STATE OF ILLINOIS

OFFICE OF THE AUDITOR GENERAL

SERVICE ORGANIZATION CONTROL REPORT

DEPARTMENT OF INNOVATION & TECHNOLOGY

For the Year Ended June 30, 2019

FRANK J. MAUTINO

AUDITOR GENERAL

You can obtain reports by contacting:

Office of the Auditor General
Iles Park Plaza
740 E. Ash
Springfield, IL 62703

217-782-6046 or TTY: 1-888-261-2887

OR

This Audit Report and a Report Digest are also available on the worldwide web at
http://www.auditor.illinois.gov

STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY

REPORT ON THE DESCRIPTION OF SYSTEM, SUITABILITY OF DESIGN, AND OPERATING EFFECTIVENESS OF CONTROLS FOR THE PERIOD JULY 1, 2018, THROUGH JUNE 30, 2019

STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY

TABLE OF CONTENTS

Section I

Section II

Section III

SECTION I

INDEPENDENT SERVICE 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 and Technology's description of its information technology general controls and application controls that support its Information Technology Shared Services System of which are included in the "Description of the IT General Controls and Application Controls for the Department of Innovation and Technology's Information Technology Shared Services System" for the user agencies throughout the period from July 1, 2018, through June 30, 2019, (description) and the suitability of the design and operating effectiveness of the State of Illinois, Department of Innovation and Technology 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 and Technology's Assertion.

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 and Technology's controls are suitably 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 State of Illinois, Department of Innovation and Technology uses the Department of Central Management Services, a subservice organization to provide building maintenance activities, 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, Virtustream, Inc., a subservice organization to provide cloud hosting services for the State's Enterprise Resource Planning (ERP) system, and NICUSA, Inc., a subservice organization to provide Software as a Service. The description includes only the control objectives and related controls of the State of Illinois, Department of Innovation and Technology and excludes the control objectives and related controls of the Department of Central Management Services, Zayo Group, LLC, Microsoft, LLC, BMC Software, Inc., Virtustream, Inc., and NICUSA, Inc.

The information about the corrective action plan, business continuity and disaster recovery, ERP disaster recovery, storage loss/mainframe outage, and user agency listings in Section V, "Other Information Provided by the State of Illinois, Department of Innovation and Technology," is presented by management of the State of Illinois, Department of Innovation and Technology to provide additional information and is not part of the State of Illinois, Department of Innovation and Technology description of the Information Technology Shared Services System made available to user agencies during the period from July 1, 2018, to June 30, 2019. Information about the State of Illinois, Department of Innovation and Technology's corrective action plan, business continuity and disaster recovery, ERP disaster recovery, storage loss/mainframe outage, 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 and Technology has provided an assertion 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 and Technology is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, 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 assertion, 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 of the United States 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 from July 1, 2018, to June 30, 2019. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our adverse 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; and
- evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service 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 its information technology general control system. 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.

Basis for adverse opinion

Our examination disclosed:

1) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System included the utilization of subservice providers. However, the State of Illinois, Department of Innovation and 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.

2) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System did not include controls to comply with the Complementary User Entity Controls documented in the subservice providers' System and Organizational Control Reports. 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.

3) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System did not include monitoring controls related to the services provided by the State of Illinois, Department of Central Management Services. 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.

4) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System did not include the controls over the maintenance and patching of the mainframe operating systems. 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.

5) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System did not include application changes (AIS, CIS, CTAS, CPS, eTime) that follow the controls documented in the Application Lifecycle Management Manual. 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.

6) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System did not document the lack of developed polices or procedures dictating the process for employees to obtain physical access to facilities. 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.

7) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System did not include the process for individuals, other than Department employees, to obtain physical access to Department facilities. 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.

8) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System did not include the process for reviewing physical access to Department facilities and highly secured areas. 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.

9) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the SQL team

received an alert for missed backups. However, the State of Illinois, Department of Innovation and Technology did not include in their description the frequency of missed backups prior to the SQL team receiving an alert. Because no criteria have been established for the frequency, these statements are not relevant to user entities' internal control over financial reporting and are not measurable within the scope of this examination.

10) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated monitoring details were discussed at internal meetings. However, the State of Illinois, Department of Innovation and Technology did not include in their description the frequency in which the internal meetings were held. Because no criteria have been established for the frequency, these statements are not relevant to user entities' internal control over financial reporting and are not measurable within the scope of this examination.

11) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated risks from potential and newly discovered vulnerabilities are assessed through interaction with security experts and vendor subscription services. The State of Illinois, Department of Innovation and Technology did not provide sufficient appropriate evidence to determine the accuracy of the statement. As a result, we were unable to determine its accuracy.

12) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated prior to March 2, 2019, vulnerability scans were scheduled monthly; after March 2, 2019, scans were scheduled weekly. Our testing determined the vulnerability scans were run semi-monthly for February 2019.

13) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the ERP Production Support initiated all communications, including incidents. Additionally, Release Management, including descriptions of any releases, is sent to the agencies from the same dedicated email address. Our testing determined the ERP Production Support did not initiate communication through the dedicated email address.

14) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated on July 1, 2017, the Illinois Tollway was added as a user agency. Our testing determine the Illinois Tollway was added as a user agency on July 1, 2018.

15) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated Department services and performance statistics were previously communicated at the DoIT Daily meetings and the CIO meetings. Our testing determined the services and performance statistics were not communicated at the DoIT Daily meetings until September 12, 2018, and were never communicated at the CIO meetings.

16) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the Department was responsible for the scheduling and monitoring of the backup process. The agencies are responsible for informing the Department of their business needs. Our testing determined the agencies were responsible for scheduling the backups of their applications and data.

17) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the secure, encrypted transfer of mainframe data is achieved using Secure File Transfer Protocol (SFTP). Our testing determined the secure, encrypted transfer of mainframe data was achieved using File Transfer Protocol Secure (FTPS).

18) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the System Administrator runs a System Management Facility violation records report weekly and provided to the manager of Mainframe Software Support. Our testing determined the System Administrator ran the System Management Facility and reviewed the report. The manager of the Mainframe Software Support did not review the report. Additionally, our testing determined the manager of Mainframe Software Support was provided the systems programmer and high profile user ID report, which they reviewed.

19) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the Wintel Admin Team conducts an annual review of technical accounts to ensure appropriateness. Our testing determined the review of technical accounts was conducted monthly.

20) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the tool automatically pushes daily virus definition files to all systems beginning eight hours after the definition files are made available from the vendor. Our testing determined the definition files were pushed out to servers beginning six hours after the definition files were available.

21) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated Authentication Servers record failed login attempts to the network equipment. Logs are reviewed by LAN staff as requested by the Department's Security Operations Center staff and as needed for troubleshooting purposes. Our testing determined the Security Operations Center had not requested the LAN staff to review logs, as failed login attempts were not monitored.

22) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated monthly, quarterly, and annually Metric Reports are completed documenting the statistics on incidents and are provided to management. Our testing determined the metrics data were recorded in near real-time via a reporting tool and could be accessed whenever by the Security Team.

23) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the IT Service Desk initiates a Remedy ticket to track and document the event that captures the asset/property tag, the user reporting the loss, and any police reports if available. Once in Remedy, End User Computing (EUC) and the Security Operation Center (SOC) are notified. Our testing determined the Lost or Stolen Equipment Policy documented the SOC was notified by the EUC if the device did not have encryption.

24) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the Incident Management Process Guide documents Department workflow and remediation process for incident management. In November 2018, the Department changed the process for reporting and handling of Major Outage Response Teams (MORTs) and unplanned outages. However, the Guide was not updated until April 2019 to reflect the change in process. Additionally, MORTs, occurring after hours, did not follow the Guide. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance the entities calls that are relevant to user entities' internal control over financial reporting are responded to, tracked, and resolved in a timely manner."

25) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated reported incidents are tracked via a Remedy ticket until appropriate remediation efforts are completed. The Department was unable to provide a population of incidents classified as Unplanned Outages. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance the entities calls that are relevant to user entities' internal control over financial reporting are responded to, tracked, and resolved in a timely manner."

26) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the Incident Reports are submitted to the Chief Information Security Officer. The Department did not provide documentation demonstrating the Incident Reports were submitted to the Chief Information Security Officer for the period of July 1, 2018, through March 31, 2019. 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 deviations, 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."

27) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated Remedy On Demand is the Department's control mechanism over changes to Department resources, including infrastructure and applications (AIS, CIS, CPS, CTAS, and eTime). However, a complete and accurate population of changes was not provided. 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."

28) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the Department's process begins with an authorized person submitting a DoIT Badge Request Form to HR. The Department did not provide a listing of individuals who were authorized to submit the DoIT Badge Request Form. 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 protect equipment and facilities that are relevant to user entities' internal control over financial reporting."

29) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the network hardware and software generates an email to the 24x7x365 Network Operations Center or console display alert when a predefined event occurs or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. The statistics and threshold metrics are reviewed and recorded monthly. The Department did not provide documentation demonstrating the statistics were reviewed. As a result, the controls are not operating effectively 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."

30) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated security banner serves as a security awareness mechanism and is displayed at initial network connection warning of prosecution for unauthorized access, Access Control Lists reside on the network device itself and restrict communication to only certain IP addresses or address ranges, and Authentication Servers control access through assignment of access right privileges (read only or update) based on Department-defined group profiles. However, a complete and accurate population of devices was not provided. As a result, the controls are not operating effectively 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."

31) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated after review and sign-off by an authorized Department approver, a badge is created using Velocity with appropriate access rights assigned. The Department did not provide a listing of individuals who were authorized to approve. As a result, the controls are not operating effectively 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 protect equipment and facilities that are relevant to user entities' internal control over financial reporting."

32) As indicated, the accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System, the Department did not report any unencrypted equipment stolen or missing during the examination period; therefore, we did not perform any tests of the design or operating effectiveness of controls related to the control objective "Controls provide reasonable assurance the entities' calls that are relevant to user entities' internal control over financial reporting are responded to, tracked, and resolved in a timely manner."

33) As indicated, the accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System, the Department did not encounter failed backups during the examination period; therefore, we did not perform any tests of the design or operating effectiveness of controls related to the control objective "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."

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 and Technology's assertion:

a. the description does not fairly present the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System that was designed and implemented throughout the period from July 1, 2018, to June 30, 2019;

b. the controls of the State of Illinois, Department of Innovation and Technology 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 from July 1, 2018, to June 30, 2019; and,

c. the controls of the State of Illinois, Department of Innovation and Technology did not operate effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period from July 1, 2018, to June 30, 2019.

Other Reporting Required by Government Auditing Standards

In accordance with *Government Auditing Standards*, we have also issued our report dated August 8, 2019, on our consideration of the State of Illinois, Department of Innovation and Technology's internal control over (1) fairly presenting the State of Illinois, Department of Innovation and Technology's description of its Information Technology Shared Services System throughout the period July 1, 2018, through June 30, 2019, 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 and Technology's description of its

Information Technology Shared Services System throughout the period July 1, 2018, through June 30, 2019 (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 and 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 and Technology's internal control over reporting and compliance.

Restricted Use

This report is intended solely for the information and use of the Department of Innovation and Technology, user agencies of the Department of Innovation and Technology's Information Technology Shared Services System during some or all of the period from July 1, 2018, to June 30, 2019, 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
Jane Clark, CPA
Director of Financial and Compliance Audits

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

August 8, 2019
Springfield, Illinois

SECTION II

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

Illinois Department of
Innovation & Technology

JB Pritzker, Governor
Ron Guerrier, CIO and Acting Secretary

Honorable Frank J. Mautino
Auditor General, State of Illinois

We have prepared the description of State of Illinois, Department of Innovation and Technology's Information Technology Shared Services system entitled "Description of the IT General Controls and Application Controls for the Department of Innovation and Technology's Information Technology Shared Services System" for the information technology general controls and application controls throughout the period from July 1, 2018, to June 30, 2019 (description) for user agencies of the system during some or all of the period from July 1, 2018, to June 30, 2019, 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 and Technology also uses the Department of Central Management Services, a subservice organization to provide facility maintenance activities, 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, Virtustream, Inc, a subservice organization to provide cloud hosting services for the State's Enterprise Resource Planning system, and NICUSA, Inc, a subservice organization to provide Software as a Service. The description includes only the control objectives and related controls of the State of Illinois, Department of Innovation and Technology and excludes the control objectives and related controls of the Department of Central Management Services, Zayo Group, LLC, Microsoft, LLC, BMC Software, Inc., Virtustream, Inc., and NICUSA, Inc.

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 and Technology's controls are suitably designed and operating effectively, along with related controls at the State of Illinois, Department of Innovation and 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 paragraph 3, 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 from July 1, 2018, to June 30, 2019, 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 and 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 and 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.

2) Except for the matters described in paragraph 3, the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period from July 1, 2018, through June 30, 2019 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 and Technology's controls throughout the period from July 1, 2018, to June 30, 2019. 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 and 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; and

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

3) Description of Deficiencies in Fair Presentation, Suitability of Design, or Operating Effectiveness.

a) The accompanying description, of the State of Illinois, Department of Innovation and 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.

b) The accompanying description, of the State of Illinois, Department of Innovation and Technology, of Information Technology Shared Services System does not include controls to comply with the Complementary User Entity Controls documented in the subservice providers' System and Organizational Control Reports. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

c) The accompanying description, of the State of Illinois, Department of Innovation and Technology, of Information Technology Shared Services System does not include monitoring controls related to the services provided by the State of Illinois, Department of Central Management Services. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

d) The accompanying description, of the State of Illinois, Department of Innovation and Technology, of Information Technology Shared Services System does not include the controls over the maintenance and patching of the mainframe operating systems. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

e) The accompanying description, of the State of Illinois, Department of Innovation and Technology, of Information Technology Shared Services System does not include application changes (AIS, CIS, CTAS, CPS, eTime) follow the controls documented in the Application Lifecycle Management Manual. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

f) The accompanying description, of the State of Illinois, Department of Innovation and Technology, of Information Technology Shared Services System does not include the lack of documented policies or procedures dictating the process for employees to obtain physical access to facilities. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

g) The accompanying description, of the State of Illinois, Department of Innovation and Technology, of Information Technology Shared Services System does not include the process for individuals, other than Department employees, to obtain physical access to

Department facilities. This control is relevant to user agencies' internal control over financial reporting. As a result, the description is not fairly presented.

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

i) The accompanying description of the State of Illinois, Department of Innovation and Technology states the SQL team received an alert for missed backups. However, we did not include in the description the frequency of missed backups prior to the SQL team receiving an alert. As a result, the description is not fairly presented.

j) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states monitoring details were discussed at internal meetings. However, we did not include in the description the frequency in which the internal meetings were held. As a result, the description is not fairly presented.

k) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states risks from potential and newly discovered vulnerabilities are assessed through interaction with security experts and vendor subscription services. 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.

l) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states prior to March 2, 2019, vulnerability scans were scheduled monthly; after March 2, 2019, scans were scheduled weekly. However, we ran the vulnerability scans semi-monthly for February 2019. As a result, the description is not fairly presented.

m) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states the ERP Production Support initiated all communications, including incidents. Additionally, Release Management, including descriptions of any releases is sent to the agencies from the same dedicated email address. However, the ERP Production Support does not initiate communication through the dedicated email address. As a result, the description is not fairly presented.

n) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated on July 1, 2017, the Illinois Tollway was added as a user agency. However, the Illinois Tollway was added as a user agency on July 1, 2018. As a result, the description is not fairly presented.

o) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states the Department services and performance statistics were previously communicated at the DoIT Daily meetings and the CIO meetings. However, the services and performance statistics were not communicated at the DoIT Daily meeting until September 12, 2018 and were never communicated at the CIO meetings. As a result, the description is not fairly presented.

p) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states the Department was responsible for the scheduling and monitoring of the backup process. The agencies are responsible for informing the Department of their business needs. However, the agencies are responsible for scheduling the backups of their applications and data. As a result, the description is not fairly presented.

q) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states the secure, encrypted transfer of mainframe data is achieved using Secure File Transfer Protocol (SFTP). However, the secure, encrypted transfer of mainframe data is achieved using File Transfer Protocol Secure (FTPS). As a result, the description is not fairly presented.

r) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states the System Administrator runs a System Management Facility violation records report weekly and provides to the manager of Mainframe Software Support. However, the System Administrator runs and reviews the System Management Facility. Additionally, the manager of Mainframe Software Support is provide the systems programmer and high profile user ID report for review. As a result, the description is not fairly presented.

s) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states the Wintel Admin Team conducts an annual review of technical accounts to ensure appropriateness. However, the review of technical accounts is conducted monthly. As a result, the description is not fairly presented.

t) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states tool automatically pushes daily virus definition files to all systems beginning eight hours after the definition files are made available from the vendor. However, the definition files are pushed out to servers beginning six hours after the definition files are made available. As a result, the description is not fairly presented.

u) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states Authentication Servers record failed login attempts to the network equipment. Logs are reviewed by LAN staff as requested by the Department's Security Operations Center staff and as needed for troubleshooting purposes. However, the Security Operations Center does not requested the

LAN staff to review logs, as failed login attempts are not monitored. As a result, the description is not fairly presented.

v) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states monthly, quarterly, and annually Metric Reports are completed documenting the statistics on incidents and are provided to management. However, the metrics data are recorded in near real-time via a reporting tool and can be accessed whenever by the Security Team. As a result, the description is not fairly presented.

w) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states the IT Service Desk also initiates a Remedy ticket to track and document the event that captures the asset/property tag, the user reporting the loss, and any police reports if available. Once in Remedy, End User Computing (EUC) and the Security Operation Center (SOC) are notified. However, the Lost or Stolen Equipment Policy documents the SOC is notified by the EUC if the device does not have encryption. As a result, the description is not fairly presented.

x) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System stated the Incident Management Process Guide documents Department workflow and remediation process for incident management. In November 2018, the Department changed the process for reporting and handling of MORTs and unplanned outages. However, the Guide was not updated until April 2019 to reflect the change in process. Additionally, Major Outage Response Team (MORTs), occurring after hours, did not follow the Guide. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance the entities calls that are relevant to user entities' internal control over financial reporting are responded to, tracked, and resolved in a timely manner."

y) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states reported incidents are tracked via a Remedy ticket until appropriate remediation efforts are completed. However, we were unable to provide a population of incidents classified as Unplanned Outages. As a result, the controls are not suitably designed to achieve the control objective "Controls provide reasonable assurance the entities calls that are relevant to user entities' internal control over financial reporting are responded to, tracked, and resolved in a timely manner."

z) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states Incident Reports are submitted to the Chief Information Security Officer. However, we did not provide documentation demonstrating the Incident Reports were submitted to the Chief Information Security Officer for the period of July 1, 2018, through March 31, 2019. 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 deviations, 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."

aa) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states Remedy On Demand (referred to as Remedy or ROD) is the Department's control mechanism over changes to Department resources, including infrastructure and applications (AIS, CIS, CPS, CTAS, and eTime). However, we did not provide a complete and accurate population of changes to the Service Auditor. As a result, the controls are not suitability 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."

bb) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states the Department's process begins with an authorized person submitting a DoIT Badge Request Form to HR. However, we did not provide a listing of individuals who were authorized to submit the DoIT Badge Request Form. 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 protect equipment and facilities that are relevant to user entities' internal control over financial reporting."

cc) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states the network hardware and software generates an email to the 24x7x365 Network Operations Center or console display alert when a predefined event occurs or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. The statistics and threshold metrics are reviewed and recorded monthly. However, we did not provide documentation demonstrating the statistics were reviewed. As a result, the controls are not operating effectively 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."

dd) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states security banner serves as a security awareness mechanism and is displayed at initial network connection warning of prosecution for unauthorized access, Access Control Lists reside on the network device itself and restrict communication to only certain IP addresses or address ranges, and Authentication Servers control access through assignment of access right privileges (read only or update) based on Department-defined group profiles. However, we did not provide a complete and accurate population of devices to the Service Auditor. As a result, the controls are not operating effectively 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."

ee) The accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services System states after review and sign-off by an authorized Department approver, a badge is created using Velocity with appropriate access rights assigned. However, we did not provide a listing of individuals who were authorized to approve. As a result, the controls are not operating effectively 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 protect equipment and facilities that are relevant to user entities' internal control over financial reporting."

4) Description of Controls for Which There Is No Population to Test

During the period July 1, 2018, through June 30, 2019, the Department did not report any unencrypted equipment stolen or missing and did not encounter failed backups.

SIGNED ORIGINAL ON FILE

Ron Guerrier
Secretary, Acting
Department of Innovation and Technology
August 8, 2019

SECTION III

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

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

Overview of the Department of Innovation and Technology

The Department of Innovation and Technology (DoIT, the Department) was initially created under Executive Order 2016-01. Effective July 20, 2018, the Department of Innovation and Technology Act (Act) (20 ILCS 1370) legitimized the Department. The Act is the implementation of the Executive Order with additional provisions to ensure the Department functions as intended under the Executive Order. As stated in Section 1-15 of the Act, the powers and duties of the Department are to "promote best-in-class innovation and technology to client agencies to foster collaboration among client agencies, empower client agencies to provide better service to residents of Illinois, and maximize the value of taxpayer resources."

Subservice Organizations

The Department utilizes the following subservice providers:

- The Department of Central Management Services (DCMS) to manage building maintenance activities of Department occupied facilities.
- Zayo Group LLC to provide an alternate data center for off-site data 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. to provide hosting of the Department's change management tool Remedy On Demand.
- NIC, Inc to provide hosting and a web-based Statewide Permits and Licensing Solution (as of May 13, 2019).

Overview of Services Provided

As cited in the Act, the Department is responsible for "information technology functions on behalf of client agencies" with specific services related to:

- management of the procurement, retention, installation, maintenance, and operation of information technology (IT) used by client agencies;
- security protection, privacy of IT information as provided by law, and back-up facilities; and
- installation and operation of IT systems.

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. The Description excludes the control objectives and related controls of the Department of Central Management Services, Zayo Group LLC, BMC Software Inc., Microsoft LLC, Virtustream Inc., and NIC, 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 covers information technology general controls and specific application controls related to:

- Accounting Information System (AIS);
- Central Inventory System (CIS);
- Central Payroll System (CPS);
- Central Time and Attendance System (CTAS);
- eTime; and
- Enterprise Resource Planning System (ERP).

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.

<u>Control Environment</u>

Organizational Structure

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 "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 1-30 of 20 ILCS 1370. During the examination period, four individuals served as Secretary which provided for a continuous fulfillment of the top executive position. The Assistant Secretary position remains unfilled.

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 Enterprise Architect, Chief Technology Officer, ERP Program Director, and seven Chief Information Officers (CIOs) grouped into service delivery taxonomies.

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 (vacant since January 1, 2019 until filled June 1, 2019) 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) (vacant since January 26, 2019 with the Deputy CISO serving as CISO until permanently appointed on April 16, 2019) 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 of encryption, recovery, monitoring controls, incident detection, and response.

The Chief Service Officer (vacant until August 15, 2018 and again February 16, 2019) 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 goals of understanding, satisfying, and exceeding, if possible, customer expectations. This position is responsible for the delivery of customer-facing IT services, customer 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 the Act 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.

The Chief Enterprise Architect (vacant from February 20, 2019 through April 15, 2019) develops and designs the enterprise architecture, sets priorities, and ensures that projects are aligned to the Department's mission, long-term strategic goals, and business objectives. Effective March 16, 2019, the position description was clarified and retitled from "Chief Strategy Officer" to "Chief Enterprise Architect" to better reflect principal responsibilities.

The Chief Technology Officer (vacant from February 14, 2019 through April 15, 2019) 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.

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. Position vacant between October 6, 2018 through October 8, 2018.

The seven Group 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 Group 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. Vacancies within the Group CIOs include: Family, Children, Elderly, and Veterans vacant from April 16, 2019; Government and Public Employee Group CIO vacant from August 4, 2018 until October 31, 2018; Natural & Cultural Resources Group CIO and the Student Group CIO were vacant one day during the audit period (July 1, 2018); Public Safety vacant from September 1, 2018 through April 15, 2019; Transportation Group CIO has not yet been filled.

Human Resources

The Department's hiring practices adhere to legal requirements as published in the State Personnel Code, Personnel Rules, union contracts, *Rutan/Shakman* decisions, court orders, and applicable state/federal laws.

Workforce members are categorized into permanent State employment workers (job protected or at will) and contractual workers (operating under a personal services contract). In addition, vendor contractors are hired based on contract requirements which follow Illinois procurement regulations and are outside of the Department's personnel hiring practices and statutorily mandated training obligations.

Each permanent State employment position is identified on the organizational chart. Approved formal written job descriptions (CMS-104 forms) document the duties, responsibilities, qualifications, minimum acceptable competency education requirements, and experience levels for each position. Minimum acceptable competency education requirements and experience levels are identified in each job description to ensure a quality and qualified workforce. For positions subject to the Personnel Code, newly developed and clarified job descriptions require final approval from the Department of Central Management Services' (DCMS) Division of Technical Services within the Bureau of Personnel. Job descriptions for positions not subject to the Personnel Code are approved by the Department's Secretary to ensure that defined duties and required qualifications are clearly documented. For personal service contractual employees (PSC), duties and responsibilities are defined initially in a PSC description of services to which the Secretary's signature is affixed and then included in the PSC contract drafted by Legal which is also signed by the PSC contractor and the Secretary.

Upon verification between Human Resources (HR) and the appropriate supervisor/manager of the accuracy of the job description or PSC description of services and identification of funding, the Department's HR prepares a Personnel Action Request (PAR) form used to initiate the posting of the employment opportunity. The Secretary and the Department's Chief Fiscal Officer approve the PAR prior to HR's posting of the position.

Interview procedures, selection, and required forms vary depending on whether the position is covered by collective bargaining. For collective bargaining positions, HR compiles appropriate information as outlined in the position's collective bargaining agreement that dictates eligibility rights and forwards it to the interview panel who then conducts interviews based on Rutan guidelines as appropriate for the position.

For protected non-bargaining unit positions, HR identifies individuals who have submitted an employment application and have been deemed qualified and eligible through DCMS' examining process. HR forwards the information to the interview panel to commence the interview process.

For PSC positions, HR forwards candidate information to the hiring unit to schedule interviews. The most qualified candidate is selected, documented on a PSC Decision Form, and the hiring process continues concluding with a contract outlining the terms and conditions of the services to be provided.

'At will' positions require approval from the Office of the Governor in order to be filled. When filling 'at will' positions, the HR Director is responsible for certifying that the selected candidate meets minimum qualifications as stated in the job description. Prior to October 12, 2018, there were no specific compulsory documentation or forms required for this certification. Beginning October 12, 2018, 'at will' appointments were captured and recorded by following a DCMS three-part form certification process which was streamlined into one form titled 'Exempt Position Certification' effective January 18, 2019. The completed certification form is provided to the Office of the Governor, the Office of the Executive Inspector General Hiring and Employment Monitor and the Special Master prior to the candidate's first working day.

New employees and PSCs must pass a background check before being offered employment. The prospective candidate's demographic information is entered into the Illinois State Police's Criminal History Information Response Process (CHIRP) system. If/when the background check returns information that is acceptable to the Department, the hiring process continues with employment offered to the prospective candidate.

For State employees, performance evaluations are scheduled for probationary periods as well as annually. For employees serving a four-month probationary period, performance evaluations are completed two weeks prior to the end of the probationary period. For employees serving a six-month probationary period, performance evaluations are completed at the end of three months and again at two weeks prior to the end of the probationary period. For certified employees, performance evaluations are completed annually. Each month, HR distributes a list of due, past due evaluations and upcoming performance evaluations (due within in the next 60 days) to each respective supervisor. It is the supervisor's responsibility and obligation to complete the performance evaluation as required. Completed evaluations are returned to HR for processing in the HRIS database, and completed evaluations bearing the Secretary's signature are provided to the employee and the supervisor as well as a being placed in the employee's personnel file.

For PSCs, the corresponding performance evaluation requirements vary dependent upon contract language. That is, a specific contract may mandate or simply recommend an evaluation be conducted. Contractual employment may be terminated without cause by either party which encourages satisfactory performance and quality work effort.

Newly-hired employees are provided the DCMS Policy Manual by HR during New Employee Orientation and are required to sign an acknowledgment form accepting responsibility to abide by the policies contained within the DCMS Policy Manual. Newly hired PSCs are governed by the terms, conditions, and duties outlined in their legally binding contract. PSCs acknowledge and accept compliance with Department policies and procedures, as each contract states that the "Contract Employee agrees to be bound by and comply with policies and procedures of the Agency."

Employees and PSCs acknowledge awareness of responsibilities through affirming to follow policies as referenced above and through mandated annual training covering Security Awareness, Safeguard Disclosure, Ethics, and Sexual Harassment Prevention. The HR Training Coordinator provides assistance to other functional areas responsible for the monitoring, tracking, and reporting of these required compulsory training. Security Awareness and Safeguard Disclosure trainings are tracked by the Department's Information Security Office while the Department's General Counsel (legal) office tracks Ethics and Sexual Harassment Prevention training.

Newly hired employees and PSCs are emailed the Security Awareness Training, Safeguard Disclosure Training, Ethics Training, and Sexual Harassment Prevention Training for State Employees. An acknowledgement is generated at the end of each training.

As directed by the Act, the Department transitioned existing, permanent State employees from other agencies into the Department in order to achieve consolidation of IT resources. Transition and consolidation of these workforce members fall outside the normal, personnel hiring regulations.

Over 220 Department badged employees from 11 agencies have been fully transformed to the Department's payroll and timekeeping systems as directed by the Act and designated by the Office of the Governor. This process involves:

- Receiving notification from the Governor's Office of Management and Budget (GOMB) that sufficient funds are available to proceed with the transition effort;
- Notifying the affected unions of the effective date of the transformation;
- Notifying the affected employees of the effective date of the transformation and if pay dates will change;
- Notifying the impacted agencies of the effective date of the transformation and providing them with a transformation checklist to be completed and returned for each impacted employee;
- Providing a spreadsheet to DoIT Enterprise Applications Membership and Benefits Manager to have the impacted employees transferred systematically from their legacy agency to DoIT's "org proc" code in the benefits system;
- Conducting abbreviated New Employee Orientation for transforming employees;
- Providing/obtaining updated documents and fulfilling training requirements;
- Coordinating with and receiving applicable personnel, medical, benefit and payroll files from legacy agencies for each transferred employee;

- Identifying and processing appropriation code changes in the DCMS Personnel System for each impacted employee on the effective date;
- Printing and distributing CMS-2 turnaround documents for each transitioned employee to Payroll, Benefits, Timekeeping and HR;
- Distributing completed CMS-204 forms, as well as the transformation checklist forms, received from legacy agency to Payroll, Benefits, Timekeeping and HR;
- Entering affected employees into HRIS (if they aren't already in HRIS), HR, Payroll, eTime and Timekeeping systems (done by batch if already in CTAS and Central Payroll; individually in both systems if they are not);
- Reconciling vacation base dates, updating and requesting any new schedule changes through DCMS Compensation to maintain employee's current schedule;
- Verifying every payroll deduction listed on the transformation checklist and CMS-204; confirming that every payroll deduction has a corresponding supporting document;
- Updating organizational charts; and
- Assembling newly-transformed employees' personnel and payroll files including appropriation code change CMS-2's and transformation checklists.

Voluntary and involuntary separation procedures for an employee or a contractor both result in HR generating an Employee Exit Form (Exit Form) which is emailed to the supervisor. Once the Exit Form is completed by the supervisor, it is automatically forwarded to the IT Coordinator group which then initiates the process of creating a Remedy Service Request to disable access and return equipment.

For an employee voluntarily separating from the Department (transferring, resigning, or retiring), once HR receives written confirmation from the employee, HR initiates a PAR, obtains appropriate Department authorizations from the Chief Fiscal Officer and the Secretary, and generates the Exit Form. For an employee non-voluntarily being terminated from the Department, once HR receives either written or verbal direction from the Secretary or his designee, HR initiates a PAR, obtains appropriate Department authorizations from the Chief Fiscal Officer and the Secretary and generates the Exit Form. For a contractor, the separation process begins upon expiration or termination of the contract at which time an Exit Form is generated.

Risk Assessment Process

The Department followed DCMS' IT Risk Assessment Policy until October 8, 2018 when the Department replaced it by publishing a new Risk Assessment Policy (Policy) on the Department's website.

The new Policy assigns responsibility for conducting risk assessments and vulnerability scanning to the Department with the scope spanning entities identified as client agencies under executive orders, compiled statutes, or inter-governmental agreements. The Policy also requires the Department to share assessment results with client agency senior management.

The Department has developed a corresponding set of procedures collectively referred to as the Risk Management Program which categorizes risk 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.

The Department conducts organizational risk assessments based on the standards of the National Institute of Standards and Technology for agencies, boards, and commissions that report to the Governor. The risk assessment process includes a series of phases that leads from one to another based on the Departments risk management methodology. The data gathered is utilized to calculate a risk maturity score to assess the strength and effectiveness of existing controls.

Agencies are responsible for providing corrective action plans corresponding to risk assessment findings. Risks and corrective action plans are captured in a Risk Register used for follow-up.

In addition, 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. A vulnerability scanning protocol is employed to assess identified servers. Prior to March 2, 2019, vulnerability scans were scheduled monthly; after March 2, 2019, scans were scheduled weekly. The Department shares vulnerability scanning results with Department senior management, Group CIO's, and agency CIO's by granting access to the vulnerability reporting tool.

Information and Communications

The Department's website delivers information to customer agencies and to Department staff covering:

- Initiatives and accomplishments,
- Policies,
- Service Catalog (which describes services available to user agencies)
- Instructions on how to order services and products as well as how to report operational problems.

