STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY
STATE OF ILLINOIS, ENTERPRISE RESOURCE PLANNING SYSTEM

REPORT ON THE DESCRIPTION OF SYSTEM, SUITABILITY OF DESIGN, AND OPERATING EFFECTIVENESS OF CONTROLS
FOR THE PERIOD
JULY 1, 2019 THROUGH JUNE 30, 2020

STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY

TABLE OF CONTENTS

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

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

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

OFFICE OF THE AUDITOR GENERAL
FRANK J. MAUTINO

INDEPENDENT SERVICE AUDITOR'S REPORT ON THE STATE OF ILLINOIS, DEPARTMENT OF INNOVATION AND TECHNOLOGY'S DESCRIPTION OF ITS ENTERPRISE RESOURCE PLANNING 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 the State of Illinois, Enterprise Resource Planning System 'system' of which are included in the "Description of the State of Illinois, Enterprise Resource Planning System for the IT General Controls and Application Controls" for the user entities throughout the period from July 1, 2019 to June 30, 2020, (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 State of Illinois, Enterprise Resource Planning 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 Virtustream, Inc. to provide cloud hosting services for the State of Illinois, Enterprise Resource Planning system. 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 organization, 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 State of Illinois, Enterprise Resource Planning System made available to user entities during the period from July 1, 2019 to June 30, 2020. Information about the State of Illinois, Department of Innovation and Technology's corrective action plan, business continuity and disaster recovery, and user entity listings has not been subjected to procedures applied in the examination of the description of the State of Illinois, Enterprise Resource Planning 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 State of Illinois, Enterprise Resource Planning System and, accordingly, we express no opinion on it.

Service Organization Responsibilities

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

Service Auditor's Responsibilities

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in *Government Auditing Standards*, issued by the Comptroller General of the United States and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on criteria in management's assertions, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period from July 1, 2019 to June 30, 2020. 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 control system. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization or a subservice organization may become ineffective.

Description of Tests of Controls

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

Basis for 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 require access modifications to the State of Illinois, Department of Innovation and Technology's resources to begin with the submission of a Remedy service request from an authorized Agency Technology Service Requester or Department IT Coordinator. However, as noted at page 48 of the description of tests of controls and results, a population of 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."

2) The State of Illinois, Department of Innovation and Technology states in its description that it has controls in place to require access revocation to the State of Illinois, Department of Innovation and Technology's resources be initiated upon receipt of a Remedy service request, or under special or emergency circumstances, by instruction of senior management. However, as noted at page 48 of the description of tests of controls and results, documentation of the timely termination of an individual's access 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."

3) As indicated in the accompanying description of the State of Illinois, Department of Innovation and Technology, ethics training was not conducted during the examination period; therefore, we did not perform any tests of design or operating effectiveness of controls related to the control objective, "Controls provide reasonable assurance that policies and procedures related to employee responsibilities and hiring have been established, new employees and contractors are screened and on-boarded, and a defined organizational structure exists, that are relevant to user entities' internal control over financial reporting."

4) 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 HANA user during the control period; therefore, we did not perform any tests 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."

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, Enterprise Resource Planning System that was designed and implemented throughout the period from July 1, 2019 to June 30, 2020.

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, 2019 to June 30, 2020; 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, 2019 to June 30, 2020.

c. the controls operate effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period from July 1, 2019 to June 30, 2020 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, 2019 to June 30, 2020.

Emphasis of Matter

As noted in the Description of the State of Illinois, Enterprise Resource Planning System for the IT 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 State of Illinois, Enterprise Resource Planning System for the IT 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 5, 2020 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 State of Illinois, Enterprise Resource Planning System throughout the period July 1, 2019 to June 30, 2020, 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 State of Illinois, Enterprise Resource Planning System throughout the period July 1, 2019 to June 30, 2020 (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, Enterprise Resource Planning System during some or all of the period from July 1, 2019 to June 30, 2020, 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 5, 2020
Springfield, Illinois

SECTION II

DEPARTMENT OF INNOVATION AND TECHNOLOGY'S ASSERTION REGARDING THE STATE OF ILLINOIS, ENTERPRISE RESOURCE PLANNING SYSTEM

Honorable Frank J. Mautino
Auditor General, State of Illinois

We have prepared the description of the State of Illinois, Enterprise Resource Planning System 'system' entitled "Description of the State of Illinois, Enterprise Resource Planning System for the IT General Controls and Application Controls" for the information technology general controls and application controls throughout the period from July 1, 2019, to June 30, 2020, (description) for user entities of the system during some or all of the period from July 1, 2019, to June 30, 2020, 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 a subservice organization to provide cloud hosting services for the State of Illinois, Enterprise Resource Planning System. 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 organization. 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 State of Illinois, Enterprise Resource Planning System 'system' made available to user entities of the system during some or all of the period July 1, 2019, to June 30, 2020, 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 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 State of Illinois, Enterprise Resource Planning System 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, 2019 to June 30, 2020 to achieve those control objectives if user entities applied the complementary user entity controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls throughout the period from July 1, 2019 to June 30, 2020. 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 29 of the description that controls are in place to require access modifications to the State of Illinois, Department of Innovation and Technology's resources begin with the submission of a Remedy service request from an authorized Agency Technology Service Requester or Department IT Coordinator. However, we were

unable to provide a population of access modifications to the State of Illinois, Department of Innovation and Technology's resources. 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."

b) We state on page 29 of the description that controls are in place to require access revocation to the State of Illinois, Department of Innovation and Technology's resources be initiated upon receipt of a Remedy service request, under special or emergency circumstances, by instruction of senior management. However, we were unable to provide documentation of the timely termination of an individual's access to the State of Illinois, Department of Innovation and Technology's resources. 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."

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

During the period July 1, 2019 to June 30, 2020, the Department did not conduct ethics training and did not have a request for a new HANA user.

SIGNED ORIGINAL ON FILE

Ron Guerrier
Secretary
Department of Innovation and Technology
August 5, 2020

SECTION III

DESCRIPTION OF THE STATE OF ILLINOIS, ENTERPRISE RESOURCE PLANNING SYSTEM FOR THE IT GENERAL CONTROLS AND APPLICATION CONTROLS

Overview of the Department of Innovation and Technology

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

Subservice Organizations

The Department utilizes Virtustream, Inc. to provide cloud hosting services for the State of Illinois Enterprise Resource Planning (ERP) System.

Overview of Services Provided

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

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

Scope of the Description

In accordance with the criteria in management's assertion, this Description includes a description of the Department's Information Technology (IT) General Controls and Application Controls for the State of Illinois ERP System provided to agencies. The Description excludes the control objectives and related controls of Virtustream, Inc.

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 for the State of Illinois ERP System that are relevant to an agency's internal control over financial reporting.

Internal Control Framework

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

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

Control Environment

Organizational Structure

The Department's organizational hierarchy supports internal control starting with the Department's Secretary. The Secretary is a member of the Governor's Cabinet and is the "Chief Information Officer for the State and the steward of State data with respect to those agencies under the jurisdiction of the Governor" per Section 1-30 of 20 ILCS 1370. During the examination period, one individual serves as Acting Secretary.

