STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY

INFORMATION TECHNOLOGY SHARED SERVICES

REPORT ON THE DESCRIPTION OF SYSTEM, SUITABILITY OF DESIGN,
AND OPERATING EFFECTIVENESS OF CONTROLS
FOR THE PERIOD
JULY 1, 2020 THROUGH JUNE 30, 2021

STATE OF ILLINOIS

DEPARTMENT OF INNOVATION AND TECHNOLOGY

TABLE OF CONTENTS

Section I

Section II

Section III

Section IV

Section V

Other Information Provided by the Department of Innovation and Technology

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

Chicago Office:

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

Office of the Auditor General
Frank J. Mautino

INDEPENDENT SERVICE AUDITOR'S REPORT ON THE STATE OF ILLINOIS, DEPARTMENT OF INNOVATION AND TECHNOLOGY'S DESCRIPTION OF ITS INFORMATION TECHNOLOGY SHARED SERVICES SYSTEM AND SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

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 Information Technology Shared Services for the Information Technology General Controls and Application Controls" for the user entities throughout the period from July 1, 2020 to June 30, 2021, (description) and the suitability of the design and operating effectiveness of the State of Illinois, Department of Innovation and Technology's 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 controls and control objectives included in the description are those that management of the State of Illinois, Department of Innovation and Technology believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Information Technology Shared Services system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity 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 entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity 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; NICUSA, Inc., a subservice organization to provide software as a service; Google LLC, a subservice organization to provide a web-based solution; Micro Focus Software, Inc., a subservice organization to provide a project and portfolio management tool; Docusign, Inc., a subservice organization to provide software as a service; Okta, Inc., a subservice organization to provide identity as a service; RiskSense, Inc., a subservice organization to provide vulnerability management system; ServiceNow, Inc., a service organization to provide hosting services; Splunk, Inc., a subservice organization to provide cloud hosting services; and Salesforce, Inc., a subservice organization to provide hosting services and 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., NICUSA, Inc., Google, LLC, Micro Focus Software, Inc., Docusign, Inc., Okta, Inc., RiskSense, Inc., ServiceNow, Inc., Splunk, Inc., and Salesforce, Inc. The description also indicates that certain control objectives specified by the State of Illinois, Department of Innovation and Technology can be achieved only if complementary subservice organization 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 the related controls at the State of Illinois, Department of Innovation and Technology. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information about the corrective action plan, business continuity and disaster recovery, and user entity 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 entities during the period from July 1, 2020 to June 30, 2021. Information about the State of Illinois, Department of Innovation and Technology's corrective action plan, business continuity and disaster recovery, and user entity listings have 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 these items.

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, 2020 to June 30, 2021. We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified 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 its assertions.

Inherent Limitations

The description is prepared to meet the common needs of the user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each user entity 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 controls and application controls 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.

Controls That Did Not Operating During Period

1) As indicated in the accompanying description of the State of Illinois, Department of Innovation and Technology, the Department did not have a request for a new system administrator during the examination period; therefore, we did not perform any test of design or operating effectiveness of controls related to 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."

2) As indicated in the accompanying description of the State of Illinois, Department of Innovation and Technology, the Department did not encounter failed backups during the examination period; therefore, we did not perform any test of 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."

Basis for Qualified Opinion

Our examination disclosed:

1) The State of Illinois, Department of Innovation and Technology states in its description that it has controls in place to ensure appropriate federal and state tax rates are utilized in the Central Payroll System. However, as noted at page 43 of the description of tests of controls and results, federal and state tax rates were not always accurate. As a result, controls were not operating effectively to achieve the control objective, "Controls provide reasonable assurance that appropriate federal and state specifications are used for tax calculations during processing, that are relevant to user entities' internal control over financial reporting."

2) The State of Illinois, Department of Innovation and Technology states in its description that it has controls in place for changes with significant or extensive impact to require test, implementation and backout plans. In addition, approval is required prior to being placed into production. However, as noted at pages 44 and 45 of the description of tests of controls and results, test, implementation and backout plans were not consistently provided. Additionally, approvals prior to being placed into production were not consistently obtained. As a result, controls were not operating effectively 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."

3) The State of Illinois, Department of Innovation and Technology states in its description that physical access is deactivated after official notice of separation or termination. However, as noted at page 49 of the description of test of controls and results, documentation demonstrating the terminated individuals' access badges was deactivated could not be provided. As a result, controls were not operating effectively to achieve the control objective "Controls provide reasonable assurance that physical access to facilities and data centers is restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting."

4) The State of Illinois, Department of Innovation and Technology states in its description that it has controls in place to require access modifications to the State of Illinois, Department of Innovation and Technology's resources begins with the submission of a Remedy service request approved by an Agency Technology Service Requestor. However, as noted at page 51 of the description of tests of controls and results, a population of Active Directory access modifications to the State of Illinois, Department of Innovation and Technology's resources could not be provided. As a result, controls were 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."

5) The State of Illinois, Department of Innovation and Technology states in its description that it has controls in place to require security software access modifications to the State of Illinois, Department of Innovation and Technology's mainframe resources begin with the submission of a Remedy service request or Mainframe Request. However, as noted at page 54 of the description of tests of controls and results, a population of security software access modifications to the State of Illinois, Department of Innovation and Technology's mainframe resources could not be provided. As a result, controls were 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."

In our opinion, except for 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 fairly presents 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, 2020 to June 30, 2021.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period from July 1, 2020, to June 30, 2021; and subservice organizations and user entities applied complementary controls assumed in the design of the State of Illinois, Department of Innovation and Technology's control throughout the period July 1, 2020 to June 30, 2021.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period from July 1, 2020 to June 30, 2021 if complementary subservice organization and user entity controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls operated effectively throughout the period July 1, 2020 to June 30, 2021.

Emphasis of Matter

As noted in the Description of the Information Technology Shared Services for the Information Technology General Controls and Application Controls, effective March 21, 2020, the Governor of the State of Illinois signed Executive Order 2020-10 requiring all individuals currently living within the State of Illinois to stay at home or at their place of residence, as a result of the global pandemic related to the COVID-19 outbreak. The Description of the Information Technology Shared Services for the Information Technology General Controls and Application Controls documents the changes to the Department's internal controls due to the requirements of Executive Order 2020-10.

The opinion was not modified as a result of this matter.

Other Reporting Required by Government Auditing Standards

In accordance with *Government Auditing Standards*, we have also issued our report dated August 4, 2021, 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, 2020 to June 30, 2021, 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, 2020 to June 30, 2021 (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 State of Illinois, Department of Innovation and Technology, user entities of the State of Illinois, Department of Innovation and Technology's Information Technology Shared Services system during some or all of the period from July 1, 2020 to June 30, 2021, and their auditors who audit and report on such user entities' 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 entities themselves, when assessing the risks of material misstatement of user entities' 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
Principal of IS Audits

August 4, 2021
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
Jennifer Ricker, Acting Secretary

Honorable Frank J. Mautino
Auditor General, State of Illinois

We have prepared the description of the State of Illinois, Department of Innovation and Technology's information technology general controls and application controls system entitled "Description of the Information Technology Shared Services for the Information Technology General Controls and Application Controls" throughout the period from July 1, 2020, to June 30, 2021, (description) for user entities of the system during some or all of the period from July 1, 2020, to June 30, 2021, and their auditors who audit and report on such user entities' 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 entities of the system themselves when assessing the risks of material misstatements of user entities' financial statements.

The State of Illinois, Department of Innovation and Technology uses subservice organizations to provide building maintenance activities of Department occupied facilities, hosting services, software as a service, identity as a service, vulnerability management system, web-based solution, project and portfolio management tool, and an alternate data center. 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 subservice organizations. The description also indicated that certain control objectives specified in the description can only be achieved if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity 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. The description does not extend to controls of the user entities.

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

1. The description fairly presents the Information Technology Shared Services system made available to user entities of the system during some or all of the period July 1, 2020, to June 30, 2021, for the information technology general controls and application controls as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    a. Presents how the system made available to user entities 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 entity controls and complementary subservice organization 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 system, while acknowledging that the description is prepared to meet the common needs of the user entities 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 entity 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, 2020, to June 30, 2021, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls throughout the period from July 1, 2020, to June 30, 2021. 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. We state on page 22 of the description that controls are in place to ensure appropriate federal and state tax rates are utilized in the Central Payroll System. However, the federal and state tax rates were not always accurate. As a result, controls were not operating effectively to achieve the control objective, "Controls provide reasonable assurance that appropriate federal and state specifications are used for tax calculations during processing, that are relevant to user entities' internal control over financial reporting."

b. We state on page 25 of the description that controls are in place for changes with significant or extensive impact to require test, implementation and backout plans. In addition, approval is required prior to being placed into production. However, test, implementation and backout plans were not consistently provided. Additionally, approvals prior to being placed into production were not consistently obtained. As a result, controls were not operating effectively 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."

c. We state on page 33 of the description that controls are in place for physical access to be deactivated after official notice of separation or termination. However, documentation demonstrating the terminated individuals' access badges was deactivated could not be provided. As a result, controls were not operating effectively to achieve the control objective "Controls provide reasonable assurance that physical access to facilities and data centers is restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting."

d. We state on page 26 of the description that controls are in place to require access modifications to the State of Illinois, Department of Innovation and Technology's resources begins with the submission of a Remedy service request approved by an Agency Technology Service Requestor. However, a population of Active Directory access modifications to the State of Illinois, Department of Innovation and Technology's resources could not be provided. As a result, controls were 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."

e. We state on page 28 of the description that controls are in place to require security software access modifications to the State of Illinois, Department of Innovation and Technology's mainframe resources begin with the submission of a Remedy service request or Mainframe Request. However, a population of security software access modifications to the State of Illinois, Department of Innovation and Technology's mainframe resources could not be provided. As a result, controls were 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.”

SIGNED ORIGINAL ON FILE

Jennifer Ricker
Acting Secretary
Department of Innovation and Technology
August 4, 2021

SECTION III

DESCRIPTION OF THE INFORMATION TECHNOLOGY SHARED SERVICES FOR THE INFORMATION TECHNOLOGY GENERAL CONTROLS AND APPLICATION CONTROLS

Description of the Information Technology Shared Services for the IT General Controls and Application Controls

Overview of the Department of Innovation and Technology

The Department of Innovation and Technology (Department) was initially created under Executive Order 2016-01, and statutorily created in the Department of Innovation and Technology Act (Act) (20 ILCS 1370). The Department delivers statewide technology, innovation and telecommunication services to state government agencies, boards and commissions as well as policy and standards development, lifecycle investment planning, enterprise solutions and privacy and security management.

The Department's mission is to empower the State of Illinois through high-value, customer-centric technology by delivering best-in-class innovation to client agencies, fostering collaboration and empowering client agencies to provide better services to residents, businesses and visitors while maximizing the value of taxpayer resources.

The Department manages the Illinois Century Network (ICN), a service that creates and maintains high speed telecommunications networks providing reliable communication links to and among Illinois schools, institutions of higher education, libraries, museums, research institutions, state agencies, units of local government and other entities that provide service to Illinois residents.