The policies located on the Department's website include:

POLICY TITLE	**EFFECTIVE**	**REVISED**
Acceptable Use Policy	11.15.2018	
Access Control Policy	11.29.2018	
Accountability, Audit, and Risk Management Privacy Policy	10.08.2018	
Audit and Accountability Policy	10.08.2018	
Awareness and Training Policy	10.08.2018	
Backup Retention Policy	03.15.2011	
Change Management Policy	12.15.2008	01.03.2012
CJIS Security Supplemental Policy	10.08.2018	
Configuration Management Policy	11.05.2018	
Contingency Planning Policy	10.08.2018	
Data Breach Notification Policy	12.01.2007	01.01.2010

Provided by the Department of Innovation and Technology

POLICY TITLE	EFFECTIVE	REVISED
Data Classification and Protection Policy	12.15.2008	01.03.2012
Data Minimization and Retention Privacy Policy	10.08.2018	
Data Quality and Integrity Privacy Policy	10.08.2018	
Enterprise Desktop/Laptop Policy	12.15.2008	01.03.2012
ESI Retention Policy	02.15.2009	
FTI Supplemental Policy	10.08.2018	
General Security for Statewide IT Resources Policy	12.15.2008	01.01.2010
General Security for Statewide Network Resources Policy	12.15.2008	01.01.2010
Identification and Authentication Policy	10.08.2018	
Identity Protection Policy	06.01.2011	
Individual Participation and Redress Privacy Policy	10.08.2018	
Information Security Incident Management Policy	10.08.2018	
IT (Information Technology) Recovery Policy	10.01.2009	
IT Governance Policy	12.15.2008	01.03.2012
IT Resources Access Policy	12.01.2007	
Laptop Data Encryption Policy	12.01.2007	01.01.2010
Media Protection Policy	10.08.2018	
Mobile Device Security Policy	09.08.2015	11.10.2016
Overarching Enterprise Information Security Policy	11.29.2018	
PCI Data Security Policy	10.08.2018	
Personnel Security Policy	12.10.2018	
PHI Supplemental	11.05.2018	
Physical and Environmental Protection Policy	10.08.2018	
Privacy Security Policy	11.05.2018	
Program Management Policy	10.08.2018	
Risk Assessment Policy	10.08.2018	
Security Assessment and Authorization Policy	10.08.2018	
Security Planning Policy	10.08.2018	
Statewide CMS/BCCS Facility Access Policy	12.15.2008	01.01.2010
System and Communication Protection Policy	10.08.2018	
System and Information Integrity Policy	10.08.2018	
System and Services Acquisition Policy	10.08.2018	
System Maintenance Policy	10.08.2018	
Transparency, Authority, and Purpose Privacy Policy	10.08.2018	
Use Limitation Privacy Policy	10.08.2018	
Wireless Communication Device Policy	12.15.2008	01.01.2010

The website also provides links to the DoIT Digest content which informs the reader of new initiatives, ongoing projects, and administrative issues such as software upgrades, newly hired executive management, and other Departmental news. Effective March 1, 2019, the Digest publication schedule changed from weekly to every two weeks.

In addition to the Department's website, customer agencies are kept informed through direct correspondence and face-to-face meetings. The Department's Communication Office sends email correspondence to appropriate agency groups (directors, CIOs, IT Coordinators, Telecom Coordinators) as appropriate to the message being conveyed. Group CIOs provide an exchange of information between the Department and agencies and keep both the Department and agencies informed regarding significant events, service issues, improvements, processes, and strategic goals. Group CIOs meet with agency CIOs when business need requires or when instructed by Department management to update and gather information from agencies. Group CIO communication occurs at an individual agency level. State-wide level agency communication is accomplished through CIO Council meetings which are held at the Secretary's request to update and inform agency CIOs of news and information.

Agency CIOs, along with Department leadership, are invited to attend "DoIT Daily" meetings (Mondays through Thursdays). DoIT Daily is a forum to share high-level and high-risk operational issues with a team equipped to discuss steps for resolution. As Department high-level executive management changed, the format and level of detail of the DoIT Daily also changed. From July 1, 2018 to March 10, 2019, the DoIT Daily communicated detailed divisional announcements and updated the progress of new initiatives or projects. From March 11, 2019 thru April 8, 2019, the DoIT Daily was shortened to a "stand-up" format where content was limited to alerts of impactful issues and outages that need to be addressed. Effective April 9, 2019, a modification to this format was made where Tuesday's discussion was expanded to include announcements regarding ongoing projects or upcoming events that may potentially impact Department services.

Department internal staff are kept informed through multiple sources such as the Department's website, the Employee Portal (intranet), Town Hall meetings, and emails. The Employee Portal provides information covering topics such as pensions and retirement, insurance, training opportunities, payroll information, and workplace safety. Town Hall meetings keep Department workforce members informed on topics such as Department strategic priorities and new Department and/or Statewide initiatives. Direct email communications alert workforce members to technical, security, or emergency issues and concerns such as outages, phishing attempts, and scheduled upgrades.

The Department communicates ERP information to the agencies through its Production Support team. Production Support initiates all communications, including incidents, from a dedicated 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 same dedicated email address.

Agencies are encouraged to contact the ERP Team as follows:

- 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.
- A general dedicated ERP email account for any general questions about the ERP Program.

Monitoring

Monitoring of Department Services and Performance

Department services and performance statistics were previously communicated and shared with agencies through the DoIT Daily and CIO meetings. From July 1, 2018 through March 10, 2019, key performance indicators, operational metrics, percent of open tickets, number of critical tickets, problem resolution trends and targets, unavailability of a service, and progress of transition activities, and functional issues were discussed at DoIT Daily meetings which enabled both Department executives and user agency CIOs the opportunity to be informed of the effectiveness of delivered services. Beginning March 11, 2019, with the appointment of a new Secretary, the monitoring details presented in the DoIT Daily were removed from the agenda but still discussed in internal meetings conducted by the IT Service Desk. The IT Service Desk manager conducts monthly meetings inviting representatives from appropriate Department teams to discuss performance metrics. In addition to storing data on a SharePoint site, service level metrics are posted on the Department's website.

Monitoring of Subservice Providers

The Department's Governance, Risk and Compliance unit collects subservice providers' System and Organization Controls (SOC) reports and communicates Complementary User Entity Controls to appropriate business owners to ensure they are aware of their accountability and for implementing corrective action plans.

Annually, the Department's ERP Team receives and reviews the SOC 1 type 2 report from Virtustream, Inc. These reports are reviewed and 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 maintained on the ERP SharePoint site.

Environment

Midrange

The Department's midrange configuration consists of several multi-core processors 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 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 Elastic Sky X Integrated (ESXi) is an enterprise class type-1 bare-metal Hyperivsor that installs onto a physical server with direct access to and control of underlying resources and can effectively partition hardware to increase virtual servers' ratios.
- Advanced Interactive eXecutive (AIX) is an enterprise-class UNIX operating system 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 for both desktop and server use.

Mainframe

The Department's mainframe configuration consists of multiple CMOS processors (Complementary Metal Oxide Semiconductor processors) segregated into logical 'production' and ‘test’ partitions. Partitions are configured in a Sysplex platform, IBM’s systems complex coupling environment. The primary operating system software includes:

- IBM z/OS: a complex operating system (OS) that functions as the system software which controls the initiation and processing of work within the mainframe.
- z/Virtual Machine (z/VM): a time-sharing, interactive, multi-programming operating system.

Primary z/OS 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.
- 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”.
- DataBase 2 (DB2) is a relational database management system for z/OS environments.

The primary z/VM subsystem is NOMAD which is a database software system.

Information Systems Overview-Applications

The Department’s Enterprise Business Applications group (also referred to as Enterprise Application & Architecture - EAA) and the Enterprise Resource Planning (ERP) group offer several applications to agencies including:

- Accounting Information System (AIS) hosted on the Department’s mainframe;
- Central Inventory System (CIS) hosted on the Department’s mainframe;
- Central Payroll System (CPS) hosted on the Department’s mainframe;
- Central Time and Attendance (CTAS) hosted on the Department’s mainframe;
- eTime hosted on the Department’s midrange, server environment; and
- Enterprise Resource Planning (ERP) hosted via Virtustream, Inc.

Agencies are responsible for the complete, accurate, and timely entry of data into Department supported applications. The Department is responsible for application updating and maintenance. Separate, stand-alone user manuals and guides are available for the AIS, CIS, CPS, CTAS applications. User instructions and guides are imbedded into the application itself for eTime. Applications have edit features designed to reject erroneous or invalid data. When erroneous or invalid data is entered, an error message is displayed on the screen indicating the problem. Various reports are generated, based on the application, to assist with data integrity and reconciliation. For ERP users, HANA analytic capabilities provide access to business intelligence tools that allow an end user to develop their own report or dashboard.

Accounting Information System

AIS addresses accounts payable, manages appropriations, fund transfers and adjustments, vendors, contracts and contract amendments. AIS also 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 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 invoice information to assure sufficient funds are available in the appropriation. 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 voucher is printed for agencies' head approval and submission to the Office of the Comptroller. In addition, the agencies can print the AIS13 for review.

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.

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 interfaces and interacts with the following 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 Management System; and
- Office of the Comptroller.

Central Inventory System

CIS manages inventory, and creates, updates, and tracks property records for equipment, furniture, real property, and vehicles. Upon receipt of an asset, agencies enter the asset's tag, location, voucher information, and description into CIS. In the event information regarding the asset needs to be revised (such as location change), the agency enters the correction. In the event an asset requires deleting, the agency contacts DCMS' Property Control Division 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 monthly.

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. Reconciliation reports assist agencies in processing their inventory.

Central Payroll System

CPS 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.

Agencies are responsible for reviewing the payroll voucher to ensure the accurate calculation of deductions.

CPS has a ten-day working pay schedule, which allows agencies to enter their payroll ensuring that vouchers are processed timely. Every pay period is assigned a close date, which is the date that 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 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, payroll vouchers are produced as a series of reports for each agency. Each agency prints the payroll voucher, approves, and submits 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. This is accomplished by the agency submitting a Remedy ticket requesting a change and assigning to the CPS Support unit. Remedy procedures route the request to appropriate Department staff who then run special ad-hoc programs to correct the specific problem and then re-run the Gross-to-Net process.

The Office of the Comptroller verbally and/or through email informs the Department of any federal tax rate change. The Department's CPS staff modifies federal tax tables accordingly.

When calculating State withholding, CPS recognizes a limited set of State identifiers which are listed in the Central Payroll User Manual. When a record is entered for which there is no recognized State identifier, CPS generates an error message. Appropriate action is taken to either correct an error or to request the addition of a State identifier.

Prior to March 8, 2019, on an annual basis, CPS staff researched tax rates for CPS-recognized states and updated state tax tables accordingly. Effective March 8, 2019, the CPS manager began receiving email notifications from a procured service that identifies state tax rate changes. Upon notification, the CPS manager creates a Remedy work order that instructs CPS support team staff to update the state tax rate for states identified within CPS where the rate has changed.

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 provides agencies with the CPS User Manual to assist in the preparation of payroll records. Reconciliation reports assist agencies in processing 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.

Central Time and Attendance

CTAS 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 records attendance information using either the positive or exception method. The positive method requires the timekeeper 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.

Each agency's timekeeper is responsible for entry and maintenance of an employee's time and attendance; vacation, sick, personal, etc.

To reconcile the time entered for a payroll period, CTAS performs a "close" process which checks for consistency and completeness and performs necessary calculations for overtime and compensatory time. The 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 complete a "pre-close" process and review 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. Discrepancies need to be reconciled before a "close" can be finalized.

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 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), 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.

eTime

eTime 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.

eTime has defined functional roles of system administrator, administrator, timekeeper, supervisor, employee, auditor, and chief financial/fiscal officer. The system administrator role is used to make agency specific changes to settings and/or to setup new agencies. The administrator role assigns roles to individuals within the administrator's agency. Agency eTime administrators are established through submission of a Remedy Service Request by the agency's IT Coordinator as approved by the agency's Human Resource Director or designee. The timekeeper role processes exceptions that may result from leave requests and/or overtime worked. The supervisor role approves employee time reports, overtime pre-approvals, overtime worked, and leave requests. The employee role permits direct entry of time worked and adjustments to the standard work schedule by the workforce member. The auditor role provides search capabilities in a view only mode. The chief financial/fiscal officer role provides limited search capabilities in view only mode.

After authentication is granted into the browser-accessible log-in screen, the user selects from multiple options based on the action to be taken and the user's functional role. For employees, the process begins with entering exceptions to standard, scheduled hours 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. Supervisors enter approvals for overtime and leave requests which are processed nightly via the CTAS batch process.

Agencies may opt to use eTime as a mechanism for capturing, collecting, and reporting contractual worker (operating under a personal services contract) hours. Actual hours worked are entered by the contractor. Once their time report is submitted, eTime routes hours entered to the appropriate supervisor 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.

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 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 module which facilitates the procurement of goods.

On July 1, 2017, the Illinois Tollway (Tollway) was added as a user agency. While all the same modules are used, the business requirements of the Tollway varied from those of other user agencies, which resulted in the need to customize the enterprise design. All user agencies, except the Tollway, are organized into the STIL company code. The Tollway uses the ILTA company code and its functionality differences as related to controls are noted in the descriptions below. Additionally, Department ERP Functional Experts referenced in the sections below, continue to support the entire enterprise. However, due to unique business requirements, one Tollway staff has been granted certain master maintenance for the ILTA company code.

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 IOCA (State of Illinois-STIL) chart of accounts is maintained by the General Ledger Functional Expert. The maintenance of the General Ledger ILTA (Tollway) chart of accounts is maintained by authorized master data maintenance Tollway staff and moved into workflow approval by the General Ledger Functional Expert.

The Department has implemented three ledgers for Company Code STIL 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. The Tollway has implemented four ledgers for Company Code ILTA to account for the multiple bases of accounting utilized by the Tollway; full accrual, modified accrual, cash basis, and Trust Indenture.

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 for Company Code STIL. The Tollway utilizes 12 regular months (January through December) and does not operate in lapse period, however, period 13 could be utilized for special adjustments on Company Code ILTA.

In order to close a period, each agency must complete recording of all transactions. In addition, the agency is required to complete various reconciliations with the Office of the Comptroller, 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 for Company Code STIL, the General Ledger Functional Expert opens the next accounting period (next month) in order for agencies to post to the next month. In addition, the General Ledger Functional Expert closes the prior period.

Closing of a period is to be conducted for Company Code STIL:

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

At the request of the Tollway for Company Code ILTA, the General Ledger Functional Expert opens the next accounting period (next month) in order for the agency to post to the next month as well as close the prior period.

Closing of a period is to be conducted for Company Code ILTA:

- Monthly-last day of the month,
- Quarterly-March, June and September, and
- Year end-December.

Quarterly and year-end closing includes tasks for required reporting requirements; C-15, C-97, etc.

Fiscal Year 2018 lapse period (period 13) and all periods for Fiscal Year 2019 remain open for Company Code STIL. Calendar year 2018 (period 12) and all periods for calendar year 2019 remain open for Company Code ILTA.

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 works 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, 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 saves the document and the Oversight Approver is notified of the invoice waiting approval. The Oversight Approver reviews 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 documents 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, a nightly batch 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. 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. 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 Supplier Relationship Management Module 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, a 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, disposed-of, and transferred assets for Company Code STIL. The Tollway records depreciation on new, disposed of, and transferred assets in the subsequent month. 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. The Tollway may contact their authorized master data maintenance staff or the Assets Functional Expert.

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 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.

For Company Code STIL, the value of the Shopping Cart directs the required approvals; supervisor, manager, and fiscal. For the Tollway, the value and the type of goods in the Shopping Cart directs the required approvals; supervisor, manager, and fiscal staff.

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. The Tollway also uses a Purchase Requisition (Shopping Cart) to request inventory from stock. However, if stock is available, a Stock Transport Order is created instead.

Public Sector Collection & Disbursements

Public Sector Collection and Disbursements provide 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 social security number, federal employer identification number, or a unique agency identifier. 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. At this level a Contract Account number is assigned to the customer which is unique to a specific agency.
- Contract Object – the third level, defines the customer's account with additional detail, specific licenses, taxes, claims, etc. At this level a Contract Object number is assigned to the customer which is unique to a specific agency.

When activity is conducted by the customer or the agency, the activity is posted at the Contract Object level. 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 is completed by utilizing the SAP Check Lot functionality which allows an agency to post payments that will be processed to the Office of the Comptroller on an Expenditure Adjustment Transmittal form (C-63) or a Receipts Deposit Transmittal (C-64). When utilizing Check Lot, the total of the individual payment posting must agree with the total of Check Lot.

Once the Office of the Treasurer's draft is received, the applicable Expenditure Adjustment Transmittal form or Receipts Deposit Transmittal is created, signed, and sent to the Office of the Comptroller, along with a batch file of the Receipts Deposit Transmittals.

Any payment(s) required to be processed on the Expenditure Adjustment Transmittal (C-63) form are still transmitted to the Office of the Comptroller in paper format.

Upon receipt of the payment, the posting is made against the AR at the Customers Contract Object level or SAP invoice (receivable) document number by the applicable agency. In the event a one-time payment is received, the payment is posted as a miscellaneous receipt and no SAP customer number is utilized to process the payment in SAP.

Monthly, agencies utilize the General Ledger Balance Report in order to balance with the Comptroller's SB04 (Monthly Revenue Status) report. In addition, the agencies 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 (FM)

Funds Management records, tracks, and reports on revenues, expenditures, commitments, obligations, and transfers.

For Company Code STIL, 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 or email. The FM Functional Expert with Firefighter access completes the creation of the new fund. The FM Functional Expert also creates/edits FM master data and budget/appropriation on behalf of all agencies.

The Tollway budget creation follows a different process in which the Tollway's Board of Directors approves an annual maintenance and operational (M&O) budget and all multi-year capital programs. The M&O budget for the fiscal year is approved by the Board of Directors in estimated classifications and divisions. The M&O budget is uploaded in detail by cost center, accounts, and months with a Board Resolution number called Functional Area. Board Resolution numbers are required to be entered for each initial budget as well as any supplemental budget programs. Approvals related to the entering of initial/supplemental budgets are handled outside of ERP by Tollway staff. New funds, or any other FM master data, can be created by either the FM Functional Expert or the authorized master data maintenance Tollway staff.

Grants Management

Grants Management is utilized to maintain the details (terms and conditions) of the grant awards between the granting entity (federal, other state agencies, private, etc.) and the user 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.

Controlling

The Controlling process in IL ACTS collects, analyzes, distributes, allocates and reports financial data according to Cost Objects such as Costs Centers, Internal Orders, and Projects/Work Breakdown Structures.

Each Agency defines its own Cost Centers according to its reporting needs, generally to distinguish individual functional and/or geographical areas within the organization which would commonly be associated with departments. Dividing an organization into Cost Centers, enables reporting and analytics on the individual cost centers and any defined groups of cost centers.