The Acting Assistant Secretary (vacant from July 1, 2019 to February 9, 2020) directly supervises the DoIT Group CIOs and applies primary focus on application development and technology delivery.

The Department's organizational hierarchy promotes separation of duties, monitoring ofcontrols, 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, ERP Program Director, and seven Chief Information Officers (CIOs) grouped into service delivery taxonomies.

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

The Chief Administrative Officer (vacant from March 2, 2020 to present) consults with the Secretary and senior management to facilitate functional compatibility and alignment of Department objectives. Subordinate managers oversee the Department's Legal Services, Human Resources, and Procurement. From July 1 to July 15, 2019, Property Control function and staff reported to the Chief Customer Officer. Effective July 16, 2019, and approved by CMS on October 1, 2019, Property Control function and staff were moved organizationally from the Chief Customer Officer to report to the Chief Administrative Officer.

The Chief Internal Auditor 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, 2019 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. This position is responsible for the delivery of customer-facing IT services, customer support, and change control.

The Chief of Staff advises the Secretary on the transformation status of legacy agency resources (personnel and equipment) to meet the requirements of the Act and provides the authority for transferring State resources into the Department. The Chief of Staff also supervises functional areas of the Department's fiscal officer, budget director, legislative liaison, and communications/public information manager.

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

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, and software distribution. Each of these business functions have been assigned separate managers.

The Chief Data Officer (vacant from July 1, 2019 to November 17, 2019) 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 serves State of Illinois constituents; drives an evolving use of emerging technologies to support the best process for increased data availability.

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

The seven Group CIOs promote quality of service and enhance the effectiveness of the Department's internal control environment through information exchange, general oversight of agency information processing, and strategic planning participation. The Group CIOs enhance agency awareness of Department policies, procedures, objectives, and new initiatives as well as providing a channel to communicate agency concerns and recommendations. These responsibilities have been categorized into seven (7) groups reflecting Statewide agency services. Categories are (1) family, children, elderly, and veterans; (2) government and public employees; (3) business and workforce; (4) natural and cultural resources; (5) public safety; (6) education; and (7) transportation. Vacancies within the Group CIOs include: Family, Children, Elderly, and Veterans vacant from July 1, 2019 to December 1, 2019; the Education (formerly referred to as students until February 9, 2020) Group CIO vacant from September 16, 2019 to November 17, 2019; Transportation Group CIO has not yet been filled.

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

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

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

Human Resources (HR) and the appropriate supervisor/manager verifies the accuracy of the job description or PSC description of services and identification of funding. The Department's HR prepares a Personnel Action Request (PAR) form used to initiate the posting of the employment opportunity. Prior to August 30, 2019, job postings advertised only the full salary range, as prescribed by the pay plan. As a result of Amendments to the Equal Pay Act and in accordance with the August 29, 2019, "Follow-up to Yesterday's Equal Pay Act Amendments Training" memorandum from DCMS, beginning with positions posted August 30, 2019, job postings advertise the full salary range, as prescribed by the pay plan in addition to an anticipated starting salary determined by the hiring agency and the collective bargaining unit salary range for bargaining unit covered positions. The Secretary and the Department's Chief Fiscal Officer approve the PAR prior to HR's posting of the position.

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

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

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

"At will" positions require approval from the Office of the Governor in order to be filled. When filling "at will" positions, the HR Director is responsible for certifying the selected candidate meets minimum qualifications as stated in the job description. Prior to July 8, 2019, the completed certification form was provided to the Office of the Governor, the Office of the Executive Inspector General Hiring and Employment Monitor and the Special Master prior to the candidate's first working day. Per directive from the Office of the Governor, effective July 8, 2019, the completed certification form is provided only to the Office of the Governor prior to the candidate's first working day.

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

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

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

Newly-hired employees are provided the DCMS Policy Manual by HR during New Employee Orientation and are required to sign an acknowledgment form accepting responsibility to abide by the policies contained within the DCMS Policy Manual. Newly-hired PSCs are governed by the terms, conditions, and duties outlined in their legally-binding contract. PSCs acknowledge and accept compliance with Department policies and procedures, as each contract states that the "Contract Employee agrees to be bound by and comply with policies and procedures of the Agency." New Employee Orientation is being conducted virtually beginning April 1, 2020 due to COVID-19 remote work directives.

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

Newly-hired employees and PSCs are directed to complete the following annual trainings via paper or through OneNet: Security Awareness Training, Safeguard Disclosure Training, Ethics Training and Sexual Harassment Prevention Training. Newly-hired employees and PSCs are required to take one-time Acceptable Use Policy training effective September of 2019, which is tracked by the Department Security Program Manager.

As directed by the Act (20 ILCS 1370), the Department transitioned existing, permanent State employees from other agencies into the Department in order to achieve consolidation of IT resources. Transition and consolidation of these workforce members fall outside the normal, personnel hiring regulations.

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

- Receiving notification from the Governor's Office of Management and Budget (GOMB) that sufficient funds are available to proceed with the transition effort;
- Notifying the affected unions of the effective date of the transformation;
- Notifying the affected employees of the effective date of the transformation and if pay dates will change;
- Notifying the impacted agencies of the effective date of the transformation and providing them with a transformation checklist to be completed and returned for each impacted employee;
- Providing a spreadsheet to DoIT Enterprise Applications Membership and Benefits Manager to have the impacted employees transferred systematically from their legacy agency to DoIT's "org proc" code in the benefits system;
- Conducting abbreviated New Employee Orientation for transforming employees;
- Providing/obtaining updated documents and fulfilling training requirements;
- Coordinating with and receiving applicable personnel, medical, benefit and payroll files from legacy agencies for each transferred employee;
- Identifying and processing appropriation code changes in the DCMS Personnel System for each impacted employee on the effective date;
- Printing and distributing CMS-2 turnaround documents for each transitioned employee to Payroll, Benefits, Timekeeping and HR;
- Distributing completed CMS-204 forms, as well as the transformation checklist forms, received from legacy agency to Payroll, Benefits, Timekeeping and HR;
- Entering affected employees into HRIS (if they aren't already in HRIS), HR, Central

Payroll System, eTime and Central Time and Timekeeping Systems;
- Reconciling vacation base dates, updating and requesting any new schedule changes through DCMS' Compensation to maintain employee's current schedule;
- Verifying every payroll deduction listed on the transformation checklist and the CMS-204 form; confirming every payroll deduction has a corresponding supporting document;
- Updating organizational charts; and
- Assembling newly-transformed employees' personnel and payroll files including appropriation code change (CMS-2) and transformation checklists.

Voluntary separation procedures for an employee or a contractor result in HR generating an electronic Employee Exit Form (Exit Form) which is emailed to the supervisor. Once the Exit Form is completed by the supervisor, it is automatically forwarded to the Department IT Coordinator group via email which then prompts the Department IT Coordinator group to initiate the process of creating a Remedy service request to disable access and return equipment.