Subservice Organizations

In accordance with the criteria in management's assertion, this Description excludes the controls of the Department's subservice organizations. A list of the subservice organizations in scope and the activities performed are provided in the table below:

Subservice Organization	Subservice Organization Description
The Department of Central Management Services (DCMS)	Provides building maintenance activities of Department occupied facilities.
BMC Software, Inc.	Provides hosting services for the Department's service management tool, Remedy On Demand.
Docusign, Inc.	Provides a cloud-based software as a service for managing the Department's electronic agreements.
Google, LLC	Provides a web-based software as a service solution.
Microsoft, LLC	Provides cloud hosting services related to the production environment.
Micro Focus Software, Inc.	Provides a project and portfolio management tool.
NICUSA, Inc.	Provides hosting services and a web-based Statewide Permits and Licensing Solution.
Okta, Inc.	Provides a cloud-based service for the Department's identity and access management.
RiskSense, Inc.	Provides a cloud-based service for risk-based vulnerability management.
Salesforce, Inc.	Provides hosting services and a web-based solution.
ServiceNow, Inc.	Provides a cloud-based service for managing the Department's Information Technology services, including

	help desk ticketing services.
Splunk, Inc.	Provides hosting services and a web-based interface for the Department data analytics.
Zayo Group LLC	Provides an alternate data center for off-site data storage and replication of the production environment.

Overview of Service 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 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.

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.

The Department's internal control components include controls that may have a pervasive effect on the organization, specific processes, account balances, disclosures, classes of transactions, or applications. Some of the components of internal control have more of an effect at the entity level, while other components are primarily related to specific processes or applications.

Control Environment

The Department's organizational hierarchy supports internal controls 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, two individuals have served in this capacity, one as Secretary through September 4, 2020, and one as Acting Secretary beginning September 5, 2020 to present.

The Assistant Secretary (vacant effective March 16, 2021) directly supervises the Group Chief Information Officers (CIOs) and applies primary focus on application development and technology delivery.

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, Chief Data Officer, Enterprise Resource Planning (ERP) Program Director, and seven 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 from July 1, 2020 to March 31, 2021) consults with the Secretary and senior management to facilitate functional compatibility and alignment of Department objectives. Subordinate managers oversee the Department's Legal Services (through December 15, 2020 when it moved to the Chief of Staff's supervision effective December 16, 2020), Human Resources, Procurement and Property Control.

The Chief Internal Auditor (vacant from September 29, 2020 to February 15, 2021) directs and manages the Department's internal audit program which validates compliance with the Fiscal Control and Internal Audit Act and verifies consistency with the Department's mission, program objectives, and regulatory statutes. In addition, internal audit operations identify and evaluate significant risk exposures and contribute to the improvement of the Department's overall control environment.

The Chief Information Security Officer (CISO) is responsible for strategies, policies, standards, processes, and assessments that promote protection over the Department's assets and reduce cyber risks. This includes development of a cybersecurity program that provides risk identification, mitigation, analysis, and resolution advice to the Department and to agencies. The CISO manages protective services of encryption, recovery, monitoring controls, incident detection, and response.

The Chief Service Officer (vacant from July 1, 2020 to present) 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.

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, communications and General Counsel (reporting structure moved here effective December 16, 2020).

The Chief Enterprise Architect develops and designs the enterprise architecture, sets priorities, and ensures projects are aligned to the Department's mission, long-term strategic goals, and business objectives.

The Chief Technology Officer is responsible for building the Department's strategy for future technology innovations as well as for managing business functions covering infrastructure, applications, network, software distribution and the delivery of customer-facing IT services, customer support, and change control. Each of these business functions have been assigned separate managers.

The Chief Data Officer (Acting October 16, 2020 through April 15, 2021, and filled effective April 16, 2021) reports to the Secretary and serves as a principal strategist and advisor. As a policy-making official, the Chief Data Officer sets and manages open government data effort including how the State of Illinois offers Application Program Interfaces (APIs) and creates public data products; implements big data strategy to create a statewide culture that is more data- and analytics-driven to better serve State of Illinois constituents; drives an evolving use of emerging technologies to support the best process for increased data availability.

The ERP Program Director (vacant from February 12 through March 9, 2021) is responsible for directing, planning, developing, administrating, and implementing the Statewide ERP program. For participating agencies, the ERP provides consolidated management over financial services.

The seven 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 (through March 31, 2021 at which time the name of the group was clarified to reflect health and human services effective April 1, 2021); (2) government and public employees; (3) business and workforce; (4) natural and cultural resources; (5) public safety (vacant March 1, 2021 to present); (6) education; and (7) transportation. The Transportation Group CIO position has not yet been filled.

Human Resources (HR)
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, the Governor's Comprehensive Employment Plan (CEP) For Agencies under the Jurisdiction of the Governor, and applicable state/federal laws.

Workforce members are categorized into 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.

The Department's organizational chart documents the organizational structure, reporting lines, authorities and responsibilities. The organizational chart is reviewed at least annually; however, it is updated when structure changes, position establishments, and position abolishment occur. Each State employee position (job protected or at will) is identified on the organizational chart. Each State employee's duties, responsibilities, qualifications, minimum acceptable competency education requirements, experience levels, preferred qualifications and specialized skills for each position are defined in written job descriptions (CMS104).

New employee and Personal Service Contractors (PSC) must pass applicable background checks prior to being offered employment.

Annually, performance evaluations are completed. Additionally, for employees' service probationary periods, performance evaluations are completed at varying intervals.

- Four-month probationary period, performance evaluations are completed two weeks prior to the end of the probationary period.
- 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.

Newly-hired employees are provided the DCMS Policy Manual during New Employee Orientation. They are required to sign an acknowledgment form stating the individual is bound to act in accordance with the DCMS Policy Manual and all updates provided or be subject to discipline, up to and including discharge. New Employee Orientation is being conducted virtually due to COVID-19 remote work directives.

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 the "Contract Employee agrees to be bound by and comply with policies and procedures of the Agency."

Newly-hired employees and PSCs are required to complete an acknowledgement of participation form for each of the following required trainings within 30 days of hire:

- Harassment and Discrimination Prevention Training as required by the State Officials and Employees Ethics Act (5 ILCS 430/1).
- Illinois Department of Revenue, Information Safeguarding Training regarding the protection of Federal Tax Information (FTI).
- Ethics Training Program for State of Illinois Employees and Appointees.
- Security Awareness Training as required by the Illinois Data Security on State Computers Act (20 ILC 450/25).

In addition, newly-hired employees and PSCs are provided the Acceptable Use Policy and are required to complete the Acceptable Use Policy Certification stating the individual will comply with the State's policies and regulations. This Acceptable Use Policy Certification is completed once, at the time of hire.

Note: a retired Department employee retained via 75-day appointment with less than a thirty (30) day break in service is not considered to be a "new" employee for purposes of background checks, new employee orientation and training.

Annually, employees and PSCs are required to complete the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training Program for State of Illinois Employees and Appointees, and Security Awareness Training via paper or OneNet and complete the acknowledgement of participation.

Risk Assessment Process

The Department has established a Risk Management Program (RMP) to offer guidelines on how to reduce risk across the enterprise. The RMP includes several components that leverage the National Institute of Standards and Technology (NIST) framework as a foundation. NIST provides a comprehensive series of technical and non-technical (i.e., administrative) controls that act as safeguards and countermeasures prescribed to protect the confidentiality, integrity, and availability of data and information systems.

In addition, the Department receives threats, vulnerability, and incident intelligence from multiple sources, including the MS-ISAC and the Illinois Statewide Terrorism and Intelligence Center. Risks from potential and newly discovered vulnerabilities are assessed through interaction with Department's security staff and vendor subscription services. The Department also maintains contact with vendors to receive vulnerability information.

An Enterprise Information Security Risk Assessment Policy has been published on the Department's website.

The Department conducts risk assessment for each agency based on the RMP. For the RMP to be effective, it is a team effort involving the participation and support of key stakeholders of the organization who interact with State of Illinois data and information systems. To ensure the accuracy of the results, the respondent must have an intimate knowledge of processes relative to applications and day-to-day business operations. The Organization Risk Assessment Questionnaire (ORAQ) is designed to gain an overall holistic view of the organization.

Risks and mitigation plans are captured and tracked in the Department's risk register. The risk register is a repository of risk information including but not limited to date identified, agency impacted, data containing a description of the risk, mitigation strategies, risk owners, and risk response. The Department conducts quarterly mitigation plan follow-up review to keep track of progress until mitigation plans are completed.

Managerial, operational and technical changes are discussed during the risk assessment process.

Information and Communication
The Department's website delivers information to client agencies and to Department staff covering:

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

The Department has implemented various policies and procedures relevant to security. The Department has published its security policies and procedures on its website. The policies located on the Department's website include:

Acceptable Use Policy
Access Control Policy
Accountability, Audit, and Risk Management Privacy Policy
Audit and Accountability Policy
Awareness and Training Policy
CJIS Security Supplemental Policy
Configuration Management Policy
Contingency Planning Policy

Data Minimization and Retention Privacy Policy
Data Quality and Integrity Privacy Policy
FTI Supplemental Policy
Identification and Authentication Policy
Individual Participation and Redress Privacy Policy
Information Security Incident Management Policy
Media Protection Policy
Overarching Enterprise Information Security Policy
PCI Data Security Policy
Personnel Security Policy
PHI Supplemental
Physical and Environmental Protection Policy
Privacy Security Policy
Program Management Policy
Risk Assessment Policy
Security Assessment and Authorization Policy
Security Planning Policy
System and Communication Protection Policy
System and Information Integrity Policy
System and Services Acquisition Policy
System Maintenance Policy
Transparency, Authority, and Purpose Privacy Policy
Use Limitation Privacy Policy
Identity Protection Policy
Mobile Device Security Policy
Wireless Communication Device Policy

The Department enterprise information security policies are reviewed every three years or more frequently when significant changes to the environment warrant an update. The reviews are conducted by the Governance, Risk and Compliance (GRC) Group. The Department's Division of Information Security is responsible for ensuring the Department's compliance with enterprise information security policies.

The website also provides links to the DoIT Digest content, which informs the reader of new initiatives, business applications, ongoing projects, administrative information, and Departmental news.

Internal Communication

Department internal staff are kept informed through multiple sources such as the Department's website, the Employee Portal (intranet), and emails. Direct email communications also alert workforce members to technical, security, and other concerns such as outages.

Due to COVID-19 and State employees working remotely, Remote Work Reminders are published on the Employee Portal when there is remote work news or information to share to facilitate work from home. A Remote Work webpage was published on the Department's website to provide guidelines and additional resources to support employees working remotely.

External Communication

In addition to the Department's website, client 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, Telecom Coordinators, Agency Technology Service Requestors (ATSR)) documenting new services/processes/outages/etc. Group CIOs discuss with agency leadership personnel relevant subjects that may include significant events, service issues, improvements, processes, and strategic goals. Group CIOs meet with agency CIOs when business needs require 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 and support staff are invited to attend "DoIT Daily" meetings (Mondays through Fridays). DoIT Daily is a forum to share high-level and high-risk operational issues with a team equipped to discuss steps for resolution.

Monitoring Activities

The Audit Committee assists the Secretary in fulfilling their responsibilities for effectively and efficiently managing and maintaining an effective system of internal control. The Audit Committee consists of the Assistant Secretary, Chief of Staff, Chief Administrative Officer, and General Counsel. The primary function of the internal Audit Committee is to assist the Secretary in fulfilling oversight and reporting responsibilities by reviewing the findings of internal and external audit reports and monitoring agency progress on remediating findings. The Committee is to meet four times per calendar year, with the authority to convene more frequently if requested.

Internal Audit provides the Department independent, objective assurance and consulting services by performing risk assessment exercises to create the annual audit plan. Furthermore, internal audit performs system pre-implementation reviews to evaluate system controls. External and internal audits' results are communicated to senior management, and management response is documented. The Chief Internal Auditor annually submits a written report to the Department's Secretary detailing the audit plan including internal audit significant findings, and the extent to which recommended changes were implemented.

