Auditor could not test the effectiveness of the control.
C10.21	Department of Central Management Services receives monthly summaries of the daily activity reports and incident reports.	Selected a sample of monthly summaries of the daily activity reports and incident reports to determine if the Department of Central Management Services had received them.	No deviation noted.

C10.22	Security alarms have been installed at various locations throughout both facilities, which are monitored by the security guards.	Observed location of security alarms to determine if the CCF and Communication Building had been alarmed.	No deviation noted.
		Observed alarm notifications to determine if they were monitored by the security guards.	No deviation noted.
C10.23	Digital cameras have been installed throughout both facilities and are monitored by the security guards.	Observed the locations of the video surveillance cameras to determine if they were monitoring the CCF and Communication Building.	No deviation noted.
		Observed the video feeds to determine if they were monitored by the security guards.	No deviation noted.
C10.24	Fire extinguishers, fire suppression, sprinkler system, water detection, cooling/heating systems, UPS, and generators have been installed at one or both facilities.	Observed the measures in place to protect against environmental factors at the CCF and Communication Building.	No deviation noted.
C10.25	Preventive maintenance agreements for the environmental measures have been entered into.	Reviewed the maintenance agreements to determine if preventative maintenance agreements were in place.	The water detection system was maintained by the Department of Central Management Services, rather than contracted. The Department did not have a maintenance contract in place for the generator located at the CCF. The maintenance contract for the Communication Building generator expired on January 31, 2018. The Department did not maintain a maintenance contract for the Communication Building UPS.

SECTION V

OTHER INFORMATION PROVIDED BY THE DEPARTMENT OF INNOVATION & TECHNOLOGY AND THE DEPARTMENT OF CENTRAL MANAGEMENT SERVICES

Department of Innovation & Technology and the Department of Central Management Service

Corrective Action Plan
(Not Examined)

Below is the Department of Innovation & Technology and the Department of Central Management Services corrective action plan related to the deviations noted within the Report.

Description of System (DOS) did not include:	**Department of Innovation & Technology's Corrective Action Plan.**
Complementary subservice organization controls.	The Department of Innovation & Technology will include complimentary subservice organization controls in the FY19 DOS.
Information regarding the configuration standards and installation requirements.	The Department of Innovation & Technology will update the FY 19 DOS to reflect the configuration standards and installation requirements.
The secondary mainframe operating system, NOMAD.	The Department of Innovation & Technology will correct and update the FY 19 DOS to reflect the statement accurately to prevent the exception.
All interfaces and protocols available to user agencies to transmit data.	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
The process for the termination of physical access.	The Department of Innovation & Technology will review and document the process for termination of physical access.
Inaccurate Statements in the Description of System	
The IT Risk Assessment Policy is located on the website.	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
The Department did not provide sufficient appropriate evidence to determine the accuracy of the statement, risks from potential and newly discovered vulnerabilities are assessed through interaction with security experts and vendor subscription services. The Department also contracts with vendors to receive patch vulnerability information at the earliest possible time.	The Department of Innovation & Technology will review the FY19 DOS, and ensure that there is sufficient evidentiary documentation to support the asserted process, and risks are adequately assessed with related supporting documentation. The Department of Innovation & Technology will also maintain, review and remediate as necessary patch vulnerability information as received.

Description of System did not include:	**Department of Central Management Services' Corrective Action Plan.**
The process for physical access provision for vendor contractors.	The Department of Central Management Services will add the process in the description of system in the next fiscal year.