For an employee voluntarily separating from the Department (transferring, resigning, or retiring), once HR receives written confirmation from the employee, HR initiates a PAR, obtains appropriate Department authorizations from the Chief Fiscal Officer and the Secretary, and initiates the Exit Form. For an employee non-voluntarily being terminated from the Department, once HR receives either written or verbal direction from the Secretary or his designee, HR coordinates with the employee's manager to execute the separation process. For a PSC, the separation process begins upon expiration or termination of the contract at which time an electronic Exit Form is generated. Once the electronic Exit Form is completed by the supervisor, it is automatically forwarded to the Department IT Coordinator group which then initiates the process of creating a Remedy service request to disable access and return equipment.

Risk Assessment Process

The Department follows the IT Risk Assessment Policy published on the Department's website. The Risk Assessment Policy assigns responsibility for conducting risk assessments and vulnerability scanning to the Department with the scope spanning entities identified as client agencies under executive orders, compiled statutes, or inter-governmental agreements. The Risk Assessment Policy also requires the Department to share assessment results with client agency senior management and appropriate designees.

During the period of July 1, 2019, to September 8, 2019, the Department followed the Risk Management Program which describes the State of Illinois Risk Management process from data and system categorization to maturity level of existing security controls. Effective September 9, 2019, the Department reviewed and updated the Risk Management Program to reflect the current process.

The Risk Management Program describes the data and system categorization process of mission critical information systems. The results and conclusions of the risk assessment is used as leverage to justify expenditures, manpower, time, budgeting, technology purchases, and general procurements.

The Department conducts organizational risk assessments based on National Institute of Standards and Technology (NIST) security and privacy controls for agencies, boards, and commissions that report to the Governor. Based on the Department's Risk Management Program, a series of steps are followed to conduct a risk assessment. Each agency is provided an organization risk assessment survey and agency responses are given a qualitative maturity value for existing security controls. The results are calculated and help to identify and prioritize potential security weaknesses. The risk assessments are conducted based on the Department's workload and the client agency availability.

Agencies are responsible for providing mitigation plans corresponding to risk assessment results. Risks and mitigation plans are captured in a Risk Register by the Risk team for follow-up. The Risk team contacts agencies based on their risk mitigation anticipated completion date to confirm risk remediation implementation. Agency risk remediation efforts are documented and updated in the Risk Register, and artifacts are stored in their individual risk folders.

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 employees and vendor subscription services. The Department also maintains contact with vendors to receive patch vulnerability information.

A vulnerability scanning process is employed to assess servers identified through server discovery scan for each agency. Vulnerability scans are scheduled weekly. The Department shares vulnerability scanning results with Group CIO's and agency CIO's via email weekly. The Department provides client agencies with the Agency Instructional Guide for Submitting Vulnerability and Remediation Tickets to mitigate identified server vulnerabilities. Unremediated vulnerabilities will continue be reported in the weekly scan reports. In the case where remediation efforts have failed or caused operational issues, corrective action plans are developed by agency CIO. Agencies are responsible for providing corrective action plans to remediate identified server vulnerabilities.

Information and Communications

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 user agencies)
- Instructions on how to order services and products as well as how to report operational problems.

The policies located on the Department's website include:

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 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. The DoIT Digest publication is scheduled every two weeks. Due to COVID-19, beginning April 3, 2020, the DoIT Digest has been published weekly to include topics related to COVID-19 and the work from home effort.

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 Requestor (ATSR) known as Department IT Coordinators through November 2019 transition period) as appropriate to the message being conveyed. Group CIOs provide an exchange of information between the Department and agencies and keep both the Department and agencies informed regarding significant events, service issues, improvements, processes, and strategic goals. Group CIOs meet with agency CIOs when business need requires or when

instructed by Department management to update and gather information from agencies. Group CIO communication occurs at an individual agency level. State-wide level agency communication is accomplished through CIO Council meetings which are held at the Secretary's request to update and inform agency CIOs of news and information.

Agency CIOs, along with Department leadership, are invited to attend "DoIT Daily" meetings (Mondays through Thursdays). DoIT Daily is a forum to share high-level and high-risk operational issues with a team equipped to discuss steps for resolution. Due to COVID-19, the DoIT Daily meetings have changed to Mondays through Fridays effective March 20, 2020 while working remotely.

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

SoundBytes is an employee blog located on the employee portal which provides a communication channel where Department employees can exchange information and updates. The blog is intended to serve as a platform for Department employees to communicate and connect virtually. The posting categories include:

- Celebrating Employees
- Comings & Goings
- Health & Fitness
- News & Updates
- Outside of Work
- Secretary G's Corner

SoundBytes allows all employees to create posts, which are then moved to a pending status. Members of the communication team are notified when there is a new post and they can either approve or reject the post.

Due to COVID-19 and State employees working remotely, beginning March 26, 2020, Remote Work – Reminder of the Day has been published daily to share information to facilitate work from home. A Remote Work webpage was published on the Department's website March 16, 2020 to provide guidelines and additional resources to support employees working remotely. Beginning June 8, 2020, Remote Work – Reminder of the Day is published as needed when there is remote work news or information to share.

The Department communicates ERP information to the agencies in the following ways:

- Through its Production Support team. Production Support initiates all incident related communications from a dedicated email address or the email addresses of individual team members. Depending on the nature of the incident and the level of coordination and

communication needed, Production Support also communicates with agencies via phone, or in person. Descriptions of all functional weekly releases are also sent from the dedicated Production Support email address.
- From a dedicated ERP team email address: These communications typically include notices for planned or emergency outages of the ERP system.
- Monthly user group meetings – ERP staff provides information regarding new functionality and support for issues being experienced by user agencies.
- Participation in weekly chief Fiscal/ Financial Officer meetings.

Agencies are encouraged to contact the ERP Team:
- IT Service Desk via Remedy ticket for all problems experienced with the ERP.
- Individual ERP team members via email or phone for any business process questions.

In addition, policies and procedures are maintained on SharePoint.

Monitoring

Monitoring of Department Services and Performance

Effective July 15, 2019, the Audit Committee was formed to assist the Secretary in fulfilling his responsibilities for effectively and efficiently managing and maintaining an effective system of internal control. The Audit Committee consists of Chief of Staff, Chief Administrative Officer, and General Counsel. Effective February 10, 2020, the Audit Committee consists of Acting Assistant Secretary, Chief of Staff, Chief Administrative Officer, and General Counsel. The Audit Committee's responsibilities include monitoring of: internal controls, internal audits, external audits, and reporting responsibilities. The Committee is to meet four times per year, with the authority to convene more frequently if requested.

Customer Support Division staff conducts monthly meetings 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. Effective January 2020, the Customer Support Division staff changed the meeting frequency to quarterly, with the authority to convene more frequently if requested. In addition to storing data on a SharePoint site, service level metrics showing the Department customer service performance are posted on the Department's website.