Customer Support Division staff conducts quarterly meetings, with the authority to convene more frequently if requested, inviting representatives from appropriate Department teams to discuss performance metrics for team awareness. Critical and high level Remedy tickets that did not meet the performance metrics are discussed for potential service improvement going forward. In addition to storing data on a SharePoint site, service level metrics showing the Department's customer service performance are posted on the Department's website.

Numerical cross-references are used to reference controls in Section III to the related control and testing in Section IV.

Scope of the Description of Services and Applications in Scope

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, BMC Software, Inc., DocuSign, Inc., Microsoft, LLC, Micro Focus Software, Inc., NICUSA, Inc., Google, LLC, Okta, Inc., RiskSense, Inc., Salesforce, Inc., ServiceNow, Inc., Splunk, Inc., and Zayo Group, LLC.

The Description is intended to provide information for the agencies and their independent auditors to understand the systems and controls in place for the Department's IT General Controls and Application Controls that are 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) 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; and
- eTime hosted on the Department's midrange, server environment.

Agencies are responsible for the complete and accurate entry and maintenance of data into the applications. The Department is responsible for application updating and maintenance. Separate, stand-alone user manuals and guides are available for the AIS, CPS, and CTAS applications. (*C1.2*) User instructions and guides are imbedded into the application itself for eTime. (*C1.3*) 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. (*C1.1*) Various reports are generated, based on the application, to assist with data integrity and reconciliation.

Accounting Information System

AIS functions include accounts payable, appropriation management, fund transfer and adjustment, vendor management, contract and contract amendment. AIS also tracks expenditures from the initial receipt of the invoice, throughout the production of vouchers, and updates the records with payment information once processed by the Office of Comptroller. AIS also provides both project and cost center accounting.

Transaction records allocate financial information into sub accounts according to the Office of 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 bureau and accounting 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 Comptroller. In addition, the agencies can print the AIS13 for review.

AIS allows agencies to issue refunds/credits and 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 interacts with the following applications and systems:

- ALS - Auto Liability System;
- ARPS - Accounts Receivable Posting System;
- CPS - Central Payroll System;
- CRIS - Comprehensive Rate Information System;
- ERP – Enterprise Resource Planning; and
- Office of Comptroller systems.

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 Comptroller for warrant generation. In addition, CPS sends an electronic file of the vouchers to the Office of Comptroller.

In the event the payroll is rejected by the Office of 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 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. *(C2.1)*

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 on the screen. Appropriate action is taken to either correct an error by the Department or agency payroll administrator by entering the correct value or to request the addition of a State identifier by the Department or agency payroll administrator working with Office of Comptroller. After the Office of Comptroller confirms the addition, the technical Payroll manager follows the Department change management process to have a change made in the application.

On an annual basis, CPS staff research tax rates for CPS-recognized states and update state tax tables accordingly. *(C2.2)*

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.

Reports are available to assist agencies in processing payroll.

CPS interacts with the following applications and systems:

- AIS;
- Enterprise Resource Planning (ERP) system; and
- Office of Comptroller systems.

Central Time and Attendance System

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. For agencies using only CTAS, timekeepers have the responsibility for entry and maintenance of an employee's time and attendance.

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.

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.

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

<u>eTime</u>

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, time reports and overtime requests. For agencies using eTime, timekeepers have the responsibility for adjustments of an employee’s time and attendance.

Specific eTime roles and access privileges are defined in the application access provisioning section.

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/delegate 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/delegate 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.

Infrastructure

<u>Midrange</u>

The Department’s midrange configuration consists of physical and virtual devices. These midrange devices host the various services the Department offers. 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.
- [redacted]r 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.

<u>Mainframe</u>
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 [redacted] 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, 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 [redacted] which is a database software system.

Information Technology General Controls

<u>Change Management- Infrastructure</u>
Control over changes to the network, mainframe, mainframe patching, 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. (*<u>C3.1</u>*) z/OS production systems are updated quarterly and when patches become available, all other mainframe software components (IMS, CICS, DB2, ISV, etc.) are updated. (*<u>C3.2)</u>*

Remedy On Demand is the Department's control mechanism over changes to Department resources. 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.

Changes with a significant or extensive impact require test, implementation, and back out information be provided within the change request. (*C3.3*) Change requests are classified into class and impact categories with the level of approval is based on the assigned impact. Approval is required prior to being placed into production. (*C3.4*)

In the event of an emergency, only verbal approval by a supervisor is required to begin remediation. Remedy documentation is finalized once the emergency has subsided. Emergency changes require a Post Implementation Review be provided within the change request. (*C3.5*)

The Department follows the Server Patch Management procedures for receiving and deploying Microsoft Windows patches monthly. *(C3.6)* The patches are first tested with the technical staff, a pilot group, and then pushed out to the general population. The Department utilizes [redacted] to push and monitor Windows patches after obtaining approval. *(C3.7)*

The Department follows the applicable patching procedures for the Linux, VMware and Unix (AIX) patches which are implemented when provided by the vendor. (*C3.8*) The patches are reviewed and tested by technicians and follow the Department's change management process. (*C3.9*)

Change Management - Applications

For application changes, processing steps are documented in Application Lifecyle Management Manual, EAA Mainframe Change Management Procedures and the EAA Distributed Change Management Procedures. (*C3.10*) Changes are controlled via Remedy.

An application change is initiated with the submission from an authorized ATSR, or Department IT Coordinator, or internal support staff. 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. (*C3.11*) Developers attach the Move Sheet to the corresponding change request record within Remedy. Supervisory approval is required before Remedy releases the activity to the Library Services group who performs the move into production. (*C3.12)* Moves to the mainframe production environment are completed by Library Services based on the instructions within the Move Sheet. (*C3.13*) Developers are limited to read only access to the Production Libraries. (*C3.14*)

For distributed systems, supervisory approval is required prior to deployment into the production environment. *(C3.15)* Designated release staff, who did not code the change, move the change into the production environment manually, and developers who coded the changes verify the changes to ensure accuracy, or via an automated release management module if configured, with supervisor approval. *(C3.16)*

Logical Access

In order to access the State's information technology environment, an Active Directory ID and password are required. (*C5.1*) Password security parameters have been established and configured to ensure access to resources is appropriate:

- Minimum password length;
- Password complexity;
- Password history;
- Minimum password age; and
- Number of invalid login attempts. (*C5.2)*

The Department is in the process of moving from Active Directory Federal Services (ADFS) to Okta Single SignOn (SSO). As of June 30, 2021, half of the agencies' applications have been moved to Okta SSO. ADFS and Okta SSO utilize the same Active Directory credentials, in addition to two-factor authentication. (*C5.48)*

Access Creation, Modification, and Revocation

Access creation or modification to Department resources (users and administrators) requires the submission of a Remedy service request from a Remedy submitter or an authorized Agency Technology Service Requestor (ATSR). (*C5.3*) Only ATSR can approve the request, and the IT Service Processing team assigns Remedy tasks to support groups to satisfy the request.

For voluntary separations of an employee or a contractor, an Employee Exit form and a Remedy service request are completed to initiate and ensure the removal of access and the retrieval of equipment. (*C5.4*)

Revoking access to Department resources is initiated upon receipt of a Remedy service request or under special or emergency circumstances, network access is disabled at the instruction of the Department senior management. (*C5.5*) A Remedy service request is created by the ATSR or Remedy submitter after the special or emergency access revocation has occurred. The Department does not have a time frame for ensuring the access is revoked timely.

Password Resets

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. (*C5.6*) 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 their password via this method. If they are unsuccessful, have not previously registered or are not eligible to use MIM/DIM, IT Service Desk staff will create a Remedy ticket. The IT Service Desk staff will then proceed with the reset after verification of two of three pieces of information; phone number, email address and physical address. (*C5.7*) Once a successful reset has taken place, users will be instructed to either register or re-register for MIM/DIM if eligible.

Reviews

On an annual basis, the Department's Security Compliance team sends a list of the technical accounts to appropriate supervisors. (*C5.8*) The supervisor of the technical account owner is requested to review and update continued access. In the event the technical account is no longer required, a Remedy ticket is submitted by the immediate supervisor or their designee to remove the account. Additionally, accounts with 60 days of inactivity are disabled.

The Department performs a monthly review of Illinois.gov Active Directory accounts and disables accounts which have been dormant for 60 days. (*C5.9*) Account deletion is processed upon receipt of the Remedy request.

Administrative Access

Department staff and vendors with a business need to access or modify network devices are added to a designated Active Directory access group (for role based and least privileges) and setup with a two-factor authentication token. (*C5.10*)

Once the supervisor request for multifactor authentication is received by the two factor administrators, administrators will work on assigning and configuring the two factor authentication with the end user. Two factor authentication activation and revocation is tracked by the individual supervisor.

Tokens serve as a secondary confirmation and in conjunction with validated AD credentials. If the AD account is disabled or deactivated, the token is rendered ineffective and useless for authentication purposes. Token remains 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.

Mainframe Resources

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. (*C5.11*) The primary means of defining an individual's level of access is the security software profile. (*C5.12*)

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. (*C5.13*)

Additionally, the security software passwords are maintained as encrypted values within the system security database. (*C5.14*)

Agencies with a Security Software Coordinator are responsible for the maintenance, monitoring and review of their agencies' security software IDs. The Department's Security Software Coordinator is responsible for the maintenance, monitoring and review of security software IDs for agencies who do not have a Security Software Coordinator (proxy agencies).

Mainframe Access Creation, Modification and Revocation

For the creation and modification of a security software account, agencies are responsible for the submission of an approved service request or Mainframe Request Form if Remedy service request is not available for the agency. Once the Remedy service request is created, or Mainframe Request Form is submitted, the Department's Software Security Coordinator will receive the Remedy ticket, and follow the Security Software ID Creation procedures to create an account as specified. (*C5.15*)

On an annual basis, the Department's Security Software Coordinator sends proxy agencies and the Department a listing of security software IDs assigned to their agency and the Department for review. (*C5.16*) The agencies and the Department are to review the listing and provide a response back to the Department's Security Software Coordinator stating the IDs are appropriate or indicating which IDs are to be revoked, re-assigned or deleted. Additionally, on a monthly basis, the Department's Security Software Coordinator or designee runs a report documenting the Department and the proxy agencies' security software IDs which have not been utilized in the past 90-days; upon review, the IDs are revoked. (*C5.17*)

The Department's Security Software Coordinator or designee runs a weekly violation report which is reviewed for invalid and unauthorized access attempts of the Department and proxy agency security software IDs. The Department's Security Software Coordinator follows up with the review results as stated in the Security Violation Report Procedure. The Department's Security Software Coordinator or designee contacts the individual or their supervisor to determine the reason for the violation. (C5.18)

Semi-monthly, the Department's Security Software Coordinator receives a separation report documenting the separations for the month. The Department's Security Software Coordinator or designee reviews the separation reports, noting separation of individuals from the Department and proxy agencies. If a separation is noted, the Security Software Coordinator will revoke the individual's security software ID. (*C5.19*)

Mainframe Password Resets

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. (*C5.20*) Email reset requests are to include the user's name, mainframe ID and a contact phone number. The IT Service Desk staff creates a Remedy ticket and contacts the user at the number provided to 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 and 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 the Department is the agency's proxy, a Remedy ticket is assigned to the Department's Security Software Coordinator or the Department's Security Software Administrator. Using information from the Remedy ticket, the Department's Security Software Coordinator or the Security Software Administrator contacts the user to reset the password. (*C5.21*) 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.