Control No.	**Department of Innovation & Technology's Corrective Action Plan.**
CE1.3	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
CE1.5	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
CE1.6	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement. The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.
CE1.7	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
CE1.8	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.
CE1.9	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence. The Department of Innovation & Technology will also review process and procedures to strengthen the controls to detect and prevent from future occurrence.
CE1.10	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.
CE1.11	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
CE1.12	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.
CE1.13	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.
CE1.14	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.
C1.3	The ERP Program will perform a review of all transaction codes that have not been used. This exception, which only occurred in a very specific scenario, was corrected as part of the 7/1/18 go live for Cluster 2.
C2.1	The Department of Innovation & Technology has corrected the affected employee tax tables for the current year. The Department of Innovation &

	Technology will review all state tax rates, correct them as needed, and implement a process to ensure the rates are updated.
C3.1	The Department of Innovation & Technology will continue to review and make recommendations for updating Department of Innovation & Technology's policies in its ongoing Policy Workgroup meetings and will add these specific concerns to the agenda for discussion. The Department Innovation & Technology will also review process and procedures to strengthen the controls to detect and prevent from future occurrence.
C3.5	The Department of Innovation & Technology will review the process and modify the process accordingly to ensure that all emergency changes are addressed at weekly CAC meeting.
C3.6	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.
C3.7	The Department of Innovation & Technology will continue to review and make recommendations for updating the Application Change Control procedures and policies. This work is already in progress.
C3.9	The Department of Innovation & Technology will update the FY 19 DOS to better represent the Change Control Approval process. In addition, the Department of Innovation & Technology will update the procedures to better implement user acceptance sign-off best practice.
C3.15	The ERP Program will review and enhance its Change Management Policies and Procedures to ensure all steps in the process are clearly described and add any controls, if needed, to ensure none of the steps are overlooked.
C3.17	The ERP Program will review and enhance its Change Management Policies and Procedures to ensure all steps in the process are clearly described and add any controls, if needed, to ensure none of the steps are overlooked.
C3.21	The ERP Program will review and enhance its Change Management Policies and Procedures to ensure all steps in the process are clearly described and add any controls, if needed, to ensure none of the steps are overlooked.
C3.23	The ERP Program will review and enhance its Change Management Policies and Procedures to ensure all steps in the process are clearly described and add any controls, if needed, to ensure none of the steps are overlooked.
C3.24	The ERP Program will review and enhance its Change Management Policies and Procedures to ensure all steps in the process are clearly described and add any controls, if needed, to ensure none of the steps are overlooked.
C3.25	The ERP Program will review and enhance its Change Management Policies and Procedures to ensure all steps in the process are clearly described and add any controls, if needed, to ensure none of the steps are overlooked.
C3.26	The ERP Program will review and enhance its Change Management Policies and Procedures to ensure all steps in the process are clearly described and add any controls, if needed, to ensure none of the steps are overlooked.
C3.27	The ERP Program will review and enhance its Change Management Policies and Procedures to ensure all steps in the process are clearly described and add any controls, if needed, to ensure none of the steps are overlooked.

C4.3	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
C4.4	The Department of Innovation & Technology will review the process and procedures to strengthen the controls to detect and prevent from future occurrence.
C4.5	The Department of Innovation & Technology has corrected this exception by updating the procedure. This will prevent this exception from future occurrence.
C5.1	The Department of Innovation & Technology will continue to review and make recommendations for updating Department of Innovation & Technology's policies in its ongoing Policy Workgroup meetings and will add these specific concerns to the agenda for discussion.
C5.2	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.
C5.3	The Department of Innovation & Technology will further review process and procedures to strengthen the controls to detect and prevent from future occurrence.
C5.4	The Department of Innovation & Technology will review the process and procedures to strengthen the controls to detect and prevent from future occurrence.
C5.5	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.
C5.7	The Department of Innovation & Technology will review the process and procedures to strengthen the controls to detect and prevent from future occurrence. Additionally, the Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
C5.8	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
C5.22	The Department of Innovation & Technology will update the FY 19 DOS to reflect the correct frequency of the control.
C5.28	The Department of Innovation & Technology will ensure that reviews are documented. The Department of Innovation & Technology will ensure that the separation reports are reviewed.
C5.39	The Department of Innovation & Technology has corrected this exception by configuring the device. The Department of Innovation & Technology will further review process and procedures to strengthen the controls to detect and prevent from future occurrence.
C6.7	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
C6.17	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.