Monitoring of Subservice Providers

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

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

Information Systems Overview-ERP

The Department implemented SAP's Enterprise Resource Planning (ERP) system on October 1,

2016. The ERP integrates the finance, human resource, procurement, and other financial related areas into a single system. The ERP Central Component (ECC) is comprised of the following modules:

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

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

On July 1, 2018, the Illinois Tollway was added as a user agency of the ERP System. While all the same modules are being used, the business requirements of the Illinois Tollway varied from those of other State of Illinois user agencies, which resulted in the need to customize the enterprise design. All agencies except the Illinois Tollway are organized in the STIL company code. The Illinois Tollway uses the ILTA company code and its functionality differences as related to controls are noted in the descriptions below. Additionally, the Department's ERP Functional Experts referenced in the sections below continue to support the entire enterprise, including the Illinois Tollway. However, due to unique business requirements, one Tollway staff person has been granted certain master data maintenance access for the ILTA company code.

The user agencies are responsible for the complete, accurate, and timely entry of data into the ERP. The Department is responsible for updates and maintenance to the ERP System.

General Ledger
The General Ledger records the financial transactions of the agencies. The General Ledger and chart of accounts master data elements govern the manner in which budgets, revenues/receipts, transfers, bonds, federal funds, or expenditures of the agency are recorded. The maintenance of the General Ledger Illinois Office of Comptroller Accounts (IOCA) (State of Illinois-STIL) chart of accounts is maintained by the General Ledger Functional Expert. The maintenance of the General Ledger ILTA (Illinois Tollway) chart of accounts is maintained by authorized master data maintenance Tollway staff and moved into Workflow approval by the General Ledger Functional Expert.

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

Each transaction is posted to the General Ledger with the associated history and documentation.

A transaction is created when a document is created and assigned a document number. In addition, Journal Entries (JE) can be made to record adjustments and month/year end adjustments.

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

Period End Closing
The fiscal year variant is the periods utilized in posting transactions. The Department is utilizing 12 regular months (July through June) with the 13th month being utilized for lapse period transactions for Company Code STIL. Periods 14 – 16 can be utilized for any special one-time adjustments. The Tollway is utilizing 12 regular months (January through December) and does not operate in lapse period, however, period 13 could be utilized for special adjustments on Company Code ILTA.

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

On the last day of the month for Company Code STIL, the General Ledger Functional Expert will open the next accounting period (next month) in order for agencies to post to the next month. In addition, the General Ledger Functional Expert will close the prior period.

- Closing of a period is to be conducted for Company Code STIL:
    - Monthly-last day of the month,
    - Quarterly-March, September, and December,
    - Year end-June, and
    - Lapse-after lapse activities are completed.

The General Ledger Functional Expert will open the next accounting period (next month) for Tollway (ILTA) at the same time the period is opened for Company code STIL for the agency to post to the next month. The General Ledger Functional Expert will close the prior period for Tollway (ILTA) when a request to do so is received from the Tollway.

- Closing of a period is to be conducted for Company Code ILTA:
    - Monthly-last day of the month,
    - Quarterly-March, June and September, and
    - Year end-December.

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

Periods one through twelve for fiscal year 2020 remain open for STIL. Periods six for calendar year 2020 is open for ILTA.

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

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

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

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

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

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

Effective January 1, 2020, the Department of Healthcare and Family Services began utilizing Locally Held Funds (LHF) functionality for payments that are not sent through Illinois Office of the Comptroller. The LHF Processor has the ability to issue checks directly from the ERP. Check signatures are applied electronically. Checks are cleared once the bank statement is received, and the agency submits a file with check information to the ERP Production Support for processing.

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

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

An asset acquisition is entered into the asset shell record in order to be added to SRM. Once the

asset has been "receipted" from the Purchase Order, the capitalization date and value are added to the asset shell. At this time, the asset number (tag number) is created; assigned by the agency.

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

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

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

On the first day of each month, a batch job is run which calculates the monthly depreciation for that month. In addition, to accommodate a requirement from the Office of the Comptroller for STIL agencies (excluding the Illinois Tollway), a second batch job is run for the monthly depreciation on new, disposed-of and transferred assets. The Illinois Tollway records the depreciation on new, disposed of and transferred assets in the subsequent month. At the completion of each batch job, the calculated depreciation is recorded against the asset and the general ledger depreciation account.

In the event a correction needs to occur in a period which has been closed, the agency must contact the Assets Functional Expert in order to make the needed correction. For corrections that relate to a transaction in a closed period that can be made in an open period, agencies can either contact the Asset Functional Expert or, effective January 1, 2020, the user at their agency with the Asset Adjustor profile can make this correction.

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

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

Material Management

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

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

Cart directs the required approvals; supervisor, manager, and fiscal staff.

Upon taking delivery of the services/materials, the goods receipt is completed, thus allowing the posting of invoices. An invoice cannot be posted to the Purchase Order until a receipt of goods/services is completed. Effective January 1, 2020, the warehouse management functionality was added which allows the received materials that are stored in warehouses, to be tracked at a more granular level.

If requesting inventory from agency warehouse stock, a Purchase Requisition (Shopping Cart) is created and approved. At that time a check is made to determine if stock is available. If there is available stock, a reservation is created and subsequently delivered. In the event stock is not available, a Purchase Order is created. The Tollway also uses a Purchase Requisition (Shopping Cart) to request inventory from stock. However, if stock is available a Stock Transport Order is created instead.

Public Sector Collection & Disbursements (PSCD)
Public Sector Collection and Disbursements provide for the activities associated with billings, payments, and Accounts Receivable (AR). The posting of AR is through a document against the Customer's Contract Object. The customer's master data is comprised of a three-tier hierarchy:

- Business Partner (Customer) – the central level of all data associated with the customer. Customer number is based on SSN, FEIN or a unique agency ID. All agencies have access to this level.
- Contract Account – this level is associated with a specific agency's activities; posting of agency payment methods, interest calculations, conditions or dunning procedures, billing methods, etc. At this level a Contract Account number is assigned to the customer which is unique to a specific agency.
- Contract Object – the third level, defines the Customer's account with additional detail, specific licenses, taxes, claims, etc. At this level a Contract Object number is assigned to the customer which is unique to a specific agency

When activity is conducted by the Customer or the agency, the activity is posted at the Contract Object level. Additionally, in the event the Customer conducts activity, but does not submit payment immediately, the AR is established at the Contract Object level.

Effective July 25, 2019, any adjustment, reversal, or write-off of receivables is routed through an approval prior to posting to the PSCD or the General Ledger. Once a Receivables Processor saves an adjustment or reversal, the Receivable Oversight is notified of the document awaiting approval. The Receivable Oversight is to review and approve the document. At that time, the document is posted to the General Ledger. In the event the Receivable Oversight rejects the document, it is returned to the Collections Processer. Within the document, the Receivable Oversight is to document the issues noted. This same process applies to write-offs, but are initiated by the Receivable Reconciler and approved by the Receivable Oversight. Prior to July 25, 2019, approvals were captured outside of ERP. The posting of payments is completed by utilizing the Check Lot functionality which allows an agency to post payments that will be processed to the Comptroller on an Expenditure Adjustment Transmittal (EAT) (C-63) or Receipt Deposit Transmittal (RDT) (C-64). When utilizing Check Lot, the total of the individual payment posting

must agree with the total of Check Lot.

Once the Treasurer's draft is received, the applicable RDT or EAT is created. Upon creation, the consolidated RDT file is signed and sent to the Office of the Comptroller, along with a batch file of the RDTs.