MASTER DATA:

- <u>Primary Cost Elements</u>: Primary Cost Elements are the links between the Financial Accounting (FI) module and Controlling (CO) module. Every revenue and expense General Ledger Account (GL Account) in FI is defined as a Revenue Element or Cost Element in CO. When a transaction is processed in FI to a revenue or expense GL Account, at the same time a posting is made to the corresponding Revenue Element or Cost Element in CO. The Primary Cost Elements are created at the same time as their corresponding General Ledger Account.
- <u>Secondary Cost Elements</u>: Secondary Cost Elements are revenue and expense components used to allocate costs as needed among CO Cost Objects including Cost Centers, Internal Orders, and Work Breakdown Structure elements (WBS). Because Secondary Cost Elements are only used for the reclassification among Cost Objects of costs already incurred in Primary Cost Elements, Secondary Cost Elements are not linked to any component in FI. Accordingly, these allocation postings are not reflected in the Financial Accounting module.
- <u>Statistical Key Figure (SKF):</u> Statistical Key Figures are quantitative amounts used in allocation rules. These form the basis of allocation of costs from a Cost Center to other Cost Centers or Cost Objects. For example, facility/building costs can be allocated among Cost Centers based on the number of square feet used by each of the Cost Centers. A SKF is used to store the data about the number of square feet. SKF's can hold any type of amounts that Agencies require to allocate their costs appropriately, including time increments, headcount-based amounts, measures of space or size, weights, percentages, and so on.

SERVICES PROVIDED TO END USER AGENCIES:

<u>Master Data Maintenance</u> – The IL ACTS CO Functional Expert executes new requests or request for change to cost center master data using their Steady State Fire Fighter ID. Internal Order and Work Breakdown Structure creation and maintenance is performed by user Agency personnel.

Change Management Support – Any testing/approvals required as part of incident resolution or new change requests. See section D for description of Change Management process and role of IL ACTS State Functional Expert.

HANA Analytics
The HANA Analytics functionality provides agency end users with enhanced reporting capabilities. Users can query their own agency data against views that have been built by the ERP team. Users are also provided access to business intelligence tools that allow an end user to develop their own report or dashboard.

Information Technology General Controls

Change Control
Remedy On Demand (referred to as Remedy or ROD) is the Department's control mechanism over changes to Department resources including infrastructure and applications (AIS, CIS, CPS, CTAS, and eTime).

Remedy components include service requests, work orders, tasks, and change requests which can originate either externally from a customer request or internally from support staff.

Remedy accepts service requests only from agency authorized IT Coordinators. Service requests may generate work orders, tasks, or change requests. Internally, Remedy work orders, tasks, and change requests may also be created by authorized Department managers or support staff. Change requests are created by support staff when the service request or work order will result in significant impact to a resource or when multiple work areas will be impacted or for a non-routine activity.

Work orders, incidents, tasks, and change requests are assigned to Department technicians, support staff, and subject matter experts through group (team) profiles and individual assignments as directed by the IT Service Desk or by a designated Department support staff. Remedy uses status indicators to manage work flow. Status indicator of complete automatically generates an email notification to the requestor. The requestor may contest or challenge the completed status within 5 days from the email notification.

Change Control – Other than Applications
Control over changes to the network, mainframe, and midrange infrastructures as well as to data storage devices are documented in the Change Management Process Guide, ROD Change Management Guide, and the Change Management User Guide which provides a quick reference of the Department's change processes.

Agencies are responsible for informing the Department of changes to Department owned or managed real property assets, infrastructure devices, and other IT equipment through the timely submission of a Remedy request which accurately and completely documents the change.

The Change Advisory Committee (CAC) supports the authorization of changes and assists Department managers and technicians in assessing and prioritizing changes and makes recommendations regarding significant impacts. The CAC 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 authorized agency personnel.

Change requests are classified into Class and Impact categories with approval levels of Support Group Manager, Enterprise Change Manager, and the Change Advisory Committee. A matrix in the Change Management User Guide, published on the CAC SharePoint site (User Guide Quick Reference), identifies the level of approval based on combinations of class and impact values.

In the event of an emergency, only verbal approval by the Support Group Manager is required to begin remediation. Remedy documentation is finalized once the emergency has subsided.

Significant or extensive impact changes require test, implementation, and back out information be provided within the change request. Emergency changes require a Post Implementation Review be provided within the change request.

Change Control - Applications (AIS, CIS, CTAS, CPS, and eTime)
For application changes, processing steps are documented in EAA Mainframe Change Management Procedures and the EAA Web Services Change Management Procedures.

An application change is initiated with the submission of a Remedy request which then follows standard processes described within. 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 reports.

For mainframe application changes, a revision control and code management system permit a developer to 'checkout' program code while prohibiting modified code from being placed back into the production area without proper authorization. Prior to December 16, 2018, Move Sheets were approved by an EAA supervisor who forwarded them to a Library Services shared email. Library Services would send an email to the originating supervisor and/or developer indicating the status of the move. After December 16, 2018, developers attach the Move Sheet to the corresponding change request record within Remedy. Remedy's built-in workflow approval process requires supervisory approval before Remedy releases the activity to the Library Services group that performs the move into production. Moves to the mainframe production environment are completed by Library Services based on Move Sheet instructions.

For web applications, prior to implementation, the EAA group supervisor approves the request for deployment into the production environment. A developer or EAA group supervisor, who did not code the change, moves the change into the production environment. In addition, there is a limited number of staff authorized to deploy to production. Starting November 2018, an additional, supplemental process was added in Team Foundation Server that now automates deployment into production upon supervisorial approval.

The Remedy request is considered resolved after all tasks have been designated as completed. Remedy status value of 'completed' automatically generates an email notification to the requestor who then may contest or challenge the result within 5 days from the notification.

Change Control-ERP

Changes to the ERP follow the processes defined in the IL ACTS ERP Change Control Process Guide.

The change management process begins with either the submission of a Remedy Help Desk ticket or a Change Request via the ERP Change Request SharePoint form. A single request may be a body of work containing multiple tasks, some of which necessitate a change to code, configuration, or application of maintenance patches to the ERP which originate from an ERP staff, development vendor, or agency user.

For Remedy Help Desk Tickets, these parties can enter the description of their issue into Remedy. Based on this description, a classification and priority code are assigned indicating emergency or normal classification and low, medium, high, or critical priority. Once a Remedy Help Desk Ticket has been assigned to an ERP team, appropriate ERP staff or ERP vendor staff become responsible for completing the tasks necessary to implement the change.

For Change Requests, designated parties enter their requirements into a SharePoint form. Categorization, urgency, and priority codes are identified at entry, enabling assignment prioritization.

Changes always begin in a development environment and are transported to quality and production environments (in that order) once all testing and approvals by the ERP team have been completed. There are certain configuration requests, however, that are not transported due to their complexity. These types of configuration requests are initially applied in a development environment. Only after testing and verification by a secondary ERP team member is the configuration applied in a quality environment, where it is tested again. After review of testing results by both ERP functional and management staff, a designated ERP team member is authorized to make the configuration change in the production environment using a Firefighter access. ERP management subsequently reviews the log of work completed. Testing results and transport movement activities are tracked in the Hewitt Packard Quality Control tool.

Remedy Help Desk tickets or Change Requests that are technical in nature, such as patches, are handled by the ERP's hosting provider and applied via transport to Production based upon an agreed upon schedule or after alignment with an ERP manager. The Help Desk ticket or Change Request is considered resolved upon completion of configuration, transport of code changes, where applicable.

Emergency Releases

The Program Managers or their delegates have the authority to allow emergency releases for defects or change requests, based upon a subjective analysis on the impact to the users. Emergency releases occur on-demand, after proper authorization and approvals are documented in the Hewitt Packard Quality Control tool (for transports) or the Governance, Risk and Compliance (GRC) (for configuration).

Change Control Over Network

Network infrastructure modifications are performed according to Enterprise Change Management Procedures.

For common infrastructure devices, the Department maintains detailed technical specifications identifying mandatory configuration parameters. New Wide Area Network (WAN) backbone equipment is energized, configured, and operated in a lab environment to help ensure faultless operation in production.

New Local Area Network (LAN) devices that meet Department standard 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 change management procedures.

IT Service Desk

The Department's IT Service Desk serves as a central point of contact for processing and managing IT service requests, password resets, as well as incident management (reporting, assignment, and resolution). Incidents are reported to the IT Service Desk by Department staff and customers via phone, email, or website submission.

Incident Management

The Incident Management Process Guide documents Department workflow and remediation processes for incident management.

An incident is defined as an unplanned interruption to an IT service, reduction in the quality of an IT service, or a failure of a configured item.

Incidents are reported to the IT Service Desk by staff and agencies via phone, email, or website form submission. When the IT Service Desk receives a report of an incident, a Remedy ticket is opened, documenting the user's name, agency, and contact information along with a detailed description of the incident. Each incident is 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 and closure of the ticket. Reported incidents are tracked via a Remedy ticket until appropriate remediation efforts are completed.

Incidents which are assigned both widespread/extensive impact and critical urgency, or events affecting an entire agency that has an unknown or uncertain resolution, are tagged as a potential major outage. Under these conditions, IT Service Desk support staff modify the Remedy ticket assignment group to "Major Outage Response Team" and update the Outage Type field to "MORT". The assigned IT Service Desk Duty Manager notifies MORT team members (subject matter experts and decision makers appropriate for the event and its resolution) via available communication media (email, phone, or other). Once a resolution or work-around has been achieved, the Duty Manager informs the IT Service Desk who then conveys the information to affected users and verifies that that service has been restored.

Lost or Stolen Equipment

As published in the Acceptable Use Policy, Enterprise Desktop/Laptop Policy, General Security for Statewide IT Resources Policy, and the Mobile Device Security Policy, users are responsible for reporting lost or stolen equipment by notifying their immediate supervisor and/or the IT Service Desk.

When notified, the IT Service Desk emails the asset owner's supervisor and manager of the event. The IT Service Desk also initiates a Remedy ticket to track and document the event that captures the asset/property tag, the user reporting the loss, and any police reports if available. Once in Remedy, End User Computing (EUC) and the Security Operation Center (SOC) are notified.

An encryption protection feature is installed as part of laptop imaging prior to deployment. At any time, authorized EUC staff with special privileges have the ability to view laptop properties to determine that this encryption feature was properly installed and is active.

If the device was encrypted, the ticket is assigned to Asset Management for disposition and SOC documentation will be recorded as no breach with no data compromised. Asset Management will complete a request for deletion of the device from inventory.

If encryption is inactive or was not installed as part of the device imaging process prior to deployment, then the SOC enacts a breach investigation that consists of steps outlined in their Security Incident Playbook. The first step is to interview the user to determine if sensitive or confidential data was stored on the device. If no sensitive or confidential resided on the device, the process continues as if the device was encrypted. Otherwise, the SOC assists with investigation and response for the resolution of and mitigating the impact of the potentially compromised data and affected users. Documentation, correspondence, and resolution actions are recorded and captured in the SOC's incident reporting tool. If further investigation is required, Asset Management forwards a copy of the police report to the Illinois State Police.

ERP- Helpdesk Monitoring Process

The IT Service Desk assigns ERP appropriate requests 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 assignment is tasked to Production Support. Production Support leverages Remedy in order to track the incident until resolution. Production Support then sends an acknowledgement to the submitter/user.

At this point, Production Support triages the Remedy request to first determine if it can be resolved without a change to the ERP. Production Support interacts with the user to address the issue. If it can be resolved without a change, Production Support modifies the status within Remedy to automatically notify the originator of the request via email.

If the Remedy request is determined to be a defect that requires a change, the Remedy record 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 Change Request in SharePoint. At this point Production Support will change the status of the SharePoint ticket to "Resolved", as well as changing to the corresponding status 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 Change Request and follow the change control 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 policies titled Identification and Authentication Policy, Personnel Security Policy, and the legacy IT Resource Access Policy address logical security and are published on the Department's website.

Access to Department resources (network, shared services, mainframe processing, and applications) begins with submission of a service request from an authorized agency IT Coordinator. The IT Service Desk applies Remedy workflow processes to satisfy the request. Access to Department resources ends when the Department has been notified that an individual is separating employment or the initial justification for access has changed. Revoking access is initiated upon submission of Remedy request or, under special or emergency circumstances, by instruction of the Chief Information Security Officer.

Access Provisioning – Applications

Access to AIS, CIS, CPS, and CTAS is a three-layer approach requiring acquisition and activation of (1) network, (2) mainframe, and (3) application-specific accounts. Remedy processes as noted above are followed to grant access to network and mainframe resources.

Application specific accounts are managed by Agency Application Administrators who are responsible for assignment of their agency's application specific accounts, associated rights and privileges, password management, and deactivation or reassignment. Agency Application

Administrators are established through IT Coordinator submission of a Remedy service request. The Department may assist an agency when issues arise which are managed through the Remedy process.

Application-specific accounts are directly related to and tightly coupled with running of production jobs for a given agency. Operational efficiency requires that application accounts remain consistently named and referenced to facilitate uninterrupted generation of production operational activities such as database updates, transaction posting, and report generation.

Access to eTime application is authenticated via Active Directory (AD). Functionality within the eTime application is based upon assigned roles. It is the responsibility of the agency to manage eTime.

Access Provisioning-ERP

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 monitoring. The HANA Analytics functionality does not currently use GRC to automate user access provisioning and changes. Manual processes being used are described below.

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 (Non-HANA Analytics)

The initial upload of an end user’s access occurs as part of the cutover process leading up to an agency’s go live date. Designated agency staff prepare and approve a final mapping of access profile to each of its end users. A segregation of duties analysis is performed by the ERP security team based on this mapping and the results are presented to the designated agency staff person to determine either remediation or mitigation of the risk. Once the segregation of duties analysis is approved by the designated agency staff, the agency users and their access are loaded into the GRC production environment using Firefighter access. Each agency end user receives an email with their SAP ERP ID and temporary password the evening before the go-live date. Upon initial login, the password must be immediately reset.

Once an agency is live on 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 Provisioning – HANA Analytics

Each agency is created as a separate user group in the HANA system to ensure access to agency data is restricted. The HANA Analytics functionality is extended to agency end users only after an initial hands-on onboarding/training session is completed. In this session, the agency provides a list of end users who will need access. Initial agency access to the HANA Analytics commences with a Remedy Help Desk Ticket submitted by ERP staff for the list of end users provided by the agency. The SAP ERP ID used is the same as what the end user already has in GRC. This ID is assigned in the agency user group and a separate temporary password is emailed to the end user. After initial onboarding, designated agency representatives submit a Remedy Help Desk Ticket for access that includes agency name, user name, user email address and the SAP ERP ID that end user already has in GRC. The Production Support team validates the SAP ERP ID and sends the end user an email with the ID and a temporary password.

Access De-Provisioning (Non-HANA Analytics)

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

Access De-Provisioning (HANA Analytics)

The designated agency representative submits a Remedy record to notify the Production Support team that access should be terminated. The Production Support team completes the termination manually.

Reviews (Non-HANA Analytics)

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

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 the Department's self-service option: DoIT Identity Management tool. 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 does not have appropriate rights to reset a mainframe password, the user is instructed to contact their Agency System Software Coordinator. In the event that the Department is the proxy, a Remedy request is assigned to the Department's Security Software Coordinator or Security Software Administrator. Using information from the Remedy request, the Coordinator or the Administrator contacts the user to reset the password. If unable to contact the user on the first attempt, a message is left asking the user to call back. No password is left in the message. Passwords used in the resetting process are temporary, one-time use only. The Remedy ticket remains open until the password has been successfully reset after which the Remedy ticket is closed.

Password Resets - Active Directory
Active Directory accounts are reset by users calling the IT Service Desk or by one of the Department's self-service options – Microsoft Identity Management (MIM) or the Department's Identity Management (DIM) tool. IT Service Desk authenticates the caller through verbal verification. IT Service Desk encourages use of the self-service option.

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 MIM/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 MIM/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 MIM/DIM if eligible.

Password Resets - Novell
Self-service options are not available for Novell. IT Service Desk staff will perform a verification of two of three pieces of information before resetting the password.

Password Resets - ERP
Agency end users are required to submit a request through the IT Service Desk, which is then assigned to dedicated non-HANA and HANA Production Support teams. 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 in GRC.

System Security
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 to verify the identity 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 as encrypted values within the system security database.

For agencies that 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.

Semi-monthly, the Security Software Administrator receives a separation report from HR. 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.

The Department performs a monthly review of Illinois.gov Active Directory accounts and disables accounts which have been dormant for a designated period of time. For the July and August 2018 monthly reports, the designated period of time triggered at 90 days or more. Starting with the September 2018 report, designated period of time triggered at 60 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 a Remedy request 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.

Administrators

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, a Remedy request is submitted to deactivate the account.

Application Administrators/Programmers

Access to application source code, Job Control Language 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 and is 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 Services

Network Services is comprised of three areas of responsibility;

- Local Area Network Services: responsible for managing firewalls, switches, servers, and software that are the components to the local area network.
- Agency Wide Area Network Services: responsible for managing firewalls, routers, switches, servers, and software that are the components to the wide area network and virtual private network infrastructures.
- Backbone Wide Area Network: responsible for managing wave equipment, firewalls,

routers, switches, cabling, servers, and software that are the components to the backbone, wide area network as well as peering and Internet Access (Illinois Century Network).

Common Controls

- Mandatory backbone design and configuration standards and guides are defined and maintained.
- A security banner serves as a security awareness mechanism and 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 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 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.
- The Department applies self-monitoring hardware and software, redundant backbone construction, scheduled backups, and vendor-based services to maintain network availability.
- Self-monitoring network hardware devices record all events and forward to multiple logging servers. These servers use filters to automatically generate alerts when a Network Services' configured parameter or condition occurs.
- Network diagrams depict common connectivity configurations.