C6.18	The Department of Innovation & Technology left out that the NOC was integrated only in Feb 2018 from the DOS and has provided Shift reports after the integration. This will prevent this exception from future occurrence.
C7.1	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
C7.2	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
C7.3	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
C7.4	The Department of Innovation & Technology will ensure that an annual access review of MoveIt and SFTP is completed and results documented.
C8.2	The Department of Innovation & Technology will review the process and procedures so that the reviews are documented to prevent this exception from future occurrence.
C8.3	The Department of Innovation & Technology will develop and implement a process to ensure that the latest product or version is applied as soon as possible upon notification or discovery of the new version or product.
C8.4	The Department of Innovation & Technology will develop and implement a process to ensure that the latest product or version is applied as soon as possible upon notification or discovery of the new version or product.
C9.26	The Department of Innovation & Technology will update the FY 19 DOS to reflect the corrected statement.
C10.1	The Department of Innovation & Technology will review process and procedures to strengthen the controls to detect and prevent from future occurrence.
	Department of Central Management Services' Corrective Action Plan
CE1.17	The Department of Central Management Services will change the description of system in the next fiscal year.
CE1.18	The Department of Central Management Services will change the description of system in the next fiscal year.
C10.7	This was an isolated incident and it will be fixed in the future.
C10.8	The Department of Central Management Services will change the description of system in the next fiscal year.
C10.10	The Department of Central Management Services will change the description of system in the next fiscal year.
C10.13	The Department of Central Management Services will change the description of system in the next fiscal year.
C10.14	The Department of Central Management Services will update the FY19 DOS to reflect the correct statement and identified information that was accidentally omitted.

C10.20	The Department of Central Management Services will continue to work with the contract vendor to ensure that the deliverables under the contract are available including daily activity reports.
C10.25	The Department of Central Management Services will review process and procedures to strengthen the controls to detect and prevent from further occurrence. The Department of Central Management Services' BOSS is continuing to work on establishing a new contract that will cover the generators for the Communication Building. Until the new contract is in place for use, the Department of Central Management Services will use the $100,000 small purchase threshold for procurement to cover any needed work on this system. Additionally, the Department of Central Management Services will update the FY 19 DOS to reflect the corrected statement and identified information that was accidentally omitted.

Department of Innovation & Technology
Business Continuity and Disaster Recovery
(Not Examined)

Illinois continuously strategizes and benchmarks against commercial, federal, state and local organizations, ensuring the application of best in class processes. Partnered with Illinois Emergency Management Agency (IEMA)/University of IL to develop a National Institute of Standards and Technology (NIST) based Cybersecurity framework and metrics to measure and ensure continuous improvement. Business impact analyses performed to establish a clear understanding of Illinois critical business processes ensuring recovery priorities, Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO) aligned with critical business. Risk assessments measure maturity of each control and alignment of policy and processes to NIST controls to minimize risk. Illinois continuously maintains and updates recovery, backup, retention, data classification, network resources, data encryption, breach notification, facilities access and wireless devices. Resiliency and Recovery Methodology, as well as Recovery Activation Plans including Network, Customer Services, Incidents and Major Outages, outline response steps. Disaster Recovery (DR) testing includes tabletop, proof of concept, and real-life exercises to educate and learn about procedures, policies, best practices, recovery plans, contracts, communications strategies, key personnel, and feasibility. Application personnel restore data and information systems and verify admin/end-user transactions. July – November 2017 testing involved a full recovery scenario of an entire State agency and recreated all aspects from critical infrastructure down to the desktop and applications. October 2017 testing, which included 10 agencies and 23 mainframe applications, show recoverability to alternate site mainframe and support subsystems (IMS, DB2, AD, DNS/DHCP servers, storage management). The Springfield Data Center is tested annually for commercial power outage resiliency. Identified systems, sub-systems, application libraries, and user data are backed up locally and replicated to the virtual tape storage system at the Alternate Data Center.