Any payment(s) required to be processed on the EAT form (C63) are still transmitted to the Office of the Comptroller in a paper format.

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

The reversal of payments is routed through the same process as noted for receivables, above.

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

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

For Company Code STIL, upon the passage of a budget, approved budget numbers (appropriations) are established at the fund level by the Office of the Comptroller. Then via an interface, the budget numbers are entered. After entry, agencies may maintain the budget numbers at the upper level (superior Funds Center) or can distribute to lower levels based on the agency's specific needs; specific Funds Center, Commitment Items, Funded Programs. In the event a new fund needs to be established, a request from the Office of the Comptroller or an agency is received, via a Help Desk Ticket or email. The FM Functional Expert with Firefighter access completes the creation of the new fund. The FM Functional Expert also creates/edits FM master data and budget/appropriation on behalf of all agencies.

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

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

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

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

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

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

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

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

Master Data

- Primary Cost Elements: Primary Cost Elements are the links between the Financial Accounting (FI) module and Controlling (CO) module. Every revenue and expense General Ledger Account (GL Account) in FI is defined as a Revenue Element or Cost Element in CO. When a transaction is processed in FI to a revenue or expense GL Account, at the same time a posting is made to the corresponding Revenue Element or Cost Element in CO. The Primary Cost Elements are created at the same time as their corresponding General Ledger Account.
- Secondary Cost Elements: Secondary Cost Elements are revenue and expense components used to allocate costs as needed among CO Cost Objects including Cost Centers, Internal Orders, and Work Breakdown Structure elements (WBS). Because Secondary Cost Elements are only used for the reclassification among Cost Objects of costs already incurred in Primary Cost Elements, Secondary Cost Elements are not linked to any

component in FI. Accordingly, these allocation postings are not reflected in FI.

- Statistical Key Figure (SKF): Statistical Key Figures are quantitative amounts used in allocation rules. These form the basis of allocation of costs from a Cost Center to other Cost Centers or Cost Objects.

Services Provided to User Agencies
Master Data Maintenance – The IL ACTS CO Functional Expert executes new requests or request for change to cost center master data using their Steady State Fire Fighter ID. Internal Order and Work Breakdown Structure creation and maintenance is performed by user Agency personnel.
Change Management Support – Any testing/approvals required as part of incident resolution or new change requests.

HANA Analytics
The HANA Analytics functionality provides agency end users with enhanced reporting capabilities. Users can query their own agency data against views that have been built by the IL ACTS Program team. Based on defined roles, users are also provided access to Business Intelligence tools that allow an end user to develop their own report. Additionally, the ERP team creates enterprise reports that are available to end users based on their access. On March 30, 2020, the SB01 Expenditure Reconciliation report was made available to ERP end users.

Shared Services Functionality
Effective January 1, 2020, the Department of Corrections will have the ability to process transactions on behalf of the following agencies: Department of Juvenile Justice, Prisoner Review Board and Sex Offender Management Board.

Information Technology General Controls

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

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

For Remedy Incident Tickets, these parties can enter the description of their issue into Remedy. Tickets are assigned to the ERP Support que for review and a classification and priority code are assigned indicating emergency or normal classification of low, medium, high, or critical priority. Once an Incident ticket has been assigned to the ERP Support que, the appropriate ERP staff or ERP vendor staff become responsible for completing the tasks necessary to implement the fix.

For Change Requests, designated parties enter their requirements into a SharePoint form. Categorization, urgency, and priority codes are identified at entry, enabling assignment prioritization. Effective September 2019, a Change Advisory Board consisting of agency Chief

Fiscal / Financial Officer's was formed and tasked with prioritizing implementation of change requests.

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

Remedy Incident Tickets or Change Requests that are technical in nature, such as patches, are handled by the ERP's hosting provider and applied to production based upon an agreed upon schedule with the State or after alignment with an ERP Program Manager.

The Remedy Incident Ticket or Change Request is considered resolved upon completion of configuration, transport of code changes, where applicable.

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

Logical Security
Access Provisioning-Active Directory
The Department policies titled Identification and Authentication Policy, Personnel Security Policy, Access Control Policy and Configuration Management Policy address logical security and are published on the Department's website.

Access or modifications to Department resources (network, and shared services begins with submission of a Remedy service request from an authorized ATSR or Department IT Coordinator. The IT Service Processing team assigns Remedy tasks to support groups to satisfy the request. Once all tasks are completed, the Remedy ticket status indicator is automatically updated to "Complete", and the system automatically generates an email notification to the requestor.

Access revocation to Department resources starts when the Department has been notified an individual is separating employment or the initial justification for access has changed. The revocation process is initiated upon receipt of Remedy service request by an authorized ATSR or Department IT Coordinator, IT Service Processing team assigns Remedy tasks to support groups to satisfy the request. Under special or emergency circumstances, network access is disabled at the instruction of the Department senior management.

Password Resets - Active Directory
Active Directory accounts are reset by users calling the IT Service Desk or by one of the Department's self-service options – Microsoft Identity Management (MIM) or the Department's Identity Management (DIM) tool. IT Service Desk 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 and proceed with the reset after verification of two of the following three pieces of information; phone number, email address and physical address. Once a successful reset has taken place, users will be instructed to either register or re-register for MIM/DIM if eligible.

Access Provisioning-ERP
The ERP utilizes the GRC tool to automate user access provisioning, provide management of roles, including emergency access, and enable proactive Segregation of Duties ("SOD") monitoring. From July 1, 2019 thru November 11, 2019, access to the HANA Analytics functionality was granted to end users using an alternate process which is described below at the end of the Access Provisioning section. However effective November 12, HANA Analytics access was transitioned to follow the same process as Non-HANA access, which is described below. On November 11, 2019, user's access was updated to enable HANA access in GRC.

There are four types of users: dialog, system, service and communication. End users are assigned dialog type. The dialog type logs in interactively and the password expires according to the defined profile parameter. For interfaces, System and Communication user types are assigned. These two types of users cannot be used to log in interactively. Firefighters are service user types. The principle of least privilege access is followed, which prescribes that every user should have access only to the information and resources that are necessary for a legitimate purpose.

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

Once an agency is live on ERP, a request to create a new ERP IDs is initiated by the agency using a service request in the Remedy system. The ERP Security team creates the ID in GRC and sends to the agency for approval. Once the ID has been established, the agency adds access using GRC and if the request results in segregation of duties conflicts, the ERP Program staff ensures mitigating controls are applied prior to access being granted. No access is granted when

segregation of duties conflicts exist and a mitigating control is not applied.

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

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

Effective March 16, 2020, due to the COVID-19 stay at home order, the ERP Program staff assisted agency staff with entering and sometimes approving access changes in GRC. These changes were a direct result of the stay at home order which left some key personnel unable to access the ERP thus necessitating changes to access and workflows. Such changes were made by ERP Program staff only when an email approval from designated agency staff was received.

Effective February 27, 2020, a service ID type (named HANA Interface ID) was created in order to facilitate an agency's ability to connect its databases to the ERP HANA database without an expiring password. An agency will be provided such an ID only when the business need, description of data needed, and IP address are provided in writing. The ERP Program monitors the ID usage on a monthly basis. An agency provided with such an ID is required to communicate any changes to business needs and/or staffing of those in possession of the ID and password.