Local Area Network (LAN)

The Department has implemented redundancy in Data Center LANs and at agency locations where technically, fiscally, and operationally feasible. Infrastructure component equipment is physically located at either Department facilities or on agency premises.

Network software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization.

Network hardware and software generates an email to LAN Services Support staff and a console display alert when a predefined event occurs, or a threshold is reached. LAN staff follow up on these alerts and engage operational teams for resolution as necessary.

Authentication Servers record failed login attempts to the network equipment. Logs are imported into the Department's security information and event management tool for archival, historical, or investigative purposes. Logs are reviewed by LAN staff as requested by the Department's Security Operations Center staff and as needed for troubleshooting purposes.

Data Center firewall and switch configurations have incremental backups performed twice a day that are stored at the Central Computing Facility (CCF). Those configurations are backed up nightly and stored for a maximum of 60 days at the CCF and/or the Alternate Data Center (ADC).

Agency Wide Area Network (WAN)

The Department has implemented last mile redundancy where technically, fiscally, and operationally feasible. Infrastructure component equipment is physically located at either Department facilities or on agency premises.

Network software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization.

Network hardware and software generates an email to the 24x7x365 Network Operations Center or console display alert when a predefined event occurs, or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. 24x7x365 Network Operation Center staff reviews each occurrence and engage operation teams for resolution.

Authentication Servers record failed login attempts to the network equipment. Failed attempts automatically generate an email notification which is forwarded notifications to Network Design & Engineering staff for determination if further action is required.

Virtual Private Networks (VPN) provide controlled and trusted connections between devices when required for data traversing 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.

Configurations are saved on Syslog servers for one week and backed up remotely on a weekly basis stored at the CCF and/or the ADC.

Backbone Wide Area Network (WAN)

Infrastructure component equipment is physically located either at Department facilities or on agency premises. The Department has implemented redundancy between Point of Presence sites where technically, fiscally, and operationally feasible and has also installed fiber optic wave transmission technologies to provide high speed backbone transport services.

Network software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization.

Network hardware and software generates an email to the 24x7x365 Network Operations Center or console display alert when a predefined event occurs or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. The statistics and threshold metrics are reviewed and recorded monthly.

Authentication Servers record failed login attempts to the network equipment. Failed attempts automatically generate an email notification which is forwarded notifications to Network Design & Engineering staff for determination if further action is required.

Configurations are saved on Syslog servers for one week and backed up remotely on a weekly basis stored at the CCF and/or the ADC.

Security Operations Center

The Security Operations Center continuously monitors 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 submitted to the Chief Information Security Officer.

Additionally, the reports below are provided to management:

- Daily the Shift 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, and annually Metric Reports are completed documenting the statistics on incidents.

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 to push and monitor Windows patches.

The Anti-Virus Group is responsible for pushing daily definitions and other antivirus software updates out. A tool is applied to manage daily definitions and antivirus software updates. The tool automatically pushes daily virus definition files to all systems beginning 8 hours after the definition files are made available from the vendor. This 8 hour delay provides the opportunity to correct a bad update or pull back a faulty update if ever notified by the tool vendor. The Anti-Virus Group has tools available to monitor the enterprise computing equipment that are out of compliance regarding antivirus definitions.

Additionally, agencies are responsible for notifying the Department of actual or suspected information security breaches, compromised accounts, or unauthorized access.

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 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 the applicable group/division for resolution.

The Daily Shift Report documents the activity conducted on mainframe production systems and incident calls received at the Operations Center. Beginning in January 2019, the Shift Report incidents are correlated with Remedy incidents. Prior to January 2019, the Shift Report was not routinely correlated to a Remedy Ticket. 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 forwarded to Enterprise Infrastructure management and supervisors for awareness and follow-up of outstanding issues.

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

The Operator Shift Change Checklist (an action list shared between shifts) 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 Operator Shift Change Checklist were not routinely signed by the Operations Shift Supervisor prior to February 2019. Effective February 1, 2019, Checklists are signed off by Operations Center supervisors.

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 Resource Measurement Facility reports which are run daily and monthly. Performance and capacity monitoring are documented via internal memorandum distributed via email to Enterprise Infrastructure management monthly.

The Department has implemented system options to protect resources and data. The System Management Facility records operating system activities. The System Administrator runs a System Management Facility violation records report weekly and provides to the manager of Mainframe Software Support. Prior to February 2019, the report was not routinely signed by the manager. The process was updated in February 2019 where the manager now signs-off on the violation report.

Midrange

Midrange availability is monitored by the Operations Command Center via the What's Up Gold system. Command Center technicians notify System and/or Storage technicians of What's Up Gold alerts.

Structured Query Language (SQL) database servers use the Idera tool set for additional monitoring. The Idera system alerts have been set up to generate emails to SQL support staff. The SQL support staff use the Idera tools to help trouble shoot SQL issues.

The Active Directory Domain Controllers use Microsoft System Center for additional monitoring. System Center alerts have been set up to email alerts to AD support staff. The AD staff uses Microsoft System Center to help trouble shoot AD issues.

The Department follows installation procedures as appropriate for the functionality of the server and its role in delivering services. After a virtual server is built, a template is produced which is used, if needed, to replicate other similar servers. Configuration settings and profiles are backed up weekly.

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 secure, encrypted transfer of mainframe data is achieved using Secure File Transfer Protocol. The software MoveIt is used to transmit midrange data between servers and applications. The MOVEit software sends email alerts for any failures to Department support staff. Access to MOVEit systems are reviewed on an annual basis by the Department's Information Security specialists.

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

Another option available to valid illinois.gov users for the secure transmission of data is the file transfer utility 'FileT'. This utility uses random key generation to access files stored on a server. Only those with a valid key may download files from the server. Files are automatically purged from the server after 5 days. The sender must acknowledge a warning of unauthorized access message by clicking a box before transfer is allowed. The sender receives a confirmation message containing a link to the transfer status as well as a link to remove the file from the server if necessary. A valid Illinois.gov email address is required to use this utility for State resources; either as the recipient or the sender.

Backups

Mainframe

The Department is responsible for the scheduling and monitoring of the backup process. Agencies are responsible for informing the Department of business needs. 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 procedures 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 record is submitted 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. Spectrum Protect and Data Protection Advisor automatically generate daily reports indicating the backup status of scheduled jobs from the prior day. These reports are emailed to the Enterprise Storage and Backup group who then investigates the cause of failures 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 DBAs 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 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 notifies vendor support. For critical issues, the Isilon call home feature additionally notifies the Enterprise Storage and Backup group.

Physical Security

The Department's warehouse physical security is managed by cameras and badge proximity readers that are installed at the front and rear entrances and at the dock doors. Dock door badge readers operate from inside the building only. Authorized badged individuals may enter the Warehouse or End User Computing (EUC) areas through swiping of a Velocity badge. Visitors alert Warehouse or EUC staff who then unlock the door. A visitor's log captures who enters the building. Unescorted access is permitted when appropriate, as determined by Warehouse or EUC staff, and for maintenance personnel.

For the Department's Communication Center and the Central Computing Facility (CCF), security guard monitor 24x7x365, proximity badge readers located at various interior and exterior entry points, security alarms, and cameras. Individuals not registered in the Velocity system (no permanent badge issued) must present proof of identification and sign the visitor register log at the guard station to obtain a visitor badge. Visitors are required to be escorted while in either building. For individuals registered in the Velocity system but not having a permanent badge immediately available, guards issue a temporary badge upon proof of identification. Temporary badges are also issued to vendors once identification has been validated by the facility security guard. Temporary badges allow movement within the building without escort.

Additional physical restrictions and levels of access are applied at the CCF to the area housing computing processing and storage equipment. Access to this secured area is limited to a small group of individuals with specific business need and requires special badge permission to exit the elevator or enter through the stairway door. Surveillance is enhanced with additional cameras and door sensors.

The Department uses Hirsh/Velocity Access Control System (Velocity) to create badges that grant physical access to a Department building, floor, or room. Velocity captures dates, times, and doors when a badge is swiped.

The Department's process begins with an authorized person submitting a DoIT Badge Request form to HR. An authorized person includes supervisors, managers, and designated Department facility approvers.

Valid proof of identity and documentation of a clear background check, performed in the past five years, must be verified prior to badge issuance. The form requires entries regarding affiliation of employee, reason for access, badge type, expiration date, and access rights needed.

After review and sign-off by an authorized Department approver, a badge is created using Velocity with appropriate access rights assigned. The badge displays a photo of the individual and an expiration date.

Badge access is revoked by the Velocity system at badge expiration date or by HR after official notice of separation/termination is provided.

Objectives and Related Controls

The Department of Innovation and Technology 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 and Technology’s 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 and Technology’s description of Information Technology Shared Services System for the information technology general controls and application controls.

Complementary User Agency Controls

The Department of Innovation and Technology's 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 and Technology. 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 and Technology. Therefore, each agency's internal control over financial reporting must be evaluated in conjunction with the Department of Innovation and Technology's 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.

Control Objective	Complementary User Agency Controls
#1	Agencies are responsible for the entry and maintenance of data into the applications.
#1	Agencies are responsible for reviewing the payroll voucher to ensure the accurate calculation of deductions.
#3	Agencies are responsible for submission of a Remedy ticket documenting issues and needs of the environment and applications.
#4	Agencies are responsible for reporting incidents to the IT Service Desk.
#4	Agencies are responsible for reporting lost or stolen equipment to the IT Service Desk.
#5	Agency IT Coordinators are responsible for the submission of an approved Service Request for the creation of user access.
#5	Agency IT Coordinators are responsible for the submission of an approved Service Request for modification of user access.
#5	Agency IT Coordinators are responsible for the submission of an approved Service Request for the termination of user access.
#5	Agencies are responsible for the submission of an approved Service Request for the creation of a security software account.
#5	Agency IT Coordinators are responsible for the submission of an approved Service Request for the establishment of the agency Application Administrator.
#5	Agency Application Administrator is responsible for the management of their agencies application accounts; assignment, modification and deactivation of rights.
#5	Agencies are responsible for ensuring proper segregation of duties in the assignment of application user access rights.
#5	Authorized agency staff are responsible for entry of an access request into GRC and first level of approval.
#5	Agencies are responsible for ensuring proper segregation of duties.
#5	Agencies are responsible for contacting the IT Service Desk or the utilization of the self-service options, in order to reset the AD, Novell, or ERP accounts.

SECTION IV

DESCRIPTION OF THE DEPARTMENT OF INNOVATION AND TECHNOLOGY'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

Description of the Department of Innovation and Technology's 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 and Technology.

Our examination was limited to the control objectives and related controls specified by the Department of Innovation and Technology 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 and Technology's controls may not compensate for such weaknesses.

The Department of Innovation and Technology's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of controls specified by the Department of Innovation and Technology. 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 and Technology, we considered aspects of the Department of Innovation and Technology's 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 of 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 and Technology, 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 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 exists, that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
CE1.1	The organizational hierarchy promotes separation 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 deviations noted.
CE1.2	The hiring practices adhere to legal requirements as published in the State Personnel Code, Personnel Rules, union contracts, *Rutan/Shakman* decisions, court orders and applicable state/federal laws.	Reviewed the hiring procedures, Personnel Code, union contracts, *Rutan/Shakman* decisions, court orders, and applicable federal and State laws to determine hiring process.	No deviations noted.
CE1.3	Vendor contractors are hired based on contract requirements, which follow Illinois procurement regulations.	Reviewed contract requirements and Illinois procurement regulations to determine hiring process.	No deviations noted.
CE1.4	Each employee position has an approved formal written job description which documents the duties, responsibilities, 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.	No deviations noted.
		Selected a sample of job descriptions to determine if they outlined duties and qualifications.	No deviations noted.

CE1.5	New employee and personal service contractors must pass a background check prior to being offered employment.	Selected a sample of new employees and personal service contractors to determine if background checks were completed prior to being offered employment.	No deviations noted.
CE1.6	Performance evaluations for new employees serving a four month probationary period are completed two weeks prior to the end of their probationary period.	Selected a sample of new employees serving a four months probationary period to determine if applicable probationary evaluations had been completed two weeks prior to the end of the probationary period.	25 of 26 employees selected had probationary evaluations completed 5 to 264 days late.
CE1.7	Performance evaluations are completed at the end of the three months and six months for employees serving a six months probationary period.	Selected a sample of new employees serving a six months probationary period to determine if the three months and six months probationary evaluations had been completed.	9 of 13 employees selected had probationary evaluations completed 3 and 114 days late.
CE1.8	Certified employee performance evaluations are completed annually.	Selected a sample of certified employees to determine if an annual evaluation had been completed.	21 of 60 employees had an annual evaluation completed 1 and 126 days late.
CE1.9	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 and contractors to determine if the DCMS Policy Manual Acknowledgement had been completed.	No deviations noted.
CE1.10	Personal service contractors acknowledge and accept compliance with Department policies and procedures, as each contract states that the "contract employee agrees to be bound by and comply with policies and procedures of the Agency."	Selected a sample of new personal service contractors to determine if the contract contained a clause the "contract employee agreed to be bound by and comply with policies and procedures of the Agency".	No deviations noted.

CE1.11	Annually, employees and personal service contractors are provided security awareness training, safeguard disclosure training, ethics training and sexual harassment prevention training.	Selected a sample of employees and personal service contractors to determine if annual security awareness training had been completed.	27 of 1,403 employees and personal service contractors selected had not completed the security awareness training.
		Selected a sample of employees and personal service contractors to determine if safeguard disclosure training had been completed.	167 of 1,401 employees and personal service contractors selected had not completed the safeguard disclosure training.
		Selected a sample of employees and personal service contractors to determine if ethics training had been completed.	No deviations noted.
		Selected a sample of employees and personal service contractors to determine if sexual harassment prevention training had been completed.	1 of 1,355 employees and personal service contractors selected had not completed the sexual harassment prevention training.
CE1.12	Annually, employees and contractors acknowledge compliance with security policies.	Selected a sample of employees and contractors to determine if the annual acknowledgment of compliance with security policies had been completed.	27 of 1,403 employees and contractors had not completed the annual acknowledgment of compliance with security policies.
CE1.13	An Employee Exit form and a Remedy Service Request are completed to ensure remove of access and retrieval of equipment for employees and contractors.	Selected a sample of terminated employees and contractors to determine if an Employee Exit form and a Remedy Service Request had been completed.	1 of 27 terminated employees selected did not have a Remedy Service Request completed.

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

	CONTROLS SPECIFIED BY THE DEPARTMENT	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 deviations noted.
C1.2	Separate, stand-alone user manuals and guides are available for AIS, CIS, CPS, and CTAS applications.	Reviewed user manuals to determine if they provided guidance to users.	No deviations noted.
C1.3	User instructions and guides are imbedded into the application itself for eTime.	Reviewed instructions and guides to determine if they provided guidance to users.	No deviations noted.
	ERP		
C1.4	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.	No deviations noted.

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	TESTS OF CONTROLS	RESULTS OF TESTS
C2.1	The Department's CPS staff modified federal tax tables accordingly.	Reviewed the federal tax rates to determine if the rates had been updated within CPS.	No deviations noted.
	Prior to March 8, 2019, annually, the CPS review and update the applicable states' tax rates within CPS. Effective March 8, 2019, the CPS staff receives email notification from a service identifying changes to state tax rates.	Reviewed the states' tax rates to determine if the rates had been updated within CPS.	4 of 24 states' (including Washington DC) tax rates were incorrect. The State of Illinois' tax rate was correct.

<u>Control Objective 3:</u> 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	TESTS OF CONTROLS	RESULTS OF TESTS
	Changes other than Applications		
C3.1	Control over changes to the network, mainframe, and midrange infrastructures as well as to data storage devices are documented in the Change Management Process Guide, ROD Change Management Guide, and the Change Management User Guide.	Reviewed the Change Management Process Guide, ROD Change Management Guide, and the Change Management User Guide to determine if controls were documented.	No deviations noted.
C3.2	Significant or extensive impact changes require test, implementation, and backout information to be provided with the change request.	Selected a sample of significant or extensive impact changes to determine if test, implementation, and backout information was provided with the change request.	The Department did not provide a complete and accurate population of changes. For the changes provided: 3 of 60 change requests selected did not have Backout Plans. 2 of 60 change requests selected did not have Test Plans.
C3.3	Emergency changes requires a Post Implementation Review be provided within the change request.	Reviewed a sample of emergency changes to determine if a Post Implementation Review was provided within the change request.	The Department did not provide a complete and accurate population of changes. For the changes provided, no deviations were noted.

	Application Changes - AIS, CIS, CTAS, CPS, eTime		
C3.4	For application changes, processing steps are documented in EAA Mainframe Change Management Procedures and the EAA Web Services Change Management Procedures.	Reviewed the EAA Mainframe Change Management Procedures and the EAA Web Services Change Management Procedures to determine if they documented the change management procedures.	The EAA Mainframe Change Management Procedures did not provide guidance related to: required approvals, testing and documentation requirements, requirements for followup after the change was moved to production and emergency change requirements. The EAA Web Service Change Management Procedures provide guidance related to: prioritization of requests, required approvals, testing and documentation requirements, and requirements for followup after the change was moved to production.
C3.5	An application change is initiated with the submission of a Remedy request.	Selected a sample of application changes to determine if a Remedy request had been submitted.	No deviations noted.