Administrative Accounts

Access to the operating system configurations is limited to system support staff. (*C5.22*) Access with powerful privileges, high-level access and access to sensitive system functions is restricted to authorized personnel. (*C5.23*) To request administrative account access, the Department access provisioning process is to be followed. (*C5.24*)

The System Coordinator and Mainframe manager review a high-level systems programmer user ID listing on an annual basis. (*C5.25*) It is signed off on by both after the listing is deemed to be correct, or modifications have been made to the Mainframe System Security Software user IDs.

Access Provisioning – Applications

AIS, CPS, and CTAS specific account provisioning is managed by the 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. Agencies are responsible for ensuring proper segregation of duties in the assignment of application user access rights. Additionally, agencies are responsible for reviewing the user access rights to their data.

Agency AIS, CPS, and CTAS Application Administrators are established through the ATSRs submission of a Remedy service request. (*C5.26*)

Access to eTime is authenticated via Active Directory (AD). Functionality within the eTime application is based upon assigned roles. Agencies are responsible for managing eTime and review the user access rights to their data.

Application Administrators/Programmers

Access to application source code, Job Control Language (JCL) streams, data files and sensitive application functions are restricted to authorized personnel. (*C5.27*) To request access, the submission of an authorized Remedy service request is required. (*C5.28*) Revoking access is initiated upon receipt of Remedy service request or, under special or emergency circumstances, by instruction of the Department senior management.

Infrastructure

Network Services is comprised of three areas of responsibilities;

- Local Area Network Services is responsible for managing firewalls, switches, servers, and software that are the components to the local area network.
- Agency Wide Area Network Services is 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 Services is 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

The Department maintains network diagrams depicting common connectivity configurations. Additionally, network segmentation permits unrelated portions of the agencies' information system to be isolated from each other. Further, enterprise wide, agencies' traffic is segmented to be isolated from each other. (*C5.29*)

Detailed design and configuration standards and guides are maintained to ensure the integrity of the design, security and configuration of the network. (*C5.30*) Additionally, access level controls are applied through the use of Access Control Lists and Authentication Servers. Further, Access Control Lists reside [redacted]. (*C5.31*)

Authentication servers control access through assignment of access right privileges (read only or update) based on Department-defined group profiles. (*C5.32*) A security banner also serves as a security awareness mechanism and is displayed at initial network connection warning of prosecution for unauthorized access. (*C5.33*)

Self-monitoring network routers and switches record all events, notifies [redacted] and forwards to multiple logging servers. These servers use filters to automatically generate alerts when a network services' configured parameter or condition occurs. (*C5.34*)

Distributed denial of service platform is utilized to monitor and mitigate network threats. Threats are reviewed and appropriate action is taken based on the individual threat. (*C5.35*)

Firewalls are in place and configured with denial rules. (*C5.36*) Additionally, an intrusion detection system is in place to monitor for malicious and unauthorized activity. (*C5.37*)

Local Area Network (LAN) Services

Network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The 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 Services Support staff follow up on these alerts and engage operational teams for resolution as necessary. (*C5.38*) Alerts are tracked in the network monitoring system.

The authentication server records failed login attempts to the network equipment. (*C5.39*) Logs are imported into the Department's security information and event management tool for archival, historical, or investigative purposes upon request.

Agency Wide Area Network (WAN) Services

Network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / 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 24x7x365 Network Operation Center staff reviews each occurrence and engage operation teams for resolution. (*C5.40*)

The authentication server records failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to the Network Design and Engineering staff to determine, on a case by case basis, if further action is required. (*C5.41*)

WAN encryption technologies are utilized to protect data. (*C5.42*) Encryption technologies or secured communication channels are used to protect transmission of data across public network providers as requested by agencies for security compliance when agency applications do not transmit encrypted data. 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. (*C5.43*)

Virtual Private Networks (VPN) provide controlled and trusted connections between devices when required for data traversing public networks including the Internet. (*C5.44)* The Department's Enterprise VPN Standard provides guidance when establishing a VPN connection. (*C5.45*)

Backbone Wide Area Network (WAN) Services

Network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / 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. Alerts are tracked in the Network monitoring system. (*C5.46*)

Authentication Servers record failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to Network Design and Engineering staff to determine, on a case by case basis, if further action is required. (*C5.47*)

Endpoint Protection

Servers

The Endpoint Protection Group is responsible for pushing antivirus definitions and antivirus software updates out. Antivirus software is applied to manage definitions and antivirus software updates. Antivirus software is used to automatically push virus definition files to all systems after receipt from antivirus vendors. (*C8.2)* The Endpoint Protection Group monitors the state of systems and detect systems which fail to load updates and are not running the latest supported version. The Endpoint Protection Group follows the Department's Change Management Process to bring these systems up to date. Additionally, agencies are responsible for notifying the Department of actual or suspected information security breaches, compromised accounts, or unauthorized access.

Data Transmission Protection

The secure, encrypted transfer of mainframe data is achieved using the File Transfer Protocol Secure (FTPS). (*C7.1*) The software MOVEit is used to transmit midrange data between servers and applications and provides email alerts for any failures to Department and agency support staff. (*C7.2*)

Access to MOVEit systems are reviewed and followed up on an annual basis by the Department's Midrange Wintel Group. (*C7.3*)

Another option available to valid Illinois.gov users for the secure transmission of data is the file transfer utility 'FileT'. (*C7.4*) This utility uses random key generation to access files stored on a server. (*C7.5*) Only those with a valid key may download files from the server. Files are automatically purged from the server after five days. (*C7.6*) The sender must acknowledge a warning of unauthorized access message by clicking a box before transfer is allowed. (*C7.7*) 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. (*C7.8*)

Physical Security Access Controls

The CCF and Communications Building house the State's infrastructure. The Warehouse receives, stores and distributes State issued equipment. The following security controls are implemented at the facilities:

- The CCF and the Communications Building are monitored 24x7x365 by security guards. (*C4.1*)

- The CCF, Communications Building, and the Warehouse are monitored by security cameras located at various interior and exterior points. The security cameras are monitored by the security guards. (*C4.2*)

- The CCF, Communications Building and the Warehouse maintain building access and perimeter monitoring. (*C4.3*)

- The interior and exterior of the CCF, Communications Building, and the Warehouse access are enforced by card key access. (*C4.4*)

- To obtain a card key (badge) for access to the CCF, Communications Building and the Warehouse, an ID Badge Request Form is submitted by an authorized individual to HR. In the event the individual requires access to the CCF secured area, additional authorization is required. (*C4.5*) The Department's HR enters the applicable access rights into the Velocity system (card key (badge) system), obtains valid proof of identity and a photo to obtain a card key (badge). (*C4.6*) In order for non-state employees to obtain a card key (badge) documentation of a clear background check, performed in the past five years, must be provided prior to initial badge issuance. (*C4.7*) The card key (badge) is then created with approved access rights.

The card key (badge) access is revoked at the expiration date or upon official notice of separation or termination. (*C4.8*) An ID Badge Request Form is submitted by an authorized individual documenting the request for deactivation.

- The Department's Midrange Wintel Manager or designee conducts monthly reviews of individuals who were granted access or had access removed in the prior month to the CCF secured area. (*C4.9*) In addition, the Department's Security team conducts quarterly access reviews of all individuals with access to the CCF (starting in December 2020), Communication Building and the Warehouse (beginning January 2021). (*C4.10*) Further, the Department's Security team conducts monthly reviews of all individuals with access to the CCF secured area. (*C4.11*)

- Visitors are required to provide identification and sign the visitor log in order to gain access to the CCF and Communications Building. (*C4.12*) The visitors are provided a visitor badge, with no access rights. The visitor is required to be escorted at all time. (*C4.13*)

- In the event an individual does not have their card key (badge) readily available, the security guards may issue a temporary access card key (badge). The access rights, as documented in Velocity, are associated with the card key (badge). (*C4.14*)

  In addition, temporary badges are issued to authorized vendors once identification has been validated. (*C4.15*) The temporary badges allow the vendor access without escort.

- Visitors requiring access to the Warehouse are required to complete the visitor log; (*C4.16)* however, unescorted access is permitted as determined by the Warehouse staff.

Backups

The Department has implemented redundancy in the Data Center LANs and at agency locations where technically, fiscally, and operationally feasible. (*C9.1*) Additionally, device configurations are saved on a network management server, which verifies device configuration revisions daily, and new configurations are backed up when detected. (*C9.2*) Configurations saved on the network management server are backed up daily to the CCF and the Alternate Data Center (ADC) through the midrange backup system. (*C9.3*)

Mainframe

The Department is responsible for the scheduling and monitoring of the backup process except for the agency database data and applications. Agencies are responsible for scheduling the backups of their applications and database data. Agencies are also responsible for informing the Department of their business needs. Data on mainframe systems are backed up daily and weekly utilizing [redacted]). (*C9.4*) The Department utilizes [redacted] to schedule and verify the completion of the backups. (*C9.5*)

The Department has implemented mainframe backup procedures to assist staff in the event of failures. (*C9.6*)

Daily, the Department's Storage staff review the output of the daily backup jobs for any failures. In the event of a mainframe daily backup job failure, the Department's Operations Center staff records the incident in the Shift Report. (*C9.7*) The next working day, the Department's Storage staff review the Shift Report to identify the problem, correct and resubmit the failed portion of the backup job.

The Department's Storage staff 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. (*C9.8*)

Data replication is performed between the CCF and the ADC. Mainframe data replication occurs every [redacted] between the CCF and the ADC [redacted]. The monitoring software sends the Enterprise Storage and Backup group an alert if the data is out of sync for more than 24 hours. (*C9.9*) If there is an issue, a Remedy ticket is submitted to track the Enterprise Storage and Backup group's progress on resolution of the issue.

The [redacted] Replicated Status log keeps a log of replication between the two [redacted]s and tracks library replication outcomes for [redacted] replication activity. (*C9.10*) These logs document the status of the replicated Data Domain pool and the time of the last sync and are maintained for seven days. The Storage staff reviews and corrects any issues.

Midrange

[redacted] are used to back up the midrange environment. (*C9.11*) [redacted] is used to monitor and report on midrange backups. (*C9.12*) Midrange server backups are performed daily or weekly and are either incremental or full. (*C9.13*) [redacted] automatically generate daily reports indicating the backup status of scheduled jobs from the prior day. These daily reports are emailed to the Enterprise Storage and Backup group who then investigates the cause of failures and works to resolve the problem. (*C9.14*) Backed up server data is written to a Data Domain storage system and then replicated to another Data Domain storage system at the ADC. The Data Domain storage systems generate a daily status report which is emailed to the Enterprise Storage and Backup group. (*C9.15*) The Data Domain storage systems also send email alerts to the Enterprise Storage and Backup group when issues arise that may need additional attention. (*C9.16*) The 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. (*C9.17*)

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. (*C9.18*) It is the responsibility of the database administrators to perform and monitor the success of the database backups.