Access Provisioning – HANA Analytics (July 1, 2019-November 11, 2019)
Each agency is created as a separate user group in HANA to ensure access to agency data is restricted. The HANA Analytics functionality is extended to agency end users only after an initial hands-on onboarding/training session is completed. In this session, the agency provides a list of end users who will need access. Initial agency access to the HANA Analytics commences with a Help Desk ticket submitted by the ERP staff for the list of end users provided by the agency. The SAP ERP ID used is the same as what the end user already has in GRC. This ID is assigned in the agency user group and a separate temporary password is emailed to the end user. After initial onboarding, designated agency representatives submit a Help Desk request for access that includes agency name, user name, user email address and the ERP ID the end user already has in GRC. The Production Support team validates the ERP ID and sends the end user an email with the ID and a temporary password.

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

Access De-Provisioning (HANA Analytics) (July 1, 2019-November 11, 2019)
The designated agency representative submits a Help Desk ticket to notify the Production Support team that access should be terminated. The Production Support team completes the termination manually within GRC.

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

to document such review and return to the ERP security team.

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

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

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

Effective March 20, 2020, due to the COVID-19 stay at home order, two additional channels were made available to ERP end users so they could submit password resets:

1. A toll free number was established that end users could call
2. An online portal that included a form for users to fill out

Information gathered from both channels was entered into Remedy by the ERP Program staff, which created an incident ticket that would follow the same process as an incident ticket created by the IT Service Desk.

Agencies are responsible for contacting the IT Service Desk or the utilization of the self-service options, in order to reset their AD or ERP System accounts.

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

At this point, Production Support triages the Remedy request to first determine if it can be resolved without a change to the ERP. Production Support interacts with the user to address the issue. If it can be resolved without a change, Production Support sets the status of the Remedy ticket to "Resolved", which in turn automatically notifies the user of resolution via email.

If the Remedy request is determined to be a defect that requires a fix, the Remedy record is replicated to the Production Support SharePoint and assigned to the appropriate Production Support team member(s). The status of the ticket is set to "Work in Progress" in the Production

Support SharePoint, an analysis is completed by Production Support and the defect follows the defect process flow.

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

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

Backups and Monitoring of Backups

Backups and recovery are executed by the ERP hosting provider, NS2/Virtustream. The process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event.

- FULL data backups are performed weekly which include everything, regardless of whether or not it has changed.
- DIFFERENTIAL data backups are performed daily; these only include objects/data that has 'changed' since the last FULL backup has been taken.

ERP receives daily operational reports from Virtustream that document success/failure of the backup process. Those reports are reviewed on a daily basis by the ERP team lead and are stored on SharePoint. Any issues are addressed directly with Virtustream.

Complementary Subservice Organization Controls

The Department's controls related to the IT General Controls and Application Controls for the State of Illinois Enterprise Resource Planning System 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 for the State of Illinois Enterprise Resource Planning System 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 IV 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 IT General Controls and Application Controls for the State of Illinois Enterprise Resource Planning System 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 IT General Controls and Application Controls for the State of Illinois Enterprise Resource Planning System 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
Risk Assessment	Agencies are responsible for providing mitigation plans corresponding to risk assessment results.
Vulnerability Scan	Agencies are responsible for providing corrective action plans to remediate identified server vulnerabilities.
C1	Agencies are responsible for the complete and accurate entry and maintenance of data into the ERP System.
C1	Agencies are responsible for the timely completion of the various reconciliations and ensure all transactions are reflected in the General Ledger.
C4	Agencies are responsible for the submission of an approved Remedy service request for the creation, modification, and termination of user access, Active Directory and ERP System.
C4	Agencies are responsible for the first level of approval in GRC of an access request for the ERP System.
C4	Agencies are responsible for ensuring proper segregation of duties in the assignment of user access rights.
C4	Agencies are responsible for entering and approving an access termination request into GRC.
C4	Agencies are responsible for reviewing the user access rights to the ERP System.
C4	Agencies are responsible for contacting the IT Service Desk or the utilization of the self-service options, in order to reset their AD or ERP System accounts.
C4	Agencies in possession of an ERP HANA Interface ID are responsible for communicating any business need or staffing changes related to ID usage.

Objectives and Related Controls

The Department of Innovation and Technology has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives, related controls, and the complementary user entity controls are presented in section IV, "Description of the Department of Innovation and Technology's Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results", and are an integral component of the Department of Innovation and Technology's description of State of Illinois, Enterprise Resource Planning System 'system' for the information technology general controls and application controls.

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

Description of the Department of Innovation and Technology's Control Objectives and Related Controls, and the Independent Service Auditor's Description of Tests of Controls and Results

Information Provided by the Independent Service Auditor

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

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

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

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

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

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

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

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

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

CE1.5	New employee and personal service contractors must pass a background check prior to being offered employment.	Selected a sample of new employees and personal service contractors to determine if background checks were completed prior to being offered employment.	No deviations noted.
CE1.6	Performance evaluations for new employees serving a four month probationary period are completed two weeks prior to the end of their probationary period.	Selected a sample of employees serving a four month probationary period to determine if applicable probationary evaluations had been completed.	34 of 38 selected employees' probationary evaluations were completed between 14 to 262 days late.
CE1.7	Performance evaluations are completed at the end of the three months and six months for employees serving a six months probationary period.	Selected a sample of employees serving six month probationary periods to determine if the three and six months probationary evaluations had been completed.	19 of 22 selected employees' probationary evaluations were completed between 3 and 152 days late.
CE1.8	Certified employee performance evaluations are completed annually.	Selected a sample of employees to determine if an annual evaluation had been completed.	31 of 60 selected employees' annual evaluations were completed between 6 and 204 days late.
CE1.9	Newly-hired employees are provided the DCMS' Policy Manual and are required to sign an acknowledgment form acknowledging responsibility to abide by the policies contained within the DCMS Policy Manual.	Selected a sample of new employees to determine if the DCMS Policy Manual acknowledgement had been signed.	No deviations noted.

CE1.10	Personal service contractors acknowledge and accept compliance with Department policies and procedures, as each contract states that the "contract employee agrees to be bound by and comply with policies and procedures of the Agency."	Selected a sample of personal service contractors to determine if the contract contained the clause the "contract employee agrees to be bound by and comply with policies and procedures of the Agency."	No deviations noted.
CE1.11	Newly-hired employees and PSCs are directed to complete the Security Awareness Training, Safeguard Disclosure Training, Ethics Training, and Sexual Harassment Prevention Training for State Employees and Acceptable Use Policy effective September 2019. An acknowledgement is generated at the end of each training.	Selected a sample of employees and personal services contractors to determine if annual Security Awareness training, Safeguards Disclosure training, Ethic training, and Sexual Harassment Prevention training and Acceptable Use Policy acknowledgement had been completed.	No deviations noted.
CE1.12	Employees and PSCs acknowledge awareness of responsibilities through affirming to follow policies as referenced above and through mandated annual calendar year training covering Security Awareness, Safeguard Disclosure, Ethics, and Sexual Harassment Prevention.	Selected a sample of employees and contractors to determine if they had completed the annual Security Awareness training, Safeguard Disclosure training, and Ethics training and Sexual Harassment Prevention training.	Ethics training was not conducted during the examination period. Therefore, the Service Auditor was unable to test the operating effectiveness of the control. 6 of 1,505 required employees and contractors selected did not complete the Safeguard Disclosure training.