C3.6	For mainframe application changes, a revision control and code management system permits a developer to "checkout" program code which prohibiting modified code from being placed back into the production area without proper authorization.	Selected a sample of mainframe changes to determine if proper authorization was obtained prior to placing in the code management system.	No deviations noted.
C3.7	Prior to December 16, 2018, Move Sheets were approved by an EAA supervisor.	Selected a sample of changes to determine if the move sheet was completed prior to implementation and approved by the EAA supervisor.	No deviations noted.
	After December 16, 2018, the developer attached the Move Sheet to the corresponding change request record in Remedy.	Selected a sample of changes to determine if the move sheet was attached to the change request.	No deviations noted.
C3.8	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 move to the production environment.	No deviations noted.
C3.9	Prior to December 16, 2018, Library Services sent an email to the originating supervisor and/or 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 deviations noted.
C3.10	Prior to implementation for web applications, the EAA group supervisor approves the request for deployment into the production environment.	Selected a sample of changes to determine if the EAA group supervisor approved the request for deployment.	No deviations noted.

C3.11	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 deviations noted.
	Application Changes - ERP		
C3.12	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.	No deviations noted.
	Defects		
C3.13	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 deviations noted.
C3.14	Transport requests to the Quality Regions are to be requested and approved via HPQC.	Selected a sample of defects to determine if transport requests to the Quality Regions had been requested and approved via HPQC.	No deviations noted.
C3.15	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 deviations noted.
C3.16	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 was requested via HPQC and approved by a State Project Manager.	No deviations noted.
C3.17	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 deviations noted.

	Change Requests		
C3.18	A Change Request is to be completed, validated, reviewed and approved via the Department's SharePoint.	Selected a sample of change requests to determine if they had been completed, validated, reviewed and approved via the Department's SharePoint.	11 of 38 change request forms did not have all required fields completed.
C3.19	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 a Functional Specification Design document had been developed and approved by the State's Functional Expert.	No deviations noted.
C3.20	Technical Specification Design document is to be developed and approved by Production Support.	Selected a sample of change requests to determine if a Technical Specification Design document had been developed and approved by Production Support.	No deviations noted.
C3.21	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, reviewed by Production Support and maintained on Production Support's SharePoint.	No deviations noted.
C3.22	Transport requests to the Quality Regions is to be requested and approved via HPQC.	Selected a sample of change requests to determine if transport requests to the Quality Regions had been requested and approved via HPQC.	No deviations noted.
C3.23	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 had been completed, reviewed by the State's Functional Expert, and maintained in HPQC.	No deviations noted.

C3.24	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 transport requests to the Production Region were requested via HPQC and approved by a State Program Manager or the State's Project Manager.	No deviations noted.

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

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C4.1	The Incident Management Process Guide documents Department workflow and remediation processes for incident management.	Reviewed the Incident Management Response Process Guide to determine if it documented the workflow and remediation process of reported incidents.	In November 2018, the Department changed the process for reporting and handling of MORTs and unplanned outages. However, the Guide was not updated until April 2019 to reflect the change in process. MORTs occurring after hours did not follow the Guide.
C4.2	Reported incidents are tracked via a Remedy ticket until appropriate remediation efforts are completed.	Reviewed Remedy and inquired with IT Service Desk staff.	The Department was unable to provide a population of incidents classified as Unplanned Outages. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
C4.3	Missing or stolen equipment is tracked via a Remedy ticket.	Reviewed Remedy to determine if missing or stolen equipment was tracked.	No deviations noted.
C4.4	An encryption protection feature is installed as part of laptop imaging prior to deployment.	Selected a sample of stolen and missing laptops to determine if verification of the installation of encryption was completed.	No deviations noted.

C4.5	If encryption is inactive or was not installed, the Security Operations Center will enact a breach investigation that consists of steps outlined in their Security Incident Playbook.	Reviewed Remedy and inquired with 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.
C4.6	Production Support hosts a weekly meeting with ERP management to provide status updates.	Selected a sample of weekly meetings to determine if status updates were provided.	No deviations noted.
C4.7	Production Support provides ERP management with written weekly updates and monthly reports.	Selected a sample of weekly and monthly reports to determine if status updates were provided to the ERP management.	No deviations noted.

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	TESTS OF CONTROLS	RESULTS OF TESTS
	Access Provisioning		
C5.1	The Department policies, Identification and Authentication Policy, Personnel Security Policy, and the IT Resource Access Policy address logical security and are published on the Department's website.	Reviewed the Identification and Authentication Policy, Personnel Security Policy, and the IT Resource Access Policy to determine if they documented logical security controls.	No deviations noted.
		Reviewed the Department's website to determine if the Identification and Authentication Policy, Personnel Security Policy, and the IT Resource Access Policy had been published.	No deviations noted.
C5.2	Access to Department resources (network, shared services, mainframe processing, and applications) requires a service request authorized by the agency IT Coordinator.	Selected a sample of new employees/contractors to determine if a service request was authorized by an agency IT Coordinator.	No deviations noted.
C5.3	Revoking access is initiated upon submission of Remedy request or, under special or emergency circumstances, by instruction of the CISO.	Selected a sample of terminated employees/contractors to determine if access was timely terminated.	1 of 31 terminated individuals selected did not have a completed Remedy request disabling network access. 20 of 31 Remedy requests for terminated individuals selected were completed 2 and 10 days after the individuals' termination date.

	Access Provisioning - AIS, CIS, CTAS, CPS, eTime		
C5.4	Agency Application Administrators are established through IT Coordinator submission of a Remedy service request.	Selected a sample of agencies established during the examination period to determine if a service request was approved by the agencies' IT Coordinator.	No deviations noted.
	Access Provisioning - ERP		
C5.5	Designated agency staff prepare and approve a final mapping of access profile to each of its end users.	Selected a sample of initial uploads to determine if final mapping of access profiles was approved by the agency.	No deviations noted.
C5.6	A segregation of duties analysis is performed by the ERP security team based on this mapping and the results are presented to the designated agency staff person to determine either remediation or mitigation of the risk.	Selected a sample of initial uploads to determine if the ERP security team completed a segregation of duties analysis.	No deviations noted.
C5.7	ERP security reviews access request to ensure no segregation of duties conflict exist prior to approving.	Selected a sample of new access requests to determine if segregation of duties conflicts were reviewed.	No deviations noted.
	ERP HANA Analytics		
C5.8	Initial agency access to the HANA Analytics commences with a Remedy Help Desk Ticket submitted by ERP staff for the list of end users provided by the agency.	Selected a sample of new HANA users to determine if a Remedy Help Desk Ticket was submitted by the agency.	19 of 45 HANA Analytics users did not have a Remedy Help Desk Ticket.
C5.9	After initial onboarding, designated agency representatives submit a Remedy Help Desk Ticket for access that includes agency name, user name, user email address and the SAP ERP ID that end user already has in GRC.	Selected a sample of new HANA users to determine if a Remedy Help Desk Ticket was submitted by the agency.	19 of 45 HANA Analytics users did not have a Remedy Help Desk Ticket.

	ERP Annual Review		
C5.10	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 deviations noted.
C5.11	In the event the 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 the Department's self-service option: DoIT Identity Management Tool.	Reviewed the DoIT Identity Management Website to determine the solutions to reset passwords.	No deviations noted.
C5.12	The IT Service Desk is to verify the individual's ID with the information within the Remedy ticket prior to resetting the password.	Observed the IT Service Desk staff to determine if an individual's identity was verified prior to resetting the password.	No deviations noted.
	Active Directory Password Reset		
C5.13	Active Directory accounts are reset by users calling the IT Service Desk or by one of the Department's self-service options - Microsoft Identity Management (MIM) or the Department's Identity Management (DIM) tool.	Reviewed the DoIT Identity Management Website to determine solutions to reset passwords.	No deviations noted.
C5.14	The IT Service Desk staff will proceed with the reset after verification of two of three pieces of information.	Observed the IT Service Desk staff to determine if an individual's identity was verified.	No deviations noted.
	Novell Password Reset		
C5.15	The IT Service Desk staff will proceed with the reset after verification of two of three pieces of information.	Observed the IT Service Desk staff to determine if an individual's identity was verified.	No deviations noted.

	ERP Password Reset		
C5.16	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 IT Service Desk take incoming call to determine if the required information was provided to reset a password.	No deviations noted.
C5.17	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 deviations noted.
	ERP SAP Firefighter		
C5.18	Access to a Firefighter ID requires a request via GRC and a need statement. The ERP security team will review, approve and submit an email to the requestor stating access has been approved.	Observed ERP security team receive a request for Firefighter ID, review, approve, and submit an approval email.	No deviations noted.
	Mainframe Security		
C5.19	The security software requires an established ID and password to verify the identity of the individual.	Observed security software ID and password was required to access the mainframe environment.	No deviations noted.
C5.20	Security software profiles define the level of access.	Selected a sample of profiles to determine if the profile defined the level of access.	No deviations noted.
C5.21	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 the systems options to determine if password standards had been established.	No deviations noted.

C5.22	Security software passwords are maintained as encrypted values within the system security database.	Reviewed the system options to determine if security software passwords were maintained as encrypted values within the system security database.	No deviations noted.
C5.23	Annually, the Security Software Administrator sends the proxy agencies a listing of security software IDs assigned to the agency for review.	Reviewed the annual proxy agency review of security software IDs to determine if the Security Software Administrator had submitted.	No deviations noted.
C5.24	Monthly, 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.	Selected a sample of monthly reports to determine if the IDs had been disabled.	No deviations noted.
C5.25	The Security Software Administrator runs a weekly violation report which is reviewed for invalid and unauthorized access attempts. The Security Software Administrator contacts the individual or their supervisor to determine the reason for the violation.	Selected a sample of weekly reports to determine if the Security Software Administrator had reviewed and followed up.	1 of 9 weekly violation reports selected was not reviewed by the Security Software Administrator.
C5.26	Semi-monthly, 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.	Selected a sample of semi-monthly reports to determine if the Security Software Administrator had reviewed and revoked individual accounts which had separated.	1 of 8 reports was not reviewed by the Security Software Administrator.
	Midrange Security		
C5.27	In order to access the midrange environment, an ID and password are required.	Observed an AD ID and password were required to gain access to the environment.	No deviations noted.

C5.28	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 the password parameters to determine whether parameters had been established.	No deviations noted.
C5.29	For the period of July and August 2018, the Department performs a monthly review of the Illinois.gov Active Directory accounts and disables accounts which have been dormant for 90 days or more.	Selected a sample of monthly reviews to determine if dormant accounts were reviewed.	No deviations noted.
C5.30	Starting in September 2018, the Department performs a monthly review of the Illinois.gov Active Directory accounts and disables accounts which have been dormant for 60 days or more.	Selected a sample of monthly reviews to determine if dormant accounts were reviewed.	No deviations noted.
	System Administrators-Mainframe		
C5.31	Access to the mainframe operating system configurations is limited to system support staff; system programmers and security software personnel.	Reviewed access rights to the mainframe operating system configurations to determine if access was limited to support staff, system programmers, and security software personnel.	3 of 16 IDs with mainframe administrator privileges no longer required access.
C5.32	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 if appropriate.	No deviations noted.

C5.33	On an annual basis the Security Software Coordinator conducts a review of security software IDS with powerful privileges.	Reviewed documentation to determine if the annual review of IDs with powerful privileges was completed.	No deviations noted.
	System Administrators-Midrange		
C5.34	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 deviations noted.
C5.35	On an annual basis, the Wintel Admin Team conducts a review of the technical accounts to ensure appropriateness.	Inquired with Wintel Admin Team staff.	The annual review of technical accounts had not been conducted. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
	Application Administrators/Programmers		
C5.36	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 deviations noted.
	Common Controls		
C5.37	Mandatory backbone design and configuration standards and guides are defined and maintained.	Reviewed backbone design and configuration standards and guides to determine if they were defined and maintained.	No deviations noted.
C5.38	A security banner services as a security awareness mechanism and is displayed at initial network connection warning of prosecution for unauthorized access.	Reviewed configurations to determine if a security banner was displayed upon initial connection to the network.	The Department did not provide complete and accurate population of devices. For the devices provided, no deviations were noted.

C5.39	Modification to the network is restricted to Department authorized technicians and authorized vendors.	Reviewed individuals with the authority to modify the network to determine if they were authorized.	No deviations noted.
C5.40	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 before network access is granted.	Selected a sample of individuals with authority to modify the network to determine if they were authorized and utilized a Department issued token.	No deviations noted.
C5.41	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.	Selected a sample of individuals with authority to modify the network to determine if they were authorized and utilized a Department issued token.	No deviations noted.
C5.42	Access Control Lists reside on the network device itself and restrict communication to only certain IP addresses or address ranges.	Reviewed configurations to determine if ACLs restrict communications.	The Department did not provide complete and accurate population of devices. For the devices provided, no deviations were noted.
C5.43	Authentication Servers control access through assignment of access right privileges (read only or update) based on Department-defined group profiles.	Reviewed configurations to determine if Authentication Servers controlled access.	The Department did not provide complete and accurate population of devices. For the devices provided, no deviations were noted.

C5.44	Self-monitoring network hardware devices record all events and forwards to multiple logging servers. These servers use filters to automatically generate alerts when a Network Services' configured parameter or condition occurs.	Reviewed hardware devices to determine if they were encoded with filters and if Network Operations Center were reviewing and resolving.	No deviations noted.
C5.45	Network diagrams depict common connectivity configurations.	Reviewed network diagrams to determine connectivity configurations.	No deviations noted.
	Local Area Network		
C5.46	The Department has implemented redundancy in Data Center LANs and at agency locations where technically, fiscally, and operationally feasible.	Review configurations to determine if they have been configured for redundancy.	No deviations noted.
C5.47	Network software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. Network hardware and software generates an email to LAN Services Support staff and a console display alert when a predefined event occurs, or a threshold is reached. LAN staff follow up on these alerts and engage operational teams for resolution as necessary.	Reviewed software configurations to determine if emails and alerts were sent when predefined events or thresholds were reached and that LAN Services Support staff followed up on the alerts.	No deviations noted.
C5.48	Authentication Servers record failed login attempts to the network equipment.	Reviewed configurations to determine if failed login attempts were logged.	No deviations noted.
	Agency Wide Area Network		
C5.49	The Department has implemented last mile redundancy where technically, fiscally, and operationally feasible.	Reviewed configurations to determine if they have been configured for redundancy.	No deviations noted.

C5.50	Network software collects and analyzes operational metrics of devices connectivity, traffic bandwidth, and process utilization. Network hardware and software generates an email to the 24x7x365 Network Operations Center or console display alert when a predefined event occurs, or a threshold is reached. The 24x7x365 Network Operations Center follows up on these alerts and engages operational teams for resolution as necessary.	Reviewed software configurations to determine if emails and alerts were sent to the 24x7x365 Network Operations Center when predefined events or thresholds were reached and the 24x7x365 Network Operations Center followed up on the alerts.	No deviations noted.
C5.51	Authentication servers record failed login attempts to network equipment. Failed attempts automatically generate an email notifications which is forwarded notifications to Network Design & Engineering staff for determination if further action is required.	Reviewed configurations to determine if failed login attempts were logged and if an email notification was sent to Network Design & Engineering staff.	No deviations noted.
C5.52	VPNs provided controlled and trusted connections between devices.	Reviewed VPN configurations to determine if security settings were configured to allow for secure remote connections.	No deviations noted.
C5.53	The Department's Enterprise VPN Standard provides guidance when establishing a VPN connection.	Reviewed the Enterprise VPN Standard to determine if they provided guidance on VPN connections.	No deviations noted.
C5.54	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 was encrypted.	No deviations noted.

	Backbone Wide Area Network		
C5.55	The Department has implemented redundancy between Point of Presence sites where technically, fiscally, and operationally feasible and has also installed fiber optic wave transmission technologies to provide high speed backbone transport services.	Reviewed configurations to determine if they have been configured for redundancy.	No deviations noted.
		Reviewed network diagrams to determine if fiber optic wave transmission technologies have been installed.	No deviations noted.
C5.56	Network software collects and analyzes operational metrics of devices connectivity, traffic bandwidth, and process utilization. Network hardware and software generates an email to the 24x7x365 Network Operations Center or console display alert when a predefined event occurs, or a threshold is reached. The 24x7x365 Network Operations Center follows up on these alerts and engages operational teams for resolution as necessary.	Reviewed software configurations to determine if emails and alerts were sent to the 24x7x365 Network Operations Center when predefined events or thresholds were reached and the 24x7x365 Network Operations Center followed up on the alerts.	No deviations noted.
C5.57	The statistics and threshold metrics are reviewed and recorded monthly.	Selected a sample of monthly statistics and threshold metrics to determined if they were reviewed.	The Department did not provide documentation supporting the review of the statistics and threshold metrics.
C5.58	Authentication Servers record failed login attempts to the network equipment. Failed attempts automatically generate an email notification to Network Design & Engineering staff for determination if further action is required.	Reviewed configurations to determine if failed login attempts were logged and if an email notification was sent to Network Design & Engineering staff.	No deviations noted.

<u>Control Objective 6:</u> Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and deviations, 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	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 AOC to determine if it monitored the environment.	No deviations 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.	1 of 60 Remedy Tickets could not be located.
C6.3 The Daily Shift Report documents the activity conducted on mainframe production systems and incident calls received at the Operations Center.	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 deviations noted.
C6.4 The Operator Shift Change Checklist is completed at the beginning of each shift.	Selected a sample of Operator Shift Change Checklist to determine if they were completed at the beginning of each shift.	No deviations noted.
C6.5 Effective February 1, 2019, Checklists are signed off by Operations Center supervisors.	Selected a sample of Operator Shift Change Checklists to determine if they were signed off by the Operations Center supervisors.	No deviations noted.
Mainframe Environment		
C6.6 The mainframe environment is monitored through the z/OS systems console for errors and issues. Operations Center continuously monitors the system console.	Observed the z/OS system console to determine if the Operations Center staff were continuously monitoring.	No deviations noted.