A [redacted] 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 and follows up for any failures. (*C9.19*) The SQL team also gets alerts from the SQL servers when backup jobs fail. (*C9.20*) Additionally, the SQL team receives alerts from the [redacted] monitoring software if a database has missed a backup. (*C9.21*)

Any data, including, but not limited to SQL, Access, DB2 databases, user shared documents and user profiles are located on tier 2 storage device via the Network File System or the Service Message Block shares. The Enterprise Storage and Backup group has policies on the [redacted] that take daily snapshots of all shares which are then retained up to 60 days. (*C9.22*) The tier 2 storage also has daily synchronization with the ADC to another [redacted] storage system. The [redacted] generates a daily report showing successful and failed synchronization attempts with the ADC. (*C9.23*) Enterprise Storage and Backup group investigate failed synchronization attempts until a satisfactory conclusion is reached. The [redacted] has a call home feature that notifies vendor support. For critical issues, the [redacted] call home feature additionally notifies the Enterprise Storage and Backup group. (*C9.24*)

Mainframe

The mainframe environment is monitored through the z/OS systems console for errors and issues. (*C6.1*) The Operations Center staff 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. (*C6.2*) Additionally, performance and capacity monitoring are documented via internal memorandum distributed via email to Enterprise Infrastructure management monthly. (*C6.3)*

The Department has implemented system options to protect resources and data. The System Management Facility records operating system activities. The System Coordinator runs a System Management Facility violation report weekly for review and signs off on the report after resolving any unusual violations. *(C8.1*)

The Department has developed operations manuals to provide staff with instruction related to their various tasks.

Midrange

Midrange availability is monitored by the Operations Command Center via the [redacted] system. (*C6.6*) Command Center technicians notify System and/or Storage technicians of [redacted] alerts.

Structured Query Language (SQL) database servers use the [redacted] tool set for additional monitoring. The [redacted] system alerts have been set up to generate emails to SQL support staff. (*C6.4*) The SQL support staff use the [redacted] tools to help trouble shoot SQL issues.

The Active Directory Domain Controllers use [redacted]r for additional monitoring. [redacted] alerts have been set up to email alerts to AD support staff. (*C6.5*) The AD staff uses [redacted] to help trouble shoot AD issues.

Data Storage

Data Storage performance and capacity are monitored using vendor specific toolsets. *(C9.25*) 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%. (*C9.26*) Midrange data backups are monitored by [redacted]

[redacted] (*C9.27*)

Complementary Subservice Organization Controls

The Department's controls related to the IT General Controls and Application Controls cover only a portion of the overall internal control for each user agency. It is not feasible for the control objectives related to the IT General Controls and Application Controls to be achieved solely by the Department. Therefore, each user agency's internal control over financial reporting must be evaluated in conjunction with the Department's controls and the related tests and results described in section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization described below.

1) Controls are implemented to provide IT managed services which are performed in accordance with contracts.

2) Controls are implemented to provide assurance that access to networks and applications is approved, reviewed periodically, and access is terminated timely.

3) Controls are implemented to provide reasonable assurance that only authorized personnel are able to make changes to network and applications.

4) Controls are implemented to provide reasonable assurance that updates to networks and applications are documented, approved, and tested prior to implementation.

5) Control are implemented to provide adequate security around the network and application operations.

6) Controls are implemented to address incidents that are identified, tracked, resolved and closed in a timely manner.

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 complete and accurate entry and maintenance of data into the applications.
#2	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.
#5	Agency ATSRs are responsible for the submission of an approved Remedy service request for the creation, modification, and termination of user access.
#5	For the creation of a security software account, agencies are responsible for the submission of an approved service request or Mainframe request form if Remedy service request is not available for the agency.
#5	Agencies are responsible for the submission of an approved Remedy service request for the establishment of the agency Application Administrator.
#5	Agencies are responsible for the submission of an approved Remedy service request for the establishment of an eTime Administrator.
#5	Agency Application Administrator is responsible for assignment of their agency's application specific accounts, associated rights and privileges, password management, and deactivation or reassignment.
#5	Agencies are responsible for ensuring proper segregation of duties in the assignment of application user access rights.
#5	Agencies are responsible for reviewing the user access rights to their data.
#5	Agencies are responsible for managing eTime and review the user access rights to their data.
#5	Agency's timekeeper is responsible for entry and maintenance of an employee's time and attendance; vacation, sick, personal, etc.
#5	Agencies are responsible for contacting the IT Service Desk or the utilization of the self-service options, in order to reset the AD or Novell accounts.
#5	Proxy agencies are responsible for reviewing the appropriateness of their agencies

	security software accounts and responding to the Security Software Coordinator or designee.
#5	Agencies with a Security Software Coordinator are responsible for monitoring/reviewing the security software accounts assigned to their agency.
#5	Agencies are responsible for reviewing AD accounts that have been dormant for 60 or more days and taking appropriate actions to keep accounts active.
#5	Agencies are responsible for scheduling the backups of their applications and database data.
#5	Agencies are responsible for informing the Department of business needs.

SECTION IV

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 Service Auditor

This report, when combined with an understanding of the controls at the client agencies, is intended to assist auditors in planning the audit of client agencies' financial statements and client agencies' internal control over financial reporting and in assessing control risk for assertions in client 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 client agencies. The examination was performed 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. It is each client agencies' responsibility to evaluate this information in relation to the internal control structure in place at each client agency in order to assess the total internal control structure. If an effective internal control structure is not in place at client agencies, the Department's controls may not compensate for such weaknesses.

It is the responsibility of each client agency and its independent auditor to evaluate this information in conjunction with the evaluation on internal control over financial reporting at client agencies in order to assess total internal control. If internal control is not effective at the client 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 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 communication.

Tests of Controls

Our test of the operational effectiveness of controls were designed to cover a representative number of activities throughout the period of July 1, 2020 to June 30, 2021, for each of the controls, which are designed to achieve the specific control objectives. In selecting particular tests of operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the examination objectives to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

The Service Auditor's testing of controls was restricted to the controls specified by the Department in Section IV, and was not extended to controls in effect at client agency locations or other controls which were not documented as tested under each control criteria listed in Section IV. The description of the Service Auditor's tests of controls and results of those tests are presented in this section of the report. The description of the tests of controls and the results of those tests are the responsibility of the Service Auditor and should be considered information provided by the Service Auditor.

The basis for all tests of operating effectiveness includes inquiry of the individual(s) responsible for the control. As part of our testing of each control, we inquired of the individual(s) to determine the fairness of the description of the controls and to evaluate the design and implementation of the control. As part of inquiries, we also gained an understanding of the knowledge and experience of the personnel managing the control(s) and corroborated evidence obtained as part of other testing procedures. While inquiries were performed for every control, our inquiries were not listed individually for every control activity tested and shown in Section IV.

Additional testing of the control activities was performed using the following methods:

Type	**Description**
Observation	Observed the application, performance, or existence of the specific control(s) as represented by management.
Inspection/Reviewed	Inspected/reviewed documents and records indicating performance of the control.
Reperformance	Reperformed the control or processing application to ensure the accuracy of its operation.

Information Provided by the Department

When using information produced by the Department, 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 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
C1.1	The applications have edit features designed to reject erroneous or invalid data. When erroneous or invalid data is entered, an error message is displayed indicating the problem.	Selected a sample of field edits to determine if they were functioning appropriately and error notifications appeared.	No deviations noted.
C1.2	Separate, stand-alone user manuals and guides are available for the AIS, 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.

Control Objective 2: Controls provide reasonable assurance that appropriate federal and state 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 modifies federal tax tables accordingly.	Reviewed the federal tax rates to determine if the rates had been updated within CPS.	The head of household federal tax rate was incorrect.
C2.2	On an annual basis, CPS staff research tax rates for CPS-recognized states and update state tax tables accordingly.	Reviewed the state tax rates within CPS to determine if the rates had been updated.	1 of 6 state tax rates were incorrect. The State of Illinois tax rate was correct.

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

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C3.1	Control over changes to the network, mainframe, mainframe patching, 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.	Reviewed the Change Management Process Guide, ROD Change Management Guide, and the Change Management User Guide to determine if controls were documented.	The required approvals documented in the ROD User Guide contradicted the required approvals documented in the Change Management Guide.
C3.2	z/OS production systems are updated quarterly and when patches become available, all other mainframe software components (IMS, CICS, DB2, ISV, etc) are updated.	Reviewed z/OS production system patches to determine if they were updated quarterly.	No deviations noted.
		Reviewed other mainframe components' patches to determine if they were patched when available.	No deviations noted.
C3.3	Changes with a significant or extensive impact require test, implementation, and back out information be provided within 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.	6 of 60 significant or extensive impact changes selected did not contain a test plan.
			6 of 60 significant or extensive impact changes selected did not contain a backout plan.
			6 of 60 significant or extensive impact changes selected did not contain a implementation plan.

C3.4	Change requests are classified into class and impact categories with the level of approval is based on the assigned impact. Approval is required prior to being placed into production.	Reviewed a sample of changes to determine if the change was properly approved based on its class and impact categories and approved prior to being placed into production.	4 of 60 medium, high and critical impact changes selected were not approved by the Change Advisory Committee.
			4 of 60 low and high impact changes selected were not approved by a group manager.
			16 of 60 low impact changes selected were not approved by the Enterprise Change Manager.
			3 of 60 low impact changes selected were not reviewed.
C3.5	Emergency changes require 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.	3 of 16 emergency changes selected did not have a Post Implementation Review conducted.
			6 of 16 emergency changes selected did not have a Post Implementation Review completed within two business days after implementation.
C3.6	The Department follows the Server Patch Management procedures for receiving and deploying Microsoft Windows patches monthly.	Selected a sample of monthly Microsoft Window patches to determine if they followed the Server Patch Management procedures.	No deviations noted.
C3.7	The Department utilizes [redacted] to push and monitor Windows patches after obtaining approval.	Reviewed the [redacted] patch schedule to determine if Window patches were pushed out and monitored.	No deviations noted.
C3.8	The Department follows the applicable patching procedures for the Linux, VMware and Unix (AIX) patches which are implemented when provided by the vendor.	Selected a sample of Linux, VMWare, and Unix patches to determine if they followed the applicable patching procedures.	4 of 4 VMWare patches did not have documentation of testing completed prior to implementation.

C3.9	The patches are reviewed and tested by technicians and follow the Department's change management process.	Selected a sample of Linux, VMWare, and Unix patches to determine if they were reviewed and tested by technicians and followed the Department's change management process.	4 of 4 VMWare patches did not have documentation of testing completed prior to implementation.
			1 of 2 Unix patches selected did not have documentation of testing being completed prior to implementation.
C3.10	For application changes, processing steps are documented in Application Lifecycle Management Manual, EAA Mainframe Change Management Procedures and the EAA Distributed Change Management Procedures.	Reviewed the Application Lifecycle Management Manual, ESA Mainframe Change Management Procedures, and the ESA Distributed Change Management Procedures to determine if they documented the change management procedures.	No deviations noted.
		Selected a sample of application changes to determine if a Remedy request had been submitted and if the change followed the Application Lifecycle Management Manual, EAA Mainframe Change Management Procedures and the EAA Distributed Change Management Procedures.	No deviations noted.
C3.11	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.	Observed the code management system to determine if modified code was prevented from being placed into production without authorization.	No deviations noted.
		Selected a sample of mainframe changes to determine if proper authorization was obtained prior to placing in the code management system.	No deviations noted.
C3.12	Supervisory approval is required before Remedy releases the activity to the Library Services group who performs the move into production.	Selected a sample of application changes to determine if supervisory approval was obtained prior to the release to Library Services.	No deviations noted.

C3.13	Moves to the mainframe production environment are completed by Library Services based on the instructions within the Move Sheet.	Selected a sample of application changes to determine if Library Services completed the move to the mainframe production environment based on the instructions.	No deviations noted.
C3.14	Developers are limited to read only access to the Production Libraries.	Reviewed developers' access to determine if their access to the production libraries was read only.	No deviations noted.
C3.15	For distributed systems, supervisory approval is required prior to deployment into the production environment.	Selected a sample of change to determine if the supervisor approved the request prior to deployment into the production environment.	No deviations noted.
C3.16	Designated release staff, who did not code the change, move the change into the production environment manually, and developers who coded the changes verify the changes to ensure accuracy, or via an automated release management module if configured, with supervisor approval.	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.