			3 of 1,429 required employees and contractors selected did not complete the Security Awareness training. No deviations noted with Sexual Harassment Prevention training.
CE1.13	An Employee Exit form and a Remedy Service Request are completed to ensure remove of access and retrieval of equipment for employees and contractors.	Selected a sample of terminated employees and contractors to determine if an Exit form and Remedy Service Request had been completed for employees and contractors.	2 of 31 terminated employees selected did not have a Remedy Service Request completed. There were no deviations noted in testing of the Exit form.

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 ERP has edit features designed to reject erroneous or invalid data entered. When erroneous or invalid data is entered, an error message will appear. The ERP will not accept the entry until the error has been corrected or deleted.	Selected a sample of field edits to determine if they were functioning appropriately and error notifications appeared.	1 of 60 edits selected was to have display access only; however, it allowed updated access.

Control Objective 2: 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
C2.1	Changes to the ERP follow the processes defined in the IL ACTS ERP Change Control Process Guide.	Reviewed the IL ACTS (ERP) Change Management Policy & Procedures to determine the change management process.	No deviations noted.
	Change Requests		
C2.2	A Change Request is to be completed, validated, reviewed and approved via the Department's SharePoint.	Selected a sample of change requests to determine if they had been completed, validated, reviewed and approved via the Department's SharePoint.	No deviations noted.
C2.3	Functional Specification Design document is to be developed by Production Support and approved by the State's Functional Expert.	Selected a sample of change requests to determine if a Functional Specification Design document had been developed by Production Support and approved by the State's Functional Expert.	No deviations noted.
C2.4	Technical Specification Design document is to be developed and approved by Production Support.	Selected a sample of change requests to determine if a Technical Specification Design document had been developed and approved by Production Support.	No deviations noted.

C2.5	Technical Unit Testing is to be completed and reviewed by Production Support and maintained on Production Support's SharePoint.	Selected a sample of change requests to determine if Technical Unit Testing was completed, reviewed by Production Support and maintained on Production Support's SharePoint.	No deviations noted.
C2.6	Transport requests to the Quality Regions is to be requested and approved via HPQC.	Selected a sample of change requests to determine if transport requests to the Quality Regions had been requested and approved via HPQC.	No deviations noted.
C2.7	Functional Unit testing is to be completed by Production Support and approved by the State's Functional Expert and maintained in HPQC.	Selected a sample of change requests to determine if Functional Unit Testing had been completed by Production Support, approved by the State's Functional Expert, and maintained in HPQC.	No deviations noted.
C2.8	Change Request transports to the Production Region are to be requested and approved by a State Program Manager or the State's Project Manager, via HPQC.	Selected a sample of change requests to determine if transport requests to the Production Region were requested via HPQC and approved by a State Program Manager or the State's Project Manager.	No deviations noted.

	Defects		
C2.9	Technical Unit Testing is to be completed and reviewed by Production Support and maintained on Production Support's SharePoint.	Selected a sample of defects to determine if Technical Unit Testing had been completed, and reviewed by Production Support and was maintained on Production Support's SharePoint.	No deviations noted.
C2.10	Transport requests to the Quality Regions are to be requested and approved via HPQC.	Selected a sample of defects to determine if transport requests to the Quality Regions had been requested and approved via HPQC.	No deviations noted.
C2.11	Functional Unit testing is to be completed by Production Support and approved by the State's Functional Expert and maintained in HPQC.	Selected a sample of defects to determine if Functional Unit Testing had been completed by Production Support, approved by the State's Functional Expert, and maintained in HPQC.	No deviations noted.
C2.12	Functional and security defect transports to the Production Region are to be requested and approved by a State Project Manager, via HPQC.	Selected a sample of defects to determine if transport to the Production Region were requested via HPQC and approved by a State Project Manager.	No deviations noted.
C2.13	Configuration defect transports are to be approved by a State Project Manager and review the Activity Log, via GRC.	Selected a sample of defects to determine if transports were approved by a State Project Manager and the associated activity log was reviewed, via GRC.	No deviations noted.

Control Objective 3: Controls provide reasonable assurance the entities' calls that are relevant to user entities' internal control over financial reporting are responded to, tracked, and resolved in a timely manner.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C3.1	Production Support hosts a weekly meeting with ERP management to provide status updates.	Selected a sample of weekly meetings to determine if status updates are provided.	No deviations noted.
C3.2	Production Support provides ERP management with written weekly updates and monthly reports.	Selected a sample weekly and monthly reports to determine if status updates are provided to the ERP management.	No deviations noted.

Control Objective 4: Controls provide reasonable assurance that logical access to applications, data, and the environment is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions that are relevant to user entities' internal control over financial reporting.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
	Access Provisioning		
C4.1	The Department policies titled Identification and Authentication Policy, Personnel Security Policy, Access Control Policy and Configuration Management Policy address logical security and are published on the Department's website.	Reviewed the Identification and Authentication Policy, Personnel Security Policy, Access Control Policy, and the Configuration Management Policy to determine if they documented logical security controls.	No deviations noted.
		Reviewed the Department's website to determine if the Identification and Authentication Policy, Personnel Security Policy, Access Control Policy, and the Configuration Management Policy had been published.	No deviations noted.
C4.2	Access or modifications to Department resources (network, shared services, mainframe processing, and applications) begins with submission of a Remedy service request from an authorized ATSR or Department IT Coordinator.	Selected a sample of new employees and contractors to determine if a Remedy service request was submitted by an authorized ATSR or Department IT Coordinator.	3 of 25 new employees' and contractors' Remedy service requests selected were not submitted by an authorized ATSR or Department IT Coordinator.

			1 of 26 new employees and contractors selected did not have a Remedy service request submitted to obtain access to the Department's resources.
		Selected a sample of access modifications to determine if a service request was submitted by an authorized ATSR or Department IT coordinator.	The Department did not provide a population of access modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
C4.3	Revoking access is initiated upon receipt of Remedy service request or, under special or emergency circumstances, by instruction of the Department senior management.	Selected a sample of terminated employees and contractors to determine if access was timely terminated.	The Department was unable to provide documentation related to the timely termination of terminated employees and contractors access. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.

	Active Directory Password Resets		
C4.4	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 Identity Management Website to determine solutions to reset passwords.	No deviations noted.
C4.5	The IT Service Desk staff will proceed with the reset after verification of two of three pieces of information.	Observed the IT Service Desk staff to determine if an individual's identity was verified.	No deviations noted.
	ERP Access Provisioning		
C4.6	Designated agency staff prepare and approve a final mapping of access profile to each of its end users.	Selected a sample of mapping uploads to determine if final mapping of access profiles was approved by the agency.	No deviations noted.
C4.7	A segregation of duties analysis is performed by the ERP security team based on this mapping and the results are presented to the designated agency staff person to determine either remediation or mitigation of the risk.	Selected a sample of mapping uploads to determine if the ERP security team completed a segregation of duties analysis.	No deviations noted.
C4.8	ERP security reviews access request to ensure no segregation of duties conflict exist prior to approving.	Selected a sample of new access requests to determine if identified segregation of duties conflicts were reviewed.	No deviations noted.