Illinois utilizes the Illinois Century Network (ICN) to serve as an Illinois local area network enabling interconnectivity, resource sharing, and access to instate content and cloud resources with 365/24/7 support. Resources are available from the IEMA and Emergency Management Assistance Compact (EMAC) to support an enterprise-wide disaster. The mainframe infrastructure at the Alternate Data Center has ample recovery resources. DR plans are published to SharePoint for ease of access and provide clearly defined notification pathways and document test results. An Enterprise Architecture Taxonomy database includes application classification information and attributes such as RTO, prioritized recovery order, confidential data indications, Governing standards (HIPAA, IRS Pub 1075, PII, etc.). Annual InfoSec Awareness Training is systemized and deployed across all agencies under the Governor.

Department of Innovation & Technology
ERP Disaster Recovery
(Not Examined)

ERP Disaster Recovery by Virtustream

The Department has contracted with Virtustream to host the ERP. The Department has created a Disaster Recovery plan and background to help keep this process simple and focused. The annual DR plan is initiated by the Department's ERP Team through communication with it's customer and hosting provider Virtustream. As part of the process the Virtustream team assigns a Project Manager (PM) to the DR test to manage the entire process. The Department's ERP Team creates a Change Request internally and a SR (Service Request) externally at Virtustream to document the DR test project and overall activity. The Virtustream Project Manager initiates planning meetings for the DR test with the Department's ERP Team. Once planning is completed the Department's ERP Team and Virtustream teams initiates the DR test alongside the Department's networking team to execute DR action items. Throughout the DR test the Department, alongside with the Virtustream Project Manager record all activities that occur during the test. Once the test is complete and approved by the Department, the Department's ERP Team and Virtustream team complete and sign off that all testing criteria has been met. In the case where DR testing criteria is not met, Virtustream will create an SR for incidents that will need to be remedied.

In April 2018, the Department's ERP Team worked with Virtustream to conduct a successful test of the disaster recovery plan and activities.

Listing of User Agencies of the Department of Innovation & Technology’s Information Technology Shared Services System (Not Examined)

1. Abraham Lincoln Presidential Library and Museum
2. Capital Development Board
3. Chicago State University
4. Commission on Government Forecasting and Accountability
5. Court of Claims
6. Criminal Justice Information Authority
7. Department of Agriculture
8. Department of Central Management Services
9. Department of Children and Family Services
10. Department of Commerce & Economic Opportunity
11. Department of Corrections
12. Department of Employment Security
13. Department of Financial & Professional Regulation
14. Department of Healthcare and Family Services
15. Department of Human Rights
16. Department of Human Services
17. Department of Innovation and Technology
18. Department of Insurance
19. Department of Juvenile Justice
20. Department of Labor
21. Department of Lottery
22. Department of Military Affairs
23. Department of Natural Resources
24. Department of Public Health
25. Department of Revenue
26. Department of Transportation
27. Department of Veterans' Affairs
28. Department on Aging
29. Eastern Illinois University
30. Emergency Management Agency
31. Environmental Protection Agency
32. Executive Ethics Commission
33. General Assembly Retirement System
34. Governor's Office of Management and Budget
35. Governor's State University
36. Guardianship and Advocacy Commission
37. House of Representatives

38 Human Rights Commission
39 Illinois Arts Council
40 Illinois Board of Higher Education
41 Illinois Civil Service Commission
42 Illinois Commerce Commission
43 Illinois Community College Board
44 Illinois Council on Developmental Disabilities
45 Illinois Deaf and Hard of Hearing Commission
46 Illinois Educational Labor Relations Board
47 Illinois Housing Development Authority
48 Illinois Gaming Board
49 Illinois Independent Tax Tribunal
50 Illinois Labor Relations Board
51 Illinois Law Enforcement Training and Standards Board
52 Illinois Math and Science Academy
53 Illinois Medical District Commission
54 Illinois Power Agency
55 Illinois Prisoner Review Board
56 Illinois Procurement Policy Board
57 Illinois Racing Board
58 Illinois State Board of Investments
59 Illinois State Police
60 Illinois State Toll Highway Authority
61 Illinois State University
62 Illinois Student Assistance Commission
63 Illinois Workers' Compensation Commission
64 Joint Committee on Administrative Rules
65 Judges' Retirement System
66 Judicial Inquiry Board
67 Legislative Audit Commission
68 Legislative Ethics Commission
69 Legislative Information System
70 Legislative Inspector General
71 Legislative Printing Unit
72 Legislative Reference Bureau
73 Legislative Research Unit
74 Northeastern Illinois University
75 Northern Illinois University
76 Office of the Architect of the Capitol
77 Office of the Attorney General
78 Office of the Auditor General