Control Objective 4: Controls provide reasonable assurance that physical access to facilities and data centers is restricted to authorized personnel, that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPAPRTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C4.1	The CCF and the Communications Building are monitored 24x7x365 by security guards.	Observed security guards at the CCF and the Communications Building.	No deviations noted.
C4.2	The CCF, Communications Building, and the Warehouse are monitored by security cameras located at various interior and exterior points. The security cameras are monitored by the security guards.	Observed security cameras were located at interior and exterior points and were monitored by the security guards.	Interior cameras at the Warehouse were not monitored by the security guards.
C4.3	The CCF, Communications Building and the Warehouse maintain building access and perimeter monitoring.	Observed building access and perimeter monitoring controls.	No deviations noted.
C4.4	The interior and exterior of the CCF, Communications Building and the Warehouse access are enforced by card key access.	Observed card key readers at interior and exterior points.	No deviations noted.
C4.5	To obtain a card key (badge) for access to the CCF, Communications Building and the Warehouse, an ID Badge Request Form is submitted by an authorized individual to HR. In the event the individual requires access to the CCF secured area, additional authorization is required.	Selected a sample of new employees and contractors to determine if an authorized ID Badge Request Form was completed and if access to the CCF secured area was properly authorized.	3 of 26 new employee and contractor ID Badge Request Forms did not have all required fields properly completed.
C4.6	The Department's HR enters the applicable access rights into the Velocity system (card key (badge) system), obtains valid proof of identity and a photo to obtain a card key (badge).	Selected a sample of new access requests to determine if a valid proof of identity and a photo were provided.	No deviations noted.

C4.7	In order for non-state employees to obtain a card key (badge) documentation of a clear background check, performed in the past five years, must be provided prior to initial badge issuance.	Selected a sample of access requests for new non-State employees to determine if a clear background check had been completed in the last five years and was provided prior to the initial badge issuance.	No deviations noted.
C4.8	The card key (badge) access is revoked at the expiration date or upon official notice of separation or termination.	Selected a sample of terminations to determine if card key access was timely deactivated.	The Department did not provide documentation demonstrating the terminated individuals' access badge had been deactivated. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
C4.9	The Department's Midrange Wintel Manager or designee conducts monthly reviews of individuals who were granted access or had access removed in the prior month to the CCF secured area.	Selected a sample of monthly reviews to determine if the Midrange Wintel Manager had reviewed individuals who were granted access or had access removed in the prior month to the CCF secured area.	No deviations noted.
C4.10	The Department's Security team conducts quarterly access reviews of all individuals with access to the CCF (starting in December 2020), Communication Building and the Warehouse (beginning January 2021).	Selected a sample of quarterly access reviews to determine if the Security team had reviewed individuals' access to the CCF (starting in December 2020), and Communication Building, and the Warehouse (beginning January 2021).	No deviations noted.
C4.11	The Department's Security team conducts monthly reviews of all individuals with access to the CCF secured area.	Selected a sample of monthly reviews to determine if the Security team conducted monthly reviews of individuals with access to the CCF secured area.	No deviations noted.
C4.12	Visitors are required to provide identification and sign the visitor log in order to gain access to the CCF and Communications Building.	Observed visitors were required to sign the visitor's log and provide identification to gain access to the CCF and Communications Building.	No deviations noted.
C4.13	The visitors are provided a visitor badge, with no access rights. The visitor is required to be escorted at all time.	Observed visitors were required to sign the visitor's log, provide identification, and be escorted.	No deviations noted.

C4.14	In the event an individual does not have their card key (badge) readily available, the security guards may issue a temporary access card key (badge). The access rights, as documented in Velocity, are associated with the card key (badge).	Observed individuals were provided temporary access card key with access rights as documented in Velocity.	No deviations noted.
C4.15	Temporary badges are issued to authorized vendors once identification has been validated.	Selected a sample of the Building Admittance Registers to determine if individuals were provided a temporary badge with appropriate access.	In the 30 Building Admittance Registers selected, there were 7 individuals with 13 instances which were not provided a temporary badge with appropriate access.
C4.16	Visitors requiring access to the Warehouse are required to complete the visitor log.	Observed visitors were required to sign the visitor's log.	No deviations noted.

<u>Control Objective 5:</u> 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
C5.1	In order to access the State's information technology environment, an Active Directory ID and password are required.	Observed an AD ID and password were required to gain access to the environment.	No deviations noted.
C5.2	Password security parameters have been established and configured to ensure access to 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.
C5.3	Access creation or modification to Department resources (users and administrators) requires the submission of a Remedy service request from a Remedy submitter or an authorized Agency Technology Service Requestor (ATSR).	Selected a sample of new employees and contractors to determine if an ATSR approved Remedy service request was submitted.	No deviations noted.
		Selected a sample of access modifications to determine if an ATSR approved Remedy service request was submitted.	The Department did not provide a population of access modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.

C5.4	For voluntary separations of an employee or a contractor, an Employee Exit form and a Remedy service request are completed to initiate and to ensure the removal of access and the retrieval of equipment.	Selected a sample to separated employees and contractors to determine if an Employee Exit form and Remedy service request had been completed.	2 of 27 terminated employees selected did not have a Remedy Service Request completed.
C5.5	Revoking access to Department resources is initiated upon receipt of a Remedy service request or under special or emergency circumstances, network access is disabled at the instruction of the Department senior management.	Selected a sample of separated users to determine if network access was disabled.	2 of 27 selected separated employees and contractors access revocation documentation was not provided.
			The Department did not have a policy documenting the required timeframe for revocation of logical access upon termination.
C5.6	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 Department's website to determine solution to reset passwords.	No deviations noted.
C5.7	The IT Service Desk staff will then proceed with the reset after verification of two of three pieces of information: phone number, email address and physical address.	Observed the IT Service Desk staff to determine if an individual's identity was verified prior to reset.	No deviations noted.
C5.8	On an annual basis, the Department’s Security Compliance team sends a list of the technical accounts to appropriate supervisors.	Reviewed the annual review to determine if the Security Compliance team conducted a review of technical accounts.	No deviations noted.
C5.9	The Department performs a monthly review of Illinois.gov Active Directory accounts and disables accounts which have been dormant for 60 days.	Selected a sample of monthly reviews to determine if dormant accounts were reviewed.	No deviations noted.

C5.10	Department staff and vendors with a business need to access or modify network devices are added to a designated Active Directory access group (for role based and least privileges) and setup with a two-factor authentication token.	Selected a sample of individuals with a business need to access or modify network devices to determine if staff and vendors were added to designated Active Directory access groups and set up with a two-factor authentication token.	1 of 20 network administrators did not require administrative rights to the environment.
C5.11	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.
C5.12	The primary means of defining an individual's level of access is the security software profile.	Observed a security software profile to determine if the profile defined the level of access.	No deviations noted.
C5.13	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.
C5.14	The 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.
C5.15	Once the Remedy service request is created, or Mainframe Request Form is submitted, the Department's Software Security Coordinator will receive the Remedy ticket, and follow the Security Software ID Creation procedures to create an account as specified.	Selected a sample of new security software accounts to determine if the Software Security Coordinator followed the Security Software ID Creation procedures to create an account.	5 of 35 new security software accounts selected were not approved by an ATSR. 4 of 35 new security software accounts selected did not have an approved Remedy ticket or Mainframe Access Request Form.

		Selected a sample of modified security software accounts to determine if the Software Security Coordinator followed the Security Software ID Creation procedures to modify the account.	The Department did not provide a population of security software ID modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
C5.16	On an annual basis, the Department's Security Software Coordinator sends proxy agencies and the Department a listing of security software IDs assigned to their agency and the Department for review.	Reviewed the annual review of security software IDs to determine if the review had been conducted.	The Department did not conduct the Security Software Annual Reconciliation.
C5.17	On a monthly basis, the Department's Security Software Coordinator or designee runs a report documenting the Department and the proxy agencies' security software IDs which have not been utilized in the past 90-days; upon review, the IDs are revoked.	Selected a sample of monthly reports to determine if the IDs had been revoked.	No deviations noted.
C5.18	The Department's Security Software Coordinator or designee runs a weekly violation report which is reviewed for invalid and unauthorized access attempts of the Department and proxy agency security software IDs. The Department's Security Software Coordinator follows up with the review results as stated in the Security Violation Report Procedure. The Department's Security Software Coordinator or designee 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 Coordinator or designee had reviewed and followed up on invalid and unauthorized access attempts.	No deviations noted.

C5.19	Semi-monthly, the Department's Security Software Coordinator receives a separation report documenting the separations for the month. The Department's Security Software Coordinator or designee reviews the separation reports, noting separation of individuals from the Department and proxy agencies. If a separation is noted, the Security Software coordinator will revoke the individual's security software ID.	Selected a sample of semi-monthly reports to determine if the Security Software Coordinator had reviewed and revoked individual accounts which had separated.	No deviations noted.
C5.20	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.	Reviewed the DoIT Identity Management website to determine solution to reset passwords.	No deviations noted.
C5.21	In the event the Department is the agency's proxy, a Remedy ticket is assigned to the Department's Security Software Coordinator or the Department's Security Software Administrator. Using information from the Remedy ticket, the Department's Security Software Coordinator or the Security Software Administrator contacts the user to reset the password.	Observed the Security Software Coordinator reset the mainframe password upon receipt of a Remedy ticket.	No deviations noted.
C5.22	Access to the operating system configurations is limited to system support staff.	Reviewed access rights to the mainframe operating system configurations to determine if access was limited to system support staff.	No deviations noted.
C5.23	Access with powerful privileges, high-level access and access to sensitive system functions is restricted to authorized personnel.	Reviewed access rights to powerful privileges, high-level access, and access to sensitive system function to determine if access was limited to authorized personnel.	No deviations noted.

C5.24	To request administrative account access, the Department access provisioning process is to be followed.	Selected a sample of new administrative accounts to determine if new administrative accounts followed the Department's access provisioning process.	The Department did not have a request for a new system administrator. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
C5.25	The System Coordinator and Mainframe manager review a high-level systems programmer user ID listing on an annual basis.	Reviewed the annual review of high-level system programmers by the System Coordinator and Mainframe manager.	No deviations noted.
C5.26	Agency AIS, CPS, and CTAS Application Administrators are established through the ATSR's submission of a Remedy service request.	Selected a sample of new agencies Application Administrators to determine if a service request was approved by the ASTR.	No deviations noted.
C5.27	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.
C5.28	To request access, the submission of an authorized Remedy service request is required.	Selected a sample of access requests to determine if an authorized Remedy service request was obtained.	No deviations noted.
C5.29	The Department maintains network diagrams depicting common connectivity configurations. Network segmentation permits unrelated portions of the agencies' information system to be isolated from each other. Enterprise wide, agencies' traffic is segmented to be isolated from each other.	Reviewed network diagrams to determine connectivity configurations.	No deviations noted.
		Reviewed device configurations to determine if networks were segmented.	No deviations noted.
C5.30	Detailed design and configuration standards and guides are maintained to ensure the integrity of the design, security and configuration of the network.	Reviewed the design and configuration standards and guides to determine if the standards and guides were maintained.	No deviations noted.