C6.7	Resource Measurement Facility reports are run daily and monthly.	Selected a sample of Resource Measurement Facility reports to determine if they were ran daily and monthly.	No deviations noted.
C6.8	Performance and capacity monitoring are documented via internal memorandum distributed via email to Enterprise Infrastructure management monthly.	Selected a sample of internal memoranda to determine if they were distributed monthly to Enterprise Infrastructure management.	No deviations noted.
	Midrange Environment		
C6.9	The midrange environment availability and performance is monitored via What's Up Gold.	Observed WUG to determine if availability and performance was monitored.	No deviations noted.
C6.10	SQL database servers use the Idera tool set for additional monitoring. The Idera system alerts have been set up to generate emails to SQL support staff.	Observed Idera to determine if email alerts were sent to the SQL support staff.	No deviations noted.
C6.11	AD Domain Controllers use Microsoft System Center for additional monitoring. System Center alerts have been set up to email alerts to AD support staff.	Observed Microsoft System Center to determine if email alerts were sent to AD support staff.	No deviations noted.
C6.12	The Security Operations Center has established Standard Operating Procedures to assist with the detection, analysis and resolution of intrusions, threats, and incidents.	Reviewed the Standard Operating Procedures to determine if they provide guidance on detection, analysis, and resolution.	No deviations noted.

C6.13	An Incident Report is completed for incidents that are classified as medium or high and are submitted to the Chief Information Security Officer. The Incident Report contains the detail of the threat and its resolution.	Selected a sample of medium and high threat incidents to determine if an Incident Report was completed, contained details of the threat, the resolution, and was submitted to the Chief Information Security Officer.	The Department did not maintain documentation of the Chief Information Security Officer's review for the period of July 1, 2018, through March 31, 2019. 1 of 17 incidents was incorrectly categorized as an incident.
C6.14	Daily the 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.	No deviations noted.
C6.15	The Weekly Activity Report summarizes the incidents noted during the week and a summary of the incidents and resolution are provided to management.	Selected a sample of Weekly Activity Reports to determine if incidents and their resolution were recorded and provided to management.	No deviations noted.
C6.16	The monthly, quarterly, and annually Metric Reports document the statistics on incidents and are provided to management.	Inquired with the Security Operations Center staff.	The Department did not document statistics on incidents monthly, quarterly, or annually in Metric Reports. The Department published the statistics on incidents, via a real time tool, which could be accessed by staff.

<u>Control Objective 7:</u> Controls provide reasonable assurance that the transmission of data between the Department and entities 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	TESTS OF CONTROLS	RESULTS OF TESTS
C7.1	The secure, encrypted transfer of mainframe data is achieved using Secure File Transfer Protocol.	Interviewed staff to determine file transfer protocols.	No deviations noted.
C7.2	The software MoveIt is used to transmit midrange data between servers and applications.	Interviewed staff to determine file transfer protocols.	No deviations noted.
C7.3	MoveIt software sends email alerts for any failures to Department support staff.	Observed MoveIt logs to determine if email alerts were sent to Department support staff.	No deviations noted.
C7.4	Access to MoveIt systems are reviewed on an annual basis by the Department's Information Security specialist.	Reviewed documentation to determine if access to MoveIt was reviewed annually.	No deviations noted.
C7.5	Another option available to valid Illinois.gov users for the secure transmission of data is the file transfer utility 'FileT'.	Observed FileT to determine the security over the transmission of the data.	No deviations noted.
C7.6	This utility (FileT) uses random key generation to access files stored on a server.	Observed FileT to determine if a random key was generated.	No deviations noted.
C7.7	Files (FileT) are automatically purged from the server after 5 days.	Observed FileT to determine if files were automatically purged after 5 days.	No deviations noted.
C7.8	The Department has developed the Data Processing Guide to provide staff with instruction related to their various tasks.	Reviewed the Data Processing Guide to determine if it provided guidance.	No deviations noted.

Control Objective 8: Controls provide reasonable assurance 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	TESTS OF CONTROLS	RESULTS OF TESTS
C8.1 System options have been implemented in order to protect resources and data.	Reviewed system operations report to determine if security options were implemented.	No deviations noted.
C8.2 The System Administrator runs a System Management Facility violation records report week and provides to the Mainframe Software Support manager. As of February 2019, the Mainframe Software Support manager signs off on the violation report.	Inquired with System Adminstrator.	The System Administrator ran and reviewed the System Management Facility report. Additionally, the manager of Mainframe Software Support was provided the systems programmer and high profile user ID report for review. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
C8.3 The Anti-Virus Group pushes daily definitions and other antivirus software updates out.	Reviewed anti-virus compliance reports to determine if definitions and updates were configured.	No deviations noted.
C8.4 The tool automatically pushes daily virus definition files to all systems beginning 8 hours after the definition files are made available from the vendor.	Reviewed tool to determine if the daily virus definition files were pushed out to all system beginning 8 hours after the definition files were made available from the vendor.	The definition files were pushed out to servers beginning six hours after the definition files were available.

C8.5	The Anti-Virus Group has tools to monitor the enterprise computing environment that are out of compliance regarding antivirus definitions.	Reviewed anti-virus compliance reports to determine if devices were monitored.	Of the devices connected on April 4, 2019: 106 of 833 systems were not up-to-date with the latest antivirus version. 112 of 833 systems were not up-to-date with the latest antivirus definitions. 1,273 of 44,244 systems were not up-to-date with the latest antivirus product version. 6,871 of 43,833 systems were not up-to-date with the latest antivirus product version. 190 of 44,934 systems did not have information on the anti-virus software installed.

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	TESTS OF CONTROLS	RESULTS OF TESTS
	Local Area Network		
C9.1	Data Center firewall and switch configurations have incremental backups performed twice a day that are stored at the CCF.	Observed firewall and switch backup schedules to determine if incremental backups were performed twice a day and if the backups were stored at the CCF.	No deviations noted.
C9.2	The configurations stored at the CCF are backed up nightly and stored for a maximum of 60 days at the CCF and the ADC.	Observed the backup schedule to determine if backups were performed nightly and stored at the CCF and the ADC for a maximum of 60 days.	No deviations noted.
	Agency Wide Area Network		
C9.3	Configurations are saved on Syslog servers for one week and backed up remotely on a weekly basis stored at the CCF and/or the ADC.	Observed the backup schedule to determine if configurations were saved to the Syslog server for one week, backed up weekly, and stored at the CCF and/or the ADC.	No deviations noted.
	Backbone Wide Area Network		
C9.4	Configurations are saved on Syslog servers for one week and backed up remotely on a weekly basis stored at the CCF and/or the ADC.	Observed the backup schedule to determine if configurations were saved to the Syslog server for one week, backed up weekly, and stored at the CCF and/or the ADC.	No deviations noted.
	Mainframe		
C 9.5	Data on mainframe systems are backed up daily and weekly utilizing Virtual Tape Technology (Disk Library Management (DLM)).	Reviewed the mainframe backup schedules to determine if backups were performed daily and weekly.	No deviations noted.

C 9.6	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 deviations noted.
C 9.7	The Department has implemented backup policies to assist staff in the event of failures.	Reviewed policies to determine if they provided guidance in the event of failed backups.	No deviations noted.
C 9.8	In the event of a mainframe daily backup job failure, the Operations Center staff records the incident in the Shift Report.	Collaboratively inquired with 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.
C9.9	The next working day, Storage staff review the Shift Report to identify problems, correct and resubmit the failed portion of the backup job.	Collaboratively inquired with Storage 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 9.10	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.	Collaboratively inquired with Storage 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 9.11	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 deviations noted.
C 9.12	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 Enterprise Storage and Backup 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 9.13	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 current replication activity was recorded and tracking the replication outcomes.	No deviations noted.
	Midrange		
C 9.14	Spectrun Protect and Avamar are used to backup the midrange environment.	Observed the Specturn Protect and Avamar to determine if they were used to backup the midrange environment.	No deviations noted.
C9.15	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 deviations noted.
C 9.16	Midrange server backups are performed daily or weekly and are either incremental or full.	Reviewed server backup schedules to determine if they were performed daily or weekly and were either incremental or full backups.	No deviations noted.

C 9.17	Spectrum Protect and Data Protection Advisor automatically generate daily reports indicating the backup status of scheduled jobs from the prior day.	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 deviations noted.
C9.18	These reports are emailed to the Enterprise Storage and Backup group who then investigates the cause of the failures and works to resolve the problem.	Interviewed Enterprise Storage and Backup staff to determine the actions taken to resolve the failures.	No deviations noted.
C9.19	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 is replicated to the ADC.	No deviations noted.
C9.20	The Data Domain storage system generates a daily status report which is emailed to the Enterprise Storage and Backup groups.	Observed the Data Domain to determine if it was configured to send daily reports of the replication status for all scheduled jobs.	No deviations noted.
C9.21	The Data Domain storage system also sends alerts to the Enterprise Storage and Backup group when issues arise that may need additional attention.	Observed the Data Domain configurations to determine if alerts were sent to the Enterprise Storage and Backup group.	No deviations noted.
C9.22	The Data Domain system automatically alert vendor support in the event of hardware to system failures.	Observed the Data Domain configurations to determine if alerts were sent to the support vendor.	No deviations noted.
C9.23	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.	Observed the replication of the Data Domain storage system to determine if it was replicated to the ADC.	No deviations noted.

C9.24	A PowerShell script goes through the production SQL servers and creates a report with the latest backup data and it is sent to the SQL team daily.	Observed the PowerShell script to determine if the status of backups was documented and if the reports were sent to the SQL team daily.	No deviations noted.
C9.25	The SQL team also gets alerts from the SQL servers when backup jobs fail.	Observed the SQL servers configurations to determine if alerts were enabled.	No deviations noted.
C9.26	The SQL team receives alerts from the Idera monitoring software if a database has missed a backup on consecutive nights.	Observed the Idera monitoring software configurations to determine if automatic alerts were enabled.	No deviations noted.
C9.27	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.	Observed the configuration of the Isilon storage device to determine the data stored on it.	No deviations noted.
C9.28	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 deviations noted.
C9.29	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 deviations noted.
C9.30	The Isilon generates a daily report showing successful and failed synchronization attempts with the ADC.	Observed the Isilon storage device configurations to determine if daily reports with the status of replication jobs were generated.	No deviations noted.

C9.31	Enterprise Storage and Backup group investigate failed synchronization attempts until a satisfactory conclusion is reached.	Interviewed Enterprise Storage and Backup staff to determine the actions taken to resolve the failures.	No deviations noted.
C9.32	The Isilon has a call home feature that notifies vendor support. For critical issues, the Isilon call home feature additionally notifies the Enterprise Storage and Backup group.	Observed the Isilon storage device configurations to determine if the call home feature was active.	No deviations 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 protect equipment and facilities that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C10.1	The Department's warehouse physical security is managed by cameras and badge proximity readers that are installed at the front and rear entrances and at the dock doors.	Observed cameras and badge proximity readers at the front and rear entrances at the dock doors.	No deviations noted.
C10.2	Authorized badged individuals may enter the Warehouse or EUC area through swiping of a Velocity badge.	Selected a sample of individuals to determine they were authorized to have access.	No deviations noted.
C10.3	A visitor's log captures who enters the building.	Observed visitors were required to sign the visitor's log.	No deviations noted.
	CCF and Communication Center		
C10.4	For the Department's Communication Center and the Central Computing Facility (CCF), security guard monitor 24x7x365, proximity badge readers located at various interior and exterior entry points, security alarms, and cameras.	Observed security guards, proximity badge readers, security alarms and cameras were present at the CCF and the Communication Center.	No deviations noted.
C10.5	Individuals not registered in the Velocity system (no permanent badge issued) must present proof of identification and sign the visitor register log at the guard station to obtain a visitor badge.	Observed visitors were to present proof of identification and sign the visitor register log in order to obtain a visitor badge.	No deviations noted.
C10.6	Visitors are required to be escorted while in either building.	Observed visitors being escorted while in the buildings.	No deviations noted.

C10.7	For individuals registered in the Velocity system but not having a permanent badge immediately available, guards issue a temporary badge upon proof of identification.	Selected a sample of the Building Admittance Registers to determine if individuals were provided a temporary badge with appropriate access.	No deviations noted.
C10.8	Temporary badges are also issued to vendors once identification has been validated by the facility security guard.	Selected a sample of the Building Admittance Registers to determine if individuals were provided a temporary badge with appropriate access.	No deviations noted.
	CCF		
C10.9	Access to this secured area is limited to a small group of individuals with specific business need and requires special badge permission to exit the elevator or enter through the stairway door.	Selected a sample of individuals with access to the secured area to determine appropriateness of access.	No deviations noted.
C10.10	Surveillance is enhanced with additional cameras and door sensors.	Observed cameras and door sensors were present in the secured area.	No deviations noted.
C10.11	Velocity captures dates, times, and doors when a badge is swiped.	Observed the Velocity Access Control system to determine if it documented the date, time and door an individual entered.	No deviations noted.
C10.12	The Department's process begins with an authorized person submitting a DoIT Badge Request form to HR.	Selected a sample of new employees and contractors to determine if an authorized DoIT Badge Request Form was submitted.	The Department did not provide a listing of individuals who were authorized to submit the DoIT Badge Request Form. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.

C10.13	Valid proof of identity and documentation of a clear background check, performed in the past five years, must be verified prior to badge issuance.	Selected a sample of new employees and contractors to determine if valid proof of identification and documentation of a cleared background check, completed within the past five years, was submitted.	No deviations noted.
C10.14	The form requires entries regarding affiliation of employee, reason for access, badge type, expiration date, and access rights needed.	Selected a sample of new employees and contractors to determine if an approved DoIT Badge Request Form contained entries regarding affiliation of employee, reason for access, badge type, and access rights needed.	The DoIT Badge Request Form for employees did not require the expiration date to be completed.
C10.15	After review and sign-off by an authorized Department approver, a badge is created using Velocity with appropriate access rights assigned.	Inquired with Human Resources staff.	The Department did not provide a listing of individuals who were authorized to approve the DoIT Badge Request Form. Therefore, the Service Auditor was unable to test the operating effectiveness of the control.
C10.16	The badge displays a photo of the individual and an expiration date.	Observed the badge displayed a photo of the individual and an expiration date.	No deviations noted.
C10.17	Badge access is revoked by the Velocity system at badge expiration date or by HR after official notice of separation/termination is provided.	Selected a sample of terminated employees and contractors to determine if their rights had been deactivated upon termination.	No deviations noted.

SECTION V

OTHER INFORMATION PROVIDED BY THE DEPARTMENT OF INNOVATION AND TECHNOLOGY

Department of Innovation and Technology

Corrective Action Plan
(Not Examined)

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

Description of System (DOS) did not include:	Department's Corrective Action Plan
Complementary subservice organizational controls	The Department will update the DOS to include complimentary subservice organizational controls.
Complementary user entity controls	The Department will update the DOS to include a description of controls to comply with complementary user entity controls that are documented in the subservice providers' SOC reports.
DCMS controls monitoring	The Department will work with the Department of Central Management Services (DCMS) and update the DOS to include monitoring controls related to the services provided by DCMS.
Mainframe patching	The Department will update the DOS to chronicle mainframe patching and version updating processes.
Application Lifecycle Management manual.	The Department will update the DOS to reference the Application Lifecycle Management manual.
Badging process	The Department will develop policies or procedures for employees to obtain physical access to Department facilities and update the DOS to include these processes.
Physical access by non-Department employees	The Department will update the DOS to include the process for non-employees to obtain physical access to Department facilities.
Physical access review	The Department will update the DOS to include the process for reviewing physical access to Department facilities and highly secured areas.
SQL backups	The Department will update the DOS to reflect the frequency of missed backups by replacing "consecutive" with a more acceptable frequency value.
Internal meeting frequency	The Department will update the DOS to clarify the frequency of these internal meetings.

Inaccurate Statements in the Description of System (DOS)	Department's Corrective Action Plan
Department did not provide sufficient appropriate evidence to determine the accuracy of the statement that risks from potential and newly discovered vulnerabilities are assessed through interaction with security experts and vendor subscription services.	The Department will update the DOS to clarify how external information is applied to protect State resources.
DOS stated prior to March 2, 2019, vulnerability scans were scheduled monthly; after March 2, 2019, scans were scheduled weekly.	The Department will update the DOS as needed to reflect changes to vulnerability scanning frequency.
DOS stated the ERP Production Support initiated communication through the dedicated email address.	The Department will update the DOS to clarify the communication process that utilizes the dedicated email address.
DOS stated that on July 1, 2017, the Illinois Tollway was added as a user agency.	The Department will verify that for future DOS narratives, any reference to a specific date is accurate.
Department services and performance statistics were previously communicated at the DoIT Daily meetings and the CIO meetings.	The Department will update the DOS as needed to describe the process for Department communication of services and performance statistics.
DOS stated the Department was responsible for the scheduling and monitoring of the backup process.	The Department will update the DOS to clarify the delineation of responsibility between the Department and agencies for scheduling and monitoring backups.
DOS stated the secure, encrypted transfer of mainframe data is achieved using Secure File Transfer Protocol (SFTP).	The Department will update the DOS to reflect how the transfer of secure and encrypted mainframe data is achieved.
DOS stated Authentication Servers record failed login attempts to the network equipment. Logs are reviewed by LAN staff as requested by the Department's Security Operations Center staff and as needed for troubleshooting purposes.	The Department will update the DOS to clarify that the failed login attempts are not monitored and are reviewed on an as needed basis for troubleshooting and security incident investigations.
DOS stated that Once in Remedy, End User Computing (EUC) and the Security Operation Center (SOC) are notified.	The Department will update the DOS to clarify the sequence of internal communication and notification steps in the event a device is lost or stolen.