79 Office of the Comptroller
80 Office of the Executive Inspector General
81 Office of the Governor
82 Office of the Lieutenant Governor
83 Office of the State Appellate Defender
84 Office of the State Fire Marshal
85 Office of the State's Attorneys Appellate Prosecutor
86 Office of the Treasurer
87 Property Tax Appeal Board
88 Secretary of State
89 Senate Operations
90 Sex Offender Management Board
91 Southern Illinois University
92 State Board of Education
93 State Board of Elections
94 State Employees' Retirement System
95 State of Illinois Comprehensive Health Insurance Board
96 State Police Merit Board
97 State Universities Civil Service System
98 State University Retirement System
99 Supreme Court Historic Preservation Commission
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. Criminal Justice Information Authority
2. Department of Agriculture
3. Department of Central Management Services
4. Department of Corrections
5. Department of Financial & Professional Regulation
6. Department of Human Rights
7. Department of Innovation & Technology
8. Department of Insurance
9. Department of Juvenile Justice
10. Department of Labor
11. Department of Lottery
12. Department of Military Affairs
13. Department of Natural Resources
14. Department of Public Health
15. Department on Aging
16. General Assembly Retirement System
17. Guardianship and Advocacy Commission
18. Human Rights Commission
19. Illinois Arts Council
20. Illinois Board of Higher Education
21. Illinois Community College Board
22. Illinois Council on Developmental Disabilities
23. Illinois Deaf and Hard of Hearing Commission
24. Illinois Educational Labor Relations Board
25. Illinois Gaming Board
26. Illinois Labor Relations Board
27. Illinois Law Enforcement Training and Standards Board
28. Illinois Prisoner Review Board
29. Illinois Racing Board
30. Illinois State Police
31. Illinois Student Assistance Commission
32. Illinois Workers' Compensation Commission
33. Judges' Retirement System
34. Judicial Inquiry Board
35. Office of the Attorney General
36. Office of the Auditor General
37. Office of the Executive Inspector General
38. Office of the State Appellate Defender

39 Office of the State Fire Marshal
40 Office of the State's Attorneys Appellate Prosecutor
41 Property Tax Appeal Board
42 Sex Offender Management Board
43 State Board of Elections
44 State Employees' Retirement System
45 State Police Merit Board
46 State Universities Civil Service System
47 Supreme Court of Illinois

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

1. Capital Development Board *
2. Criminal Justice Information Authority
3. Department of Agriculture
4. Department of Central Management Services
5. Department of Corrections
6. Department of Employment Security *
7. Department of Financial & Professional Regulation
8. Department of Human Rights
9. Department of Innovation & Technology
10. Department of Juvenile Justice
11. Department of Lottery
12. Department of Military Affairs
13. Department of Natural Resources (Historic Preservation)
14. Department of Public Health
15. Department of Transportation
16. Department of Veterans' Affairs
17. Department on Aging
18. Environmental Protection Agency *
19. Governor's Office of Management and Budget
20. Illinois Deaf and Hard of Hearing Commission
21. Illinois Educational Labor Relations Board
22. Illinois Law Enforcement Training and Standards Board
23. Illinois Prisoner Review Board
24. Office of the Attorney General
25. Office of the Governor *
26. Office of the Lieutenant Governor *
27. Office of the State's Attorneys Appellate Prosecutor

*****Although the agency has transitioned to the ERP, data remains within CIS.

Listing of User Agencies of the Central Payroll System (Not Examined)