C5.31	Access level controls are applied through the use of Access Control Lists and Authentication Servers. Access Control Lists reside [redacted]	Reviewed configurations to determine if ACLs restricted communications.	No deviations noted.
C5.32	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.	No deviations noted.
C5.33	A security banner also serves 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.	No deviations noted.
C5.34	Self-monitoring network routers and switches record all events, notifies [redacted] and forwards to multiple logging servers. These servers use filters to automatically generate alerts when a network services' configured parameter or condition occurs.	Reviewed network routers and switches to determine if they were encoded with filters and if the Network Operations Center were reviewing and resolving alerts received.	No deviations noted.
C5.35	Distributed denial of service platform is utilized to monitor and mitigate network threats. Threats are reviewed and appropriate action is taken based on the individual threat.	Reviewed the distributed denial of services platform configurations and alerts to determine if threats were mitigated and reviewed.	No deviations noted.
C5.36	Firewalls are in place and configured with denial rules.	Selected a sample of firewalls to determine if the firewalls were configured with denial rules.	No deviations noted.
C5.37	An intrusion detection system is in place to monitor for malicious and unauthorized activity.	Selected a sample of egress firewalls to determine if the egress firewalls were configured to monitor malicious and unauthorized activity.	No deviations noted.

C5.38	LAN Services network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The 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 Services Support 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 and LAN Services Support staff followed up on the alerts.	No deviations noted.
C5.39	The authentication server records failed login attempts to the network equipment.	Reviewed configurations to determine if failed login attempts were logged.	No deviations noted.
C5.40	WAN Services network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / 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 24x7x365 Network Operation Center staff reviews each occurrence and engages operation teams for resolution.	Reviewed software configurations to determine if emails and alters 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.

C5.41	WAN Services authentication server records failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to Network Design and Engineering staff to determine, on a case by case basis, 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 and Engineering staff.	No deviations noted.
C5.42	WAN encryption technologies are utilized to protect data.	Reviewed configurations to determine if data traversing the network was encrypted.	No deviations noted.
C5.43	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.
C5.44	Virtual Private Networks (VPN) provide controlled and trusted connections between devices when required for data traversing public networks including the Internet.	Reviewed VPN configurations to determine if security settings were configured to allow for secure remote connections.	No deviations noted.
C5.45	The Department's Enterprise VPN Standard provides guidance when establishing a VPN connection.	Reviewed the Enterprise VPN Standard to determine if the Standards provided guidance on VPN connections.	No deviations noted.

C5.46	Backbone WAN Services network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / 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. Alerts are tracked in the Network monitoring system.	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.
C5.47	Backbone WAN Services authentication servers record failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to Network Design and Engineering staff to determine, on a case by case basis, if further action is required.	Reviewed configurations to determine if failed login attempts were logged and if email notification was sent to Network Design and Engineering staff.	No deviations noted.
C5.48	ADFS and Okta SSO utilize the same Active Directory credentials, in addition to two-factor authentication.	Observed ADFS and Okta to determine if it utilized AD credentials and two-factor authentication.	No deviations noted.

Control Objective 6: 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 mainframe environment is monitored through the z/OS systems console for errors and issues.	Observed the z/OS system console to determine if errors and issues were documented.	No deviations noted.
C6.2	Mainframe system performance and capacity is monitored by System Software programming personnel, via Resource Measurement Facility reports which are run daily and monthly.	Selected a sample of Resource Measurement Facility reports to determine if they were ran daily and monthly and monitored by System Software programming personnel.	No deviations noted.
C6.3	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.
C6.4	SQL database servers use the [redacted] tool set for additional monitoring. The [redacted] system alerts have been set up to generate emails to SQL support staff.	Reviewed the [redacted] configuration to determine if monitoring and email alerts to SQL support staff were configured.	No deviations noted.
C6.5	The Active Directory Domain Controllers use [redacted] for additional monitoring. [redacted] alerts have been set up to email alerts to AD support staff.	Reviewed [redacted]onfigurations to determine if monitoring and email alerts to AD support staff were configured.	No deviations noted.
C6.6	Midrange availability is monitored by the Operations Command Center via the [redacted] system.	Observed [redacted] to determine if availability and performance was monitored.	No deviations noted.

<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 the File Transfer Protocol Secure (FTPS).	Observed the file transfer protocol to determine if the mainframe data was secure and encrypted during transfer.	No deviations noted.
C7.2	The software MOVEit is used to transmit midrange data between servers and applications and provides email alerts for any failures to Department and agency support staff.	Reviewed the MOVEit software configurations to determine if MOVEit was used to transmit data between servers and applications and if email alerts were sent for failures to Department and agency support staff.	No deviations noted.
C7.3	Access to MOVEit systems are reviewed and followed up on an annual basis by the Department’s Midrange Wintel Group.	Reviewed the annual review of access to MOVEit by the Department's Midrange Wintel Group.	No deviations noted.
C7.4	Another option available to valid Illinois.gov users for the secure transmission of data is the file transfer utility ‘FileT’.	Reviewed the FileT configurations to determine the security over the transmission of the data.	No deviations noted.
C7.5	This utility uses random key generation to access files stored on a server.	Reviewed file transfer protocol configurations to determine if random key generation was utilized.	No deviations noted.
C7.6	Files are automatically purged from the server after five days.	Reviewed filed transfer protocol configurations to determine if files were purged after five days.	No deviations noted.
C7.7	The sender must acknowledge a warning of unauthorized access message by clicking a box before transfer is allowed.	Observed the sender must acknowledge a warning of unauthorized access message.	No deviations noted.
C7.8	A valid Illinois.gov email address is required to use this utility for State resources; either as the recipient or the sender.	Observed a valid Illinois.gov address was required.	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	The System Coordinator runs a System Management Facility violation report weekly for review and signs off on the report after resolving any unusual violations.	Reviewed a sample of weekly System Management Facility violation reports to determine if unusual violations were resolved and the reports were signed off on by the System Coordinator.	No deviations noted.
C8.2	Antivirus software is used to automatically push virus definition files to all systems after receipt from antivirus vendors.	Reviewed antivirus compliance reports to determine if definitions and updates were configured.	7 of 233 servers' DAT versions were out of compliance.
			15 of 2,760 servers' AMCore Content versions were out of compliance.

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
C9.1	The Department has implemented redundancy in the 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.
C9.2	Device configurations are saved on a network management server, which verifies device configuration revisions daily, and new configurations are backed up when detected.	Reviewed configurations' backup schedule to determine if the configurations were saved on a network management server.	From April 15, 2021 to April 23, 2021 device configuration revisions were not backed up.
C9.3	Configurations saved on the network management server are backed up daily to the CCF and the Alternate Data Center (ADC) through the midrange backup system.	Reviewed the backup schedule to determine if the network management server was backed up daily to the CCF and the ADC.	No deviations noted.
C9.4	Data on mainframe systems are backed up daily and weekly utilizing V[redacted]	Observed the [redacted] to determine if mainframe backups were performed daily and weekly.	No deviations noted.
C9.5	The Department utilizes [redacted] to schedule and verify the completion of the backups.	Selected a sample of backup schedules to determine if mainframe backups were scheduled and the completion was verified.	No deviations noted.
C9.6	The Department has implemented mainframe backup procedures to assist staff in the event of failures.	Reviewed policies to determine if they outlined procedures in the event of failed backups.	No deviations noted.

C9.7	In the event of a mainframe daily backup job failure, the Department's Operations Center staff records the incident in the Shift Report.	Reviewed a sample of daily and weekly backup reports, Remedy tickets, and Daily Shift reports to determine if mainframe backup jobs had failed.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating the effectiveness of this control.
C9.8	The Department's Storage staff 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.	Reviewed a sample of daily and weekly backup reports, Remedy tickets, and Daily Shift reports to determine if mainframe backup jobs had failed.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating the effectiveness of this control.
C9.9	Mainframe data replication occurs every [redacted] between the CCF and the ADC [redacted] The monitoring software sends the Enterprise Storage and Backup group an alert if the data is out of sync for more than 24 hours.	Reviewed the [redacted] configurations to determine if replication occurred every [redacted] and an alert was sent if the data was out of sync for more than 24 hours.	No deviations noted.
C9.10	The [redacted] Replicated Status log keeps a log of replication between the two [redacted]s and tracks library replication outcomes for [redacted] replication activity.	Reviewed the [redacted] replication log to determine if the current replication activity was recorded and tracked the replication outcomes.	No deviations noted.
C9.11	[redacted] are used to back up the midrange environment.	Reviewed [redacted]o determine if they were used to backup the midrange environment.	No deviations noted.
C9.12	[redacted] is used to monitor and report on midrange backups.	Reviewed [redacted] to determine if it monitored and reported on midrange backups.	No deviations noted.
C9.13	Midrange server backups are performed daily or weekly and are either incremental or full.	Reviewed the [redacted] design to determine if midrange servers were backed up daily or weekly and were either incremental or full.	No deviations noted.

C9.14	[redacted] automatically generate daily reports indicating the backup status of scheduled jobs from the prior day. These daily reports are emailed to the Enterprise Storage and Backup group who then investigates the cause of failures and works to resolve the problem.	Observed [redacted] to determine if they were configured to send daily reports of the backup status for all scheduled jobs.	No deviations noted.
		Interviewed Enterprise Storage and Backup staff to determine the actions taken to resolve the failures.	No deviations noted.
C9.15	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.	Reviewed the replication of the Data Domain storage system to determine if it was replicated to the ADC.	No deviations noted.
		Reviewed the Data Domain configuration to determine if daily reports of the replication status for all scheduled jobs were emailed to the Enterprise Storage and Backup group.	No deviations noted.
C9.16	The Data Domain storage systems also send email alerts to the Enterprise Storage and Backup group when issues arise that may need additional attention.	Reviewed the Data Domain configuration to determine if alerts were sent to the Enterprise Storage and Backup group.	No deviations noted.
C9.17	The Data Domain systems automatically alert vendor support in the event of hardware or system failures.	Reviewed the Data Domain storage system configuration to determine if alerts were sent to the support vendor.	No deviations noted.
C9.18	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.	Reviewed the replication of the Data Domain storage system to determine if it was replicated to the ADC.	No deviations noted.
C9.19	A [redacted] 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 and follows up for any failures.	Reviewed the SQL configuration to determine the status of backups was documented daily.	No deviations noted.
C9.20	The SQL team also gets alerts from the SQL servers when backup jobs fail.	Reviewed the SQL servers configurations to determine if alerts were enabled.	No deviations noted.

C9.21	The SQL team receives alerts from the [redacted] monitoring software if a database has missed a backup.	Reviewed the [redacted] monitoring software configurations to determine if automatic alerts were enabled.	No deviations noted.
C9.22	The Enterprise Storage and Backup group has policies on the [redacted] that take daily snapshots of all shares which are then retained up to 60 days.	Reviewed the [redacted] policies to determine if daily snapshots of all shares were taken and retained for up to 60 days.	No deviations noted.
C9.23	The [redacted] generates a daily report showing successful and failed synchronization attempts with the ADC.	Reviewed the [redacted] storage device configuration to determine if daily reports documenting successful and failed syncornzation attempt were generated.	No deviations noted.
C9.24	The [redacted] has a call home feature that notifies vendor support. For critical issues, the [redacted] call home feature additionally notifies the Enterprise Storage and Backup group.	Reviewed the [redacted] configuration to determine if the call home feature was activated and notifications were sent to the Enterprise Storage and Backup group.	No deviations noted.
C9.25	Data Storage performance and capacity are monitored using vendor specific toolsets.	Reviewed toolsets' configurations to determine if data storage performance and capacity were monitored.	No deviations noted.
C9.26	Automated alerts are sent via email to Data Storage technicians and management when capacity is reached or exceeds 80%.	Reviewed storage system configurations to determine if automated alerts were configured.	No deviations noted.
C9.27	Midrange data backups are monitored by [redacted]	Reviewed the [redacted] configurations to determine if midrange system data backups were monitored.	No deviations noted.