CTL No.	Department's Corrective Action Plan
CE1.6	The Department will determine if additional viable, practical, realistic controls can be instituted that will compel individuals to meet Department timelines related to performance evaluation submissions.
CE1.7	The Department will determine if additional viable, practical, realistic controls can be instituted that will compel individuals to meet Department timelines related to performance evaluation submissions.
CE1.8	The Department will determine if additional viable, practical, realistic controls can be instituted that will compel individuals to meet Department timelines related to performance evaluation submissions.
CE1.11	The Department will determine if additional viable, practical, realistic controls can be instituted that will compel individuals into completing mandated training and will update employee policy and procedures to apply these controls.
CE1.12	The Department will determine if additional viable, practical, realistic controls can be instituted that will compel individuals into completing mandated training and will update employee policy and procedures to apply these controls.
CE1.13	The Department will examine this isolated occurrence and remind staff of the offboarding process.
C2.1	The Department has corrected the tax rates. The Department will also consult with the data owner agency for transferring responsibility of tax table accuracy from the Department to them.
C3.2	The Department has upgraded to a newer version of the software that caused the inability to produce a population sample. The defect does not appear to exist in the current version of Remedy On Demand. The Department will identify the cause of the omissions and develop a compensating control or oversight action to reduce the occurrence.
C3.3	The Department has upgraded to a newer version of the software that caused the inability to produce a population sample. The defect does not appear to exist in the current version of Remedy On Demand.
C3.4	The Department will update the DOS to reference all relevant change management documentation.
C3.18	The Department will revise its change request review process and will remind staff to ensure all required fields are completed.
C4.1	The Department will update the DOS to reflect changes to operational processes, new terminology, and Remedy upgrades related to the enhanced and more responsive classification of an incident.
C4.2	The Department will move the Remedy development (test) environment to production status that will enable a population of incidents to be provided.
C5.3	The Department will review the offboarding process and update procedures and/or the DOS as necessary.
C5.8	The Department will remind staff regarding proper access procedures.
C5.9	The Department will remind staff regarding proper access procedures.

CTL No.	Department's Corrective Action Plan
C5.25	The Department will continue to improve its current logical access review process to strengthen safeguards over who has access to what resource and will determine if it is operationally and technically feasible to terminate logical and physical access in a more timely manner.
C5.26	The Department will continue to improve its current logical access review process to strengthen safeguards over who has access to what resource and will determine if it is operationally and technically feasible to terminate logical and physical access in a more timely manner.
C5.31	The Department will continue to improve its current logical access review process to strengthen safeguards over who has access to what resource and will determine if it is operationally and technically feasible to terminate logical and physical access in a more timely manner.
C5.35	The Department will update the DOS to clarify: • mainframe administrator privilege account access processes, • mainframe access violation report processes including frequency and who receives the reports, and • frequency of midrange technical accounts reviews (monthly and no longer annually).
C5.38	The Department will determine a process to document when devices to be tested are decommissioned as well as retaining device configurations of those decommissioned devices which will account for the continuous improvement in the delivery of customer services where frequent device changes occur, including those in active status.
C5.42	The Department will determine a process to document when devices to be tested are decommissioned as well as retaining device configurations of those decommissioned devices which will account for the continuous improvement in the delivery of customer services where frequent device changes occur, including those in active status.
C5.43	The Department will determine a process to document when devices to be tested are decommissioned as well as retaining device configurations of those decommissioned devices which will account for the continuous improvement in the delivery of customer services where frequent device changes occur, including those in active status.
C5.57	The Department will update the DOS to clarify the steps associated with network threshold metrics.
C6.2	The Department will remind staff to follow all established procedures.
C6.13	The Department will update the DOS to clarify that events are classified into severity levels and only certain levels are forwarded to the Chief Information Security Officer for notification and awareness. The Department will assess the instructions for categorizing events within the Security Operations Center and clarify if necessary. The Department will also reiterate the definition of an incident and stress the importance of appropriate classification to information security specialists.
C6.16	The Department will clarify the DOS.
C8.2	The Department will update the DOS to clarify roles, responsibilities, reviews, and report titles related to mainframe violation reporting.

CTL No.	Department's Corrective Action Plan
C8.4	The Department will update the DOS to clarify the process, to distinguish the timing difference between server and end-user workstations, and also to indicate that a specific period of time (such as 8 hours) is not 100% possible due to dependence on when the provider first delivers the source file.
C8.5	The Department will continue to improve data protection efforts which includes the transition of user applications from outdated, unsupported devices to newer infrastructure environments where up-to-date software can be installed. The Department will also document procedures outlining when, where, and under what circumstances anti-virus and other protective services are installed on servers and workstations.
10.12	The Department will update the DOS to include the criteria used to determine which individuals are authorized to request physical access for Department workforce members and to submit a badge request form.
10.14	The Department will update the DOS to clarify that for State employees, the badge expiration date is defaulted to an automatic 4 years within the Velocity system and therefore, is not necessary to be manually entered into the badge request form.
10.15	The Department will update the DOS to include the criteria used to determine which individuals are authorized to request physical access for Department workforce members and to submit a badge request form.

Department of Innovation and 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. The Department partnered with Illinois Emergency Management Agency (IEMA)/University of Illinois 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 and Recovery Point Objectives 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 and response plans including network, customer services, incidents and major outages, outline response teams' roles and responsibilities. Disaster Recovery 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 Department's Central Computing facility 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 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. Legacy disaster recovery, along with infrastructure and information system contingency 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, recovery time objectives, prioritized recovery order, confidential data indications, and governing standards (HIPAA, IRS Pub 1075, PII, etc.).

Provided by the Department of Innovation and Technology

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

The Department has contracted with Virtustream to host the ERP. The Department has created a Disaster Recovery (DR) 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 its customer and hosting provider Virtustream. As part of the process the Virtustream team assigns a Project Manager to the DR test to manage the entire process. The Department's ERP Team creates a Change Request internally in SharePoint as well as a Change Request internally in Remedy and a 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's team 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 a service request for incidents that will need to be remedied.

In April 2019, the Department's ERP Team worked with Virtustream to conduct a successful test of the disaster recovery plan and activities.

Department of Innovation and Technology
Storage Loss/Mainframe Outage Summary
(Not Examined)

Mainframe Storage Background and Incident

During migration of VMAX tier 1 storage to new equipment on July 8, 2019, an error resulted in the loss of less than 3% (80 of 3,000 volumes) of data in storage. While determining the cause of the service disruption, mainframe operations were ceased. This event impacted 13 agencies and approximately 800 applications. Most applications and impacted agencies were restored and functional by the morning of July 10; one system remained inoperable but was fully restored on July 13. Migration of additional storage to new equipment is currently paused to review all processes and procedures and ensure we implement any necessary mitigation measures prior to continuing.

SharePoint

At approximately 5:00 pm on July 11, 2019, several new servers were created and assigned IP addresses that were erroneously duplicated. The duplicate IP addresses being assigned caused the outage of nine partner-facing SharePoint web servers impacting eight agencies (including DoIT). The issue was corrected, and sites were available on July 12, 2019.

Provided by the Department of Innovation and Technology

Listing of User Agencies of the Department of Innovation and Technology’s Information Technology Shared Services Systems (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 and Economic Opportunity

11 Department of Corrections

12 Department of Employment Security

13 Department of Financial and 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 the 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 Governors State University

36 Guardianship and Advocacy Commission

37 House of Representatives

Provided by the Department of Innovation and Technology

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 Gaming Board
48 Illinois Independent Tax Tribunal
49 Illinois Labor Relations Board
50 Illinois Law Enforcement Training and Standards Board
51 Illinois Math and Science Academy
52 Illinois Medical District Commission
53 Illinois Power Agency
54 Illinois Prisoner Review Board
55 Illinois Procurement Policy Board
56 Illinois Racing Board
57 Illinois State Board of Investments
58 Illinois State Police
59 Illinois State Toll Highway Authority
60 Illinois State University
61 Illinois Student Assistance Commission
62 Illinois Workers' Compensation Commission
63 Joint Committee on Administrative Rules
64 Judges' Retirement System
65 Judicial Inquiry Board
66 Legislative Audit Commission
67 Legislative Ethics Commission
68 Legislative Information System
69 Legislative Printing Unit
70 Legislative Reference Bureau
71 Legislative Research Unit
72 Northeastern Illinois University
73 Northern Illinois University
74 Office of the Architect of the Capitol
75 Office of the Attorney General
76 Office of the Auditor General
77 Office of the Comptroller

78 Office of the Executive Inspector General
79 Office of the Governor
80 Office of the Lieutenant Governor
81 Office of the State Appellate Defender
82 Office of the State Fire Marshal
83 Office of the State's Attorneys Appellate Prosecutor
84 Office of the Treasurer
85 Property Tax Appeal Board
86 Secretary of State
87 Senate Operations
88 Southern Illinois University
89 State Board of Education
90 State Board of Elections
91 State Charter School Commission
92 State Employees' Retirement System
93 State of Illinois Comprehensive Health Insurance Board
94 State Police Merit Board
95 State Universities Civil Service System
96 State Universities Retirement System
97 Supreme Court Historic Preservation Commission
98 Supreme Court of Illinois
99 Teachers' Retirement System of the State of Illinois
100 University of Illinois
101 Western Illinois University

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

1 Department of Corrections
2 Department of Human Rights
3 Department of Juvenile Justice
4 Department of Military Affairs
5 Department on Aging
6 General Assembly Retirement System
7 Illinois Board of Higher Education
8 Illinois Community College Board
9 Illinois Council on Developmental Disabilities
10 Illinois State Police
11 Illinois Student Assistance Commission
12 Judges' Retirement System
13 Judicial Inquiry Board
14 Office of the Attorney General
15 Office of the Auditor General
16 Office of the State Appellate Defender
17 Office of the State Fire Marshal
18 Office of the State's Attorneys Appellate Prosecutor
19 Sex Offender Management Board
20 State Board of Elections
21 State Employees' Retirement System
22 State Universities Civil Service System
23 Supreme Court of Illinois

Provided by the Department of Innovation and Technology

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

1 Department of Corrections
2 Department of Human Rights *
3 Department of Juvenile Justice
4 Department of Military Affairs
5 Department of Natural Resources (Historic Preservation)*
6 Department of Transportation
7 Department on Aging
8 Illinois Deaf and Hard of Hearing Commission*
9 Illinois Law Enforcement Training and Standards Board*
10 Illinois Prisoner Review Board
11 Office of the Attorney General
12 Office of the State's Attorneys Appellate Prosecutor

**Agency transitioned to ERP during examination period.*

Provided by the Department of Innovation and Technology

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 and Economic Opportunity
10 Department of Financial and Professional Regulation
11 Department of Healthcare and Family Services
12 Department of Human Rights
13 Department of Human Services
14 Department of Innovation and Technology
15 Department of Insurance
16 Department of Labor
17 Department of the 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

Provided by the Department of Innovation and Technology

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 Office of the Architect of the Capitol
60 Office of the Attorney General
61 Office of the Auditor General
62 Office of the Executive Inspector General
63 Office of the Governor
64 Office of the Lieutenant Governor
65 Office of the State Appellate Defender
66 Office of the State Fire Marshal
67 Office of the State's Attorneys Appellate Prosecutor
68 Office of the Treasurer
69 Property Tax Appeal Board
70 Sex Offender Management Board
71 State Board of Education
72 State Board of Elections
73 State Employees' Retirement System
74 State of Illinois Comprehensive Health Insurance Board
75 State Police Merit Board
76 State Universities Civil Service System
77 Supreme Court Historic Preservation Commission
78 Teachers' Retirement System of the State of Illinois

Listing of User Agencies of the Central Time and 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 and Economic Opportunity
7 Department of Financial and Professional Regulation
8 Department of Human Rights
9 Department of Innovation and Technology
10 Department of Insurance
11 Department of Labor
12 Department of the 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

Provided by the Department of Innovation and Technology

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 and Economic Opportunity
7 Department of Financial and Professional Regulation
8 Department of Human Rights
9 Department of Innovation and Technology
10 Department of Insurance
11 Department of Labor
12 Department of the 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

Provided by the Department of Innovation and Technology

Listing of User Agencies of the Enterprise Resource Planning 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 Children and Family Services
7. Department of Employment Security
8. Department of Financial and Professional Regulation
9. Department of Human Rights
10. Department of Human Services – Mabley Mental Health Center
11. Department of Innovation and Technology
12. Department of Insurance
13. Department of Labor
14. Department of the Lottery
15. Department of Natural Resources (Historic Preservation)
16. Department of Public Health
17. Department of Revenue
18. Department of Veterans' Affairs
19. Emergency Management Agency
20. Environmental Protection Agency
21. Executive Ethics Commission
22. Governor's Office of Management and Budget
23. Guardianship and Advocacy Commission
24. Human Rights Commission
25. Illinois Arts Council
26. Illinois Civil Service Commission
27. Illinois Commerce Commission
28. Illinois Council on Developmental Disabilities
29. Illinois Deaf and Hard of Hearing Commission
30. Illinois Educational Labor Relations Board
31. Illinois Gaming Board
32. Illinois Independent Tax Tribunal
33. Illinois Labor Relations Board
34. Illinois Power Agency
35. Illinois Procurement Policy Board
36. Illinois Racing Board
37. Illinois State Toll Highway Authority

Provided by the Department of Innovation and Technology

38 Illinois Workers' Compensation Commission
39 Office of the Executive Inspector General
40 Office of the Governor
41 Office of the Lieutenant Governor
42 Property Tax Appeal Board
43 State Police Merit Board

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 Department of Agriculture
7 Department of Central Management Services
8 Department of Human Rights
9 Department of Labor
10 Department of Military Affairs
11 Department of Veterans’ Affairs
12 Eastern Illinois University
13 Emergency Management Agency
14 Environmental Protection Agency
15 Executive Ethics Commission
16 Governors State University
17 Governor's Office of Management and Budget
18 Guardianship and Advocacy Commission
19 House of Representatives
20 Human Rights Commission
21 Illinois Arts Council
22 Illinois Civil Service Commission
23 Illinois Commerce Commission
24 Illinois Community College Board
25 Illinois Council on Developmental Disabilities
26 Illinois Deaf and Hard of Hearing Commission
27 Illinois Educational Labor Relations Board
28 Illinois Housing Development Authority
29 Illinois Independent Tax Tribunal
30 Illinois Labor Relations Board
31 Illinois Law Enforcement Training and Standards Board
32 Illinois Math and Science Academy
33 Illinois Medical District Commission
34 Illinois Power Agency
35 Illinois Prisoner Review Board
36 Illinois Procurement Policy Board
37 Illinois State Board of Investments
38 Illinois State Toll Highway Authority

Provided by the Department of Innovation and Technology

39 Illinois State University

40 Joint Committee on Administrative Rules

41 Judicial Inquiry Board

42 Legislative Audit Commission

43 Legislative Ethics Commission

44 Legislative Information System

45 Legislative Inspector General

46 Legislative Printing Unit

47 Legislative Reference Bureau

48 Legislative Research Unit

49 Northeastern Illinois University

50 Northern Illinois University

51 Office of the Architect of the Capitol

52 Office of the Attorney General

53 Office of the Comptroller

54 Office of the Executive Inspector General

55 Office of the Governor

56 Office of the Lieutenant Governor

57 Office of the State Appellate Defender

58 Office of the State Fire Marshal

59 Office of the State's Attorneys Appellate Prosecutor

60 Office of the Treasurer

61 Property Tax Appeal Board

62 Secretary of State

63 Senate Operations

64 Southern Illinois University

65 State Board of Education

66 State Board of Elections

67 State of Illinois Comprehensive Health Insurance Board

68 State Police Merit Board

69 State Universities Civil Service System

70 State Universities Retirement System

71 University of Illinois

72 Western Illinois University

ACRONYM GLOSSARY

AD – Active Directory
ADC – Alternate Data Center
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
CHIRP – Criminal History Information Response Process
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
CO – Controlling
CPS – Central Payroll System
CRIS – Comprehensive Rate Information System
CTAS – Central Time and Attendance
DB2 – Database 2
DCMS – Department of Central Management Services
Department – Department of Innovation and Technology
DIM – Department's Identity Management
DLM – Disk Library Management
DoIT – Department of Innovation and Technology
DOS – Description of System
EAA – Enterprise Application & Architecture
ERP – Enterprise Resource Planning
ESXi – Elastic Sky X Integrated
EUC – End User Computing
FBI – Federal Bureau of Investigation
FI – Financial Accounting
FLEET – Vehicle Management System
FM – Funds Management
GL – General Ledger
GOMB – Governor's Office of Management and Budget
GRC – Governance, Risk, and Compliance
GUI – Graphical User Interface
HR – Human Resources
HRIS – Human Resources Information System
ID – Identification
ILCS – Illinois Compiled Statutes

ILTA – Illinois State Toll Highway Authority
IMS – Information Management System
IT – Information Technology
JE – Journal Entry
LAN – Local Area Network
LLC – Limited Liability Company
M&O – Maintenance and Operational
MIM – Microsoft Identity Management
MORT – Major Outage Response Team
MS-ISAC – Multi-State Information Sharing and Analysis Center
OS – Operating System
PAR – Personnel Action Request
PSC – Personal Service Contractor
ROD – Remedy on Demand
SAMS – Statewide Accounting Management System
SAP – Systems, Applications and Products
SOC – System and Organization Controls
SOC – Security Operation Center
SKF – Statistical Key Figure
STIL – State of Illinois
SQL – Structured Query Language
VPN – Virtual Private Network
WAN – Wide Area Network
WBS – Work Breakdown Structure
z/OS – Zero Downtime Operating System
z/VM – Zero Downtime Virtual Machine