1 Abraham Lincoln Presidential Library and Museum
2 Capital Development Board
3 Commission on Government Forecasting and Accountability
4 Court of Claims
5 Criminal Justice Information Authority
6 Department of Agriculture
7 Department of Central Management Services
8 Department of Children and Family Services
9 Department of Commerce & Economic Opportunity
10 Department of Financial & Professional Regulation
11 Department of Healthcare and Family Services
12 Department of Human Rights
13 Department of Human Services
14 Department of Innovation & Technology
15 Department of Insurance
16 Department of Labor
17 Department of Lottery
18 Department of Military Affairs
19 Department of Natural Resources
20 Department of Public Health
21 Department of Revenue
22 Department on Aging
23 Emergency Management Agency
24 Environmental Protection Agency
25 Executive Ethics Commission
26 Governor's Office of Management and Budget
27 Guardianship and Advocacy Commission
28 House of Representatives
29 Human Rights Commission
30 Illinois Arts Council
31 Illinois Board of Higher Education
32 Illinois Civil Service Commission
33 Illinois Commerce Commission
34 Illinois Community College Board
35 Illinois Council on Developmental Disabilities
36 Illinois Deaf and Hard of Hearing Commission
37 Illinois Educational Labor Relations Board
38 Illinois Gaming Board
39 Illinois Independent Tax Tribunal

40 Illinois Labor Relations Board
41 Illinois Law Enforcement Training and Standards Board
42 Illinois Math and Science Academy
43 Illinois Power Agency
44 Illinois Prisoner Review Board
45 Illinois Procurement Policy Board
46 Illinois Racing Board
47 Illinois State Board of Investments
48 Illinois State Police
49 Illinois Student Assistance Commission
50 Illinois Workers' Compensation Commission
51 Joint Committee on Administrative Rules
52 Judges' Retirement System
53 Judicial Inquiry Board
54 Legislative Audit Commission
55 Legislative Ethics Commission
56 Legislative Information System
57 Legislative Printing Unit
58 Legislative Reference Bureau
59 Legislative Research Unit
60 Office of the Architect of the Capitol
61 Office of the Attorney General
62 Office of the Auditor General
63 Office of the Executive Inspector General
64 Office of the Governor
65 Office of the Lieutenant Governor
66 Office of the State Appellate Defender
67 Office of the State Fire Marshal
68 Office of the State's Attorneys Appellate Prosecutor
69 Office of the Treasurer
70 Property Tax Appeal Board
71 Senate Operations
72 Sex Offender Management Board
73 State Board of Education
74 State Board of Elections
75 State Employees' Retirement System
76 State of Illinois Comprehensive Health Insurance Board
77 State Police Merit Board
78 State Universities Civil Service System
79 Supreme Court Historic Preservation Commission
80 Teachers' Retirement System of the State of Illinois

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

1 Abraham Lincoln Presidential Library and Museum
2 Capital Development Board
3 Criminal Justice Information Authority
4 Department of Agriculture
5 Department of Central Management Services
6 Department of Commerce & Economic Opportunity
7 Department of Financial & Professional Regulation
8 Department of Human Rights
9 Department of Innovation & Technology
10 Department of Insurance
11 Department of Labor
12 Department of Lottery
13 Department of Natural Resources (Historic Preservation)
14 Department of Public Health
15 Department of Revenue
16 Department on Aging
17 Emergency Management Agency
18 Environmental Protection Agency
19 Executive Ethics Commission
20 Guardianship and Advocacy Commission
21 Human Rights Commission
22 Illinois Civil Service Commission
23 Illinois Council on Developmental Disabilities
24 Illinois Deaf and Hard of Hearing Commission
25 Illinois Educational Labor Relations Board
26 Illinois Gaming Board
27 Illinois Labor Relations Board
28 Illinois Law Enforcement Training and Standards Board
29 Illinois Prisoner Review Board
30 Illinois Procurement Policy Board
31 Illinois Racing Board
32 Illinois State Police
33 Illinois Workers' Compensation Commission
34 Judges' Retirement System
35 Office of the Attorney General
36 Office of the Executive Inspector General
37 Office of the State Fire Marshal
38 Property Tax Appeal Board

39 State Board of Elections
40 State Employees' Retirement System
41 State of Illinois Comprehensive Health Insurance Board