SECTION V

OTHER INFORMATION PROVIDED BY THE STATE OF ILLINOIS, DEPARTMENT OF INNOVATION AND TECHNOLOGY

DEPARTMENT OF INNOVATION AND TECHNOLOGY
Corrective Action Plan
(Not Examined)

Report Control	Department's Response
C2.1	The Department has updated the tax table as noted above and will review the data entry in the future.
C2.2	The Department has updated the tax table as noted above and will review the data entry in the future.
C3.1	The Department will retire the Remedy on Demand User Guide when the Department starts using the new service management tool in FY22.
C3.3	The Department will update the internal document and remind staff of the internal process guide.
C3.4	The Department will continue to follow the enterprise change management process guide and retire the Remedy on Demand change management process guide in FY22 that caused the exception.
C3.5	The Department will continue to follow the enterprise change management process guide and retire the Remedy on Demand change management process guide in FY22 that caused the exception.
C3.8	The Department will remind staff of the internal process guide and documentation of testing.
C3.9	The Department will remind staff of the internal process guide and documentation of testing.
C4.2	The Department will evaluate the necessary physical security monitoring controls at the Warehouse.
C4.5	The Department will remind staff of the internal process guide.
C4.8	The Department will research opportunities to generate reports in the requested format for future audit testing.
C4.15	The Department will follow up with the Department of Central Management Services (DCMS) to ensure that the DCMS follows the Department's badging process.
C5.3	The Department will research opportunities to generate reports in the requested format for future audit testing.
C5.4	The Department will continue working on cleaning up the offboarding tickets.
C5.5	The Department will review and clarify the employee offboarding process and will remind staff of service request requirements.
C5.10	The Department will review the list of individuals with administrative rights and modify access as necessary.

DEPARTMENT OF INNOVATION AND TECHNOLOGY
Corrective Action Plan
(Not Examined)

C5.15 The Department will research opportunities to generate reports in the requested format for future audit testing. Additionally, the Department will remind staff of the service request requirements.

C5.16 The Department continues completing the RACF reconciliation.

C8.2 It is common that some endpoints will be out of compliance at any given time due to being offline, out of network connectivity, and other reasons. The Endpoint Protection team utilizes a process to investigate and correct endpoints that are out of compliance. The team will continue to investigate and address any out-of-date files or updates as well as additional tools.

C9.2 The Department will continue to back up devices before implementing a tool migration in order to minimize risk and allow for recovery of the backup as needed.

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 planning model, as well as recovery activation and response plans include 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. FY21 testing involved mainframe and midrange information system contingency plans testing. Testing included mainframe infrastructure, CCF generator, 4 mainframe applications and 18 live SDDC application failover tests, and 2 midrange application tabletop tests. Annual testing of the State of Illinois Cyber Disruption Plan was also conducted with IEMA, Illinois State Police, Illinois National Guard, and Statewide Terrorism and Intelligence 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. 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, along with the implementation of snapshots and Site Recovery Manager (SRM) of the mainframe environment. The midrange environment has also implemented SRM within the hyperconverged hardware and hybrid cloud software to build a geo-diverse private cloud software defined data center (SDDC) spread between both State of Illinois data centers.

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

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

85 Office of the State Appellate Defender
86 Office of the State Fire Marshal
87 Office of the State's Attorneys Appellate Prosecutor
88 Office of the Treasurer
89 Pollution Control Board
90 Property Tax Appeal Board
91 Secretary of State
92 Senate Operations
93 Southern Illinois University
94 State Board of Education
95 State Board of Elections
96 State Charter School Commission
97 State Employees' Retirement System
98 State of Illinois Comprehensive Health Insurance Board
99 State Police Merit Board
100 State Universities Civil Service System
101 State Universities Retirement System
102 Supreme Court Historic Preservation Commission
103 Supreme Court of Illinois
104 Teachers' Retirement System of the State of Illinois
105 University of Illinois
106 Western Illinois University

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

1. General Assembly Retirement System
2. Illinois Board of Higher Education
3. Illinois Community College Board*
4. Illinois Law Enforcement Training & Standards Board
5. Illinois Student Assistance Commission
6. Judges' Retirement System
7. Office of the Attorney General*
8. Office of the State's Attorneys Appellate Prosecutor
9. State Board of Elections*
10. State Employees' Retirement System
11. State Universities Civil Service System*
12. Supreme Court of Illinois

*Transitioned to the Statewide Enterprise Resource Planning System on July 1, 2021.

Provided by the Department of Innovation and Technology

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

1. Abraham Lincoln Presidential Library and Museum
2. Capital Development Board
3. Commission on Government Forecasting and Accountability
4. Coroner Training Board
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 Financial and Professional Regulation
13. Department of Healthcare and Family Services
14. Department of Human Rights
15. Department of Human Services
16. Department of Innovation and Technology
17. Department of Insurance
18. Department of Juvenile Justice
19. Department of Labor
20. Department of the Lottery
21. Department of Military Affairs
22. Department of Natural Resources
23. Department of Public Health
24. Department of Revenue
25. Department on Aging
26. Environmental Protection Agency
27. Executive Ethics Commission
28. General Assembly
29. Governor's Office of Management and Budget
30. Guardianship and Advocacy Commission
31. Human Rights Commission
32. Illinois Arts Council
33. Illinois Board of Higher Education
34. Illinois Civil Service Commission
35. Illinois Commerce Commission
36. Illinois Community College Board
37. Illinois Council on Developmental Disabilities
38. Illinois Deaf and Hard of Hearing Commission
39. Illinois Educational Labor Relations Board
40. Illinois Emergency Management Agency
41. Illinois Gaming Board
42. Illinois Health Information Exchange Authority
43. Illinois Independent Tax Tribunal
44. Illinois Labor Relations Board

Provided by the Department of Innovation and Technology

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

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

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

Provided by the Department of Innovation and Technology

41. State Employees' Retirement System
42. State of Illinois Comprehensive Health Insurance Board

Listing of User Agencies of the Department's 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. Executive Ethics Commission
17. Guardianship and Advocacy Commission
18. Illinois Civil Service Commission
19. Illinois Council on Developmental Disabilities
20. Illinois Deaf and Hard of Hearing Commission
21. Illinois Emergency Management Agency
22. Illinois Gaming Board
23. Illinois Labor Relations Board
24. Illinois Liquor Control Commission
25. Illinois Prisoner Review Board
26. Illinois Procurement Policy Board
27. Illinois Racing Board
28. Illinois State Police
29. Illinois Workers' Compensation Commission
30. Office of the Executive Inspector General
31. Property Tax Appeal Board
32. State Employees' Retirement System
33. State of Illinois Comprehensive Health Insurance Board

Provided by the Department of Innovation and Technology

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. Coroner Training Board
6. Court of Claims
7. Department of Agriculture
8. Department of Central Management Services
9. Department of Human Rights
10. Department of Innovation and Technology
11. Department of Labor
12. Department of Military Affairs
13. Department of Veterans Affairs
14. Eastern Illinois University
15. Emergency Management Agency
16. Executive Ethics Commission
17. Governors State University
18. Governor's Office of Management and Budget
19. Guardianship & Advocacy Commission
20. House of Representatives
21. Human Rights Commission
22. Illinois Arts Council
23. Illinois Civil Service Commission
24. Illinois Commerce Commission
25. Illinois Community College Board
26. Illinois Council on Developmental Disabilities
27. Illinois Deaf and Hard of Hearing Commission
28. Illinois Educational Labor Relations Board
29. Illinois Finance Authority
30. Illinois Housing Development Authority
31. Illinois Independent Tax Tribunal
32. Illinois Law Enforcement Training and Standards Board
33. Illinois Mathematics and Science Academy
34. Illinois Power Agency
35. Illinois Prisoner Review Board
36. Illinois State Toll Highway Authority
37. Illinois State University
38. Joint Committee on Administrative Rules
39. Judicial Inquiry Board
40. Labor Relations Board
41. Legislative Audit Commission

42. Legislative Ethics Commission
43. Legislative Information System
44. Legislative Printing Unit
45. Legislative Reference Bureau
46. Liquor Control Commission
47. Medical District Commission
48. Northeastern Illinois University
49. Northern Illinois University
50. Office of Executive Inspector General
51. Office of Legislative Inspector General
52. Office of State Appellate Defender
53. Office of the Architect of the Capitol
54. Office of the Attorney General
55. Office of the Comptroller
56. Office of the Governor
57. Office of the Lieutenant Governor
58. Office of the Secretary of State
59. Office of the State's Attorneys Appellate Prosecutor
60. Office of the Treasurer
61. Procurement Policy Board
62. Property Tax Appeal Board
63. Senate
64. Southern Illinois University
65. State Board of Education
66. State Board of Elections
67. State Board of Investment
68. State Fire Marshal
69. State Police Merit Board
70. State Universities Civil Service System
71. State Universities Retirement System
72. Supreme Court Historic Preservation Commission
73. University of Illinois
74. Western Illinois University

ACRONYM GLOSSARY

Act – Department of Innovation and Technology Act
AD – Active Directory
ADC – Alternate Data Center
ADFS - Active Directory Federal Services
AIS – Accounting Information System
AIX – Advanced Interactive eXecutive
APIs – Application Program Interfaces
ATSR – Agency Technology Service Requester
CAC – Change Advisory Committee
CCF – Central Computer Facility
CEP – Comprehensive Employment Plan
CICS – Customer Information Control System
CIOs – Chief Information Officers
CISO – Chief Information Security Officer
CJIS – Criminal Justice Information Services
CMOS – Complementary Metal Oxide Semiconductor
CMS – Central Management Services
CPS – Central Payroll System
CTAS – Central Time and Attendance System
DB2 – Database 2
DCMS – Department of Central Management Services
Department – Department of Innovation and Technology
DIM – Department's Identity Management
[redacted]
DoIT – Department of Innovation and Technology
EAA – Enterprise Application & Architecture
Employee Portal - intranet
ERP – Enterprise Resource Planning
[redacted]
EUC – End User Computing
FTI – Federal Tax Information
FTPS – File Transfer Protocol Secure
GRC – Governance, Risk and Compliance
GUI – Graphical User Interface
HR – Human Resources
ICN – Illinois Century Network
ID – Identification
ILCS – Illinois Compiled Statutes
IMS – Information Management System
IT – Information Technology
JCL – Job Control Language
LAN – Local Area Network
MIM – Microsoft Identity Management
MORT – Major Outage Response Team

MS-ISAC – Multi-State Information Sharing and Analysis Center
NIST – National Institute of Standards and Technology
Obligations data - contracts
ORAQ – Organization Risk Assessment Questionnaire
OS – Operating System
PAR – Personnel Action Request
PCI – Payment Card Industry
PHI – Protected Health Information
PSC – Personal Service Contractor
ROD – Remedy on Demand
RMP – Risk Management Program
SAMS – Statewide Accounting Management System
SAP – Systems, Applications and Products
SOC – System and Organization Controls
SOC – Security Operation Center
SSO – Single SignOn
SQL – Structured Query Language
Velocity – Velocity Access Control System
VPN – Virtual Private Network
WAN – Wide Area Network
z/OS – Zero Downtime Operating System
z/VM – Zero Downtime Virtual Machine