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

1. Abraham Lincoln Presidential Library and Museum
2. Capital Development Board
3. Criminal Justice Information Authority
4. Department of Agriculture
5. Department of Central Management Services
6. Department of Commerce & Economic Opportunity
7. Department of Financial & Professional Regulation
8. Department of Human Rights
9. Department of Innovation & Technology
10. Department of Insurance
11. Department of Labor
12. Department of Lottery
13. Department of Public Health
14. Department of Revenue
15. Department on Aging
16. Emergency Management Agency
17. Executive Ethics Commission
18. Guardianship and Advocacy Commission
19. Illinois Deaf and Hard of Hearing Commission
20. Illinois Gaming Board
21. Illinois Labor Relations Board
22. Illinois Prisoner Review Board
23. Illinois Procurement Policy Board
24. Illinois Racing Board
25. Illinois State Police
26. Illinois Workers' Compensation Commission
27. Office of the Executive Inspector General
28. Property Tax Appeal Board
29. State Employees' Retirement System
30. State of Illinois Comprehensive Health Insurance Board

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

1 Abraham Lincoln Presidential Library and Museum
2 Capital Development Board
3 Illinois Civil Service Commission
4 Department of Children and Family Services
5 Department of Employment Security
6 Department of Human Services-Mabley
7 Department of Natural Resources (Historic Preservation)
8 Department of Revenue
9 Department of Veterans' Affairs
10 Emergency Management Agency
11 Environmental Protection Agency
12 Executive Ethics Commission
13 Governor's Office of Management and Budget
14 Illinois Council on Developmental Disabilities
15 Illinois Independent Tax Tribunal
16 Illinois Procurement Policy Board
17 Office of the Governor
18 Office of the Lieutenant Governor

Listing of Security Software Proxy Agencies
(Not Examined)

1 Abraham Lincoln Presidential Library and Museum
2 Capital Development Board
3 Chicago State University
4 Commission on Government Forecasting and Accountability
5 Court of Claims
6 Criminal Justice Information Authority
7 Department of Agriculture
8 Department of Central Management Services
9 Department of Corrections
10 Department of Human Rights
11 Department of Labor
12 Department of Military Affairs
13 Department of Veterans Affairs
14 Eastern Illinois University
15 Emergency Management Agency
16 Executive Ethics Commission
17 Governor State University
18 Governor's Office of Management and Budget
19 Guardianship and Advocacy Commission
20 House of Representatives
21 Human Rights Commission
22 Illinois Arts Council
23 Illinois Civil Service Commission
24 Illinois Commerce Commission
25 Illinois Community College Board
26 Illinois Council on Developmental Disabilities
27 Illinois Deaf and Hard of Hearing Commission
28 Illinois Educational Labor Relations Board
29 Illinois Housing Development Authority
30 Illinois Independent Tax Tribunal
31 Illinois Labor Relations Board
32 Illinois Law Enforcement Training and Standards Board
33 Illinois Math and Science Academy
34 Illinois Medical District Commission
35 Illinois Power Agency
36 Illinois Prisoner Review Board
37 Illinois Procurement Policy Board
38 Illinois State Board of Investments

39 Illinois State Toll Highway Authority
40 Illinois State University
41 Joint Committee on Administrative Rules
42 Judicial Inquiry Board
43 Legislative Audit Commission
44 Legislative Ethics Commission
45 Legislative Information System
46 Legislative Inspector General
47 Legislative Printing Unit
48 Legislative Reference Bureau
49 Legislative Research Unit
50 Northeastern Illinois University
51 Northern Illinois University
52 Office of the Architect of the Capitol
53 Office of the Attorney General
54 Office of the Comptroller
55 Office of the Executive Inspector General
56 Office of the Governor
57 Office of the Lieutenant Governors
58 Office of the State Appellate Defender
59 Office of the State Fire Marshal
60 Office of the State's Attorneys Appellate Prosecutor
61 Office of the Treasurer
62 Property Tax Appeal Board
63 Secretary of State
64 Senate Operations
65 Southern Illinois University
66 State Board of Education
67 State Board of Elections
68 State of Illinois Comprehensive Health Insurance Board
69 State Police Merit Board
70 State University Civil Service System
71 State University Retirement System
72 University of Illinois
73 Western Illinois University

ACRONYM GLOSSARY

ACL – Access Control List
ACTS – Accountability Credibility Transparency Sustainability
AD – Active Directory
ADC – Alternate Data Center
AICPA – American Institute of Certified Public Accountants
AIS – Accounting Information System
AIX – Advanced Interactive eXecutive
ALS – Auto Liability System
AR – Accounts Receivable
ARPS – Accounts Receivable Posting System
BCCS – Bureau of Communications and Computer Services
CAC – Change Advisory Committee
CCF – Central Computer Facility
CICS – Customer Information Control System
CIO – Chief Information Officer
CIS – Central Inventory System
CISO – Chief Information Security Officer
CMOS – Complementary Metal Oxide Semiconductor
CMS – Central Management Services
CPS – Central Payroll System
CR – Change Request
CRIS – Comprehensives Rate Information System
CTAS – Central Time and Attendance
DB2 – Database 2
DC – District of Columbia
DCMS – Department of Central Management Services
Department – Department of Innovation and Technology
DHCP – Dynamic Host Configuration Protocol
DIM – DoIT Id Management
DLM – Disk Library Management
DNR – Department of Natural Resources
DNS – Domain Name Service
DoIT – Department of Innovation and Technology
DOS-Description of System
DR – Disaster Recovery
EAA – Enterprise Application & Architecture
ECC – ERP Central Component
EDP – Electronic Data Processing
EEO – Equal Employment Opportunity

EMAC – Emergency Management Assistance Compact
ERP – Enterprise Resource Planning
ESR – Enterprise Service Request
ESXi – Elastic Sky X Integrated
FBI – Federal Bureau of Investigation
FEIN – Federal Employer Identification Number
FIM – Forefront Id Management Solution
FMLA – Family and Medical Leave Act
FSD – Functional Specification Design
FTPS – File Transfer Protocol Secure
FUT – Functional Unit Testing
GAAP – Generally Accepted Accounting Principles
GRC – Governance, Risk, and Compliance
GUI – Graphical User Interface
HIPAA – Health Insurance Portability and Accountability Act
HPQC – Hewitt Packard Quality Control
HR – Human Resources
ICN – Illinois Century Network
ID – Identification
IDOR – Illinois Department of Revenue
IEMA – Illinois Emergency Management Agency
IGPS – Inter-Governmental Procurement System
ILCS – Illinois Compiled Statutes
IMS – Information Management System
IOC – Illinois Office of the Comptroller
IP – Internet Protocol
IRS – Internal Revenue Service
ISD – Infrastructure Services Division
IT – Information Technology
JCL – Job Control Language
JE – Journal Entry
LLC – Limited Liability Company
MORT – Major Outage Response Team
MS-ISAC – Multi-State Information Sharing and Analysis Center
NIST – National Institute of Standards and Technology
OS – Operating System
PAR – Personnel Action Request
PII – Personally Identifiable Information
PIR – Post Implementation Review
PM – Project Manager

PSC – Personal Service Contractor
PSC&D – Public Sector Collection & Disbursements
RDT – Receipts Deposit Transmittal
RFC – Request for Change
RMF – Remote Measurement Facility
RPO – Recovery Point Objective
RTO – Recovery Time Objective
SaaS – Software as a Service
SAMS – Statewide Accounting Management System
SAP – Systems, Applications and Products
SCCM – System Center Configuration Manager
SOC – Service Organization Control
SOD – Segregation of Duties
SFTP – Secure File Transfer Protocol
SLA – Service Level Agreement
SMF – System Management Facility
SR – Service Request
SRM – Supplier Relationship Management
SSN – Social Security Number
SQL – Structured Query Language
TSD – Technical Specification Design
TUT – Technical Unit Testing
UPS – Uninterruptible Power Supply
VPN – Virtual Private Network
WUG – What's Up Gold
z/OS – Zero Downtime Operating System
z/VM – Zero Downtime Virtual Machine