	HANA Analytics		
C4.9	Initial agency access to the HANA Analytics commences with a Remedy Help Desk Ticket submitted by ERP staff for the list of end users provided by the agency.	Selected a sample of new HANA users to determine if a Remedy Help Desk Ticket was submitted by the agency.	The Department did not receive requests for a HANA user during the period covered by the control. Therefore, the Service Auditor was unable to test the operating the effectiveness of the control.
C4.10	After initial onboarding, designated agency representatives submit a Remedy Help Desk Ticket for access that includes agency name, user name, user email address and the SAP ERP ID that end user already has in GRC.	Selected a sample of new HANA users to determine if a Remedy Help Desk Ticket was submitted by the agency.	The Department did not receive requests for a HANA user during the period covered by the control. Therefore, the Service Auditor was unable to test the operating the effectiveness of the control.
	ERP Annual Review		
C4.11	Annually, the ERP security team provides agencies with the User Access Report for review of their users and associated rights.	Reviewed documentation to determine if the User Access Report was reviewed annually.	No deviations noted.

	ERP Password Resets		
C4.12	To reset a SAP password, users are to contact Production Support, via the IT Service Desk, and provide their name, agency, ID and contact phone number.	Observed IT Service Desk take incoming calls and required information was provided to reset passwords.	No deviations noted.
C4.13	Once the SAP password is reset, a temporary password is emailed to the email addressed associated with the user ID.	Observed an email was sent with a temporary password.	No deviations noted.
	ERP Firefighter		
C4.14	Access to a Firefighter ID requires a request via GRC and a need statement. The ERP security team will review, approve and submit an email to the requestor stating access has been approved.	Observed ERP security team receive a request for Firefighter ID, review, approve, and submit an approval email.	No deviations noted.

Control Objective 5: 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
C5.1	Full data backups are performed weekly, and differntial data backups are peformed daily.	Reviewed backup schedules to determine if daily and weekly performed.	No deviations noted.
C5.2	ERP receives daily operational reports from Virtustream that document success/failure of the backup process.	Reviewed SharePoint to determine if daily operational reports, regarding the success/failure of the backups, were received by the ERP staff.	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	Opinion / Exception	Department Response
1	Opinion1	The Department could not provide a population of access modifications to the Department's resources.	The Department will research opportunities to generate reports in the requested format for future audit testing.
2	Opinion2	The Department could not provide documentation of the timely termination of an individual's access to the Department's resources.	The Department now generates a monthly report to record individual access termination information.
3	CE1.6	34 of 38 selected employees' probationary evaluations were completed between 14 to 262 days late.	The Department will continue distributing monthly evaluation tickler reports. It is the supervisor's responsibility and obligation to complete the performance evaluation as required and submit to HR for processing.
4	CE1.7	19 of 22 selected employees' probationary evaluations were completed between 3 and 152 days late.	The Department will continue distributing monthly evaluation tickler reports. It is the supervisor's responsibility and obligation to complete the performance evaluation as required and submit to HR for processing.
5	CE1.8	31 of 60 selected employees' annual evaluations were completed between 6 and 204 days late.	The Department will continue distributing monthly evaluation tickler reports. It is the supervisor's responsibility and obligation to complete the performance evaluation as required and submit to HR for processing.

6	CE1.12	Ethics training was not conducted during the examination period. Therefore, the Service Auditor was unable to test the operating effectiveness of the control. 6 of 1,505 required employees and contractors selected did not complete the Safeguard Disclosure training. 3 of 1,429 required employees and contractors selected did not complete the Security Awareness training. No deviations noted with Sexual Harassment Prevention training.	The Department will continue sending training reminders to the employees.
7	CE1.13	2 of 31 terminated employees selected did not have a Remedy Service Request completed. There were no deviations noted in testing of the Exit form.	The Department will examine this isolated occurrence and remind staff of the offboarding process.
8	C1.1	1 of 60 tcodes selected was to have display access only; however, it allowed updated access.	The Department has opened up a ticket to identify the root cause for the bug and to provide a resolution.

9	C4.2	3 of 25 selected new employees' and contractors' Remedy service requests were not submitted by an authorized ATSR or Department IT Coordinator. 1 of 26 selected new employees and contractors did not have a Remedy service request submitted to obtain access to the Department's resources. The Department did not provide a complete and accurate population of access modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.	The Department will remind staff of the onboarding process. Regarding the population of access modifications, the Department will research opportunities to generate reports in the requested format for future audit testing.

DEPARTMENT OF INNOVATION AND TECHNOLOGY
ERP Disaster Recovery
(Not Examined)

The Department has contracted with Virtustream (through our SAP NS2 support contract) to host the ERP infrastructure environment. The Department has created a Disaster Recovery (DR) plan and background to help keep this process simple and focused. The annual DR plan is initiated by the Department's ERP Team through communication with its customer and hosting provider Virtustream. As part of the process the Virtustream team assigns a Project Manager to the DR test to manage the entire process. The Department's ERP Team creates a Change Request internally in SharePoint as well as a Change Request internally in Remedy and a Service Request externally at Virtustream to document the DR test project and overall activity. The Virtustream Project Manager initiates planning meetings for the DR test with the Department's ERP Team. Once planning is completed the Department's ERP Team and Virtustream's team initiate the DR test alongside the Department's networking team to execute DR action items. Throughout the DR test the Department, alongside with the Virtustream Project Manager record all activities that occur during the test. Once the test is complete and approved by the Department, the Department's ERP Team and Virtustream team complete and sign off that all testing criteria has been met. In the case where DR testing criteria is not met, Virtustream will create a service request for incidents that will need to be remedied.

In March 2020, the Department's ERP Team worked with Virtustream to conduct a successful test of the ACTS SAP team disaster recovery plan and activities.

Listing of User Agencies of the Department's Enterprise Resource Planning System (Not Examined)

1. Abraham Lincoln Presidential Library and Museum
2. Capital Development Board
3. Criminal Justice Information Authority
4. Department of Agriculture
5. Department of Central Management Services
6. Department of Children and Family Services
7. Department of Corrections*
8. Department of Employment Security
9. Department of Financial & Professional Regulation
10. Department of Healthcare and Family Services*
11. Department of Human Rights
12. Department of Human Services-Mabley Mental Health Center
13. Department of Innovation and Technology
14. Department of Insurance
15. Department of Juvenile Justice*
16. Department of Labor
17. Department of Lottery
18. Department of Military Affairs*
19. Department of Natural Resources (Historic Preservation)
20. Department of Public Health
21. Department of Revenue
22. Department of State Police*
23. Department of Transportation*
24. Department of Veterans' Affairs
25. Environmental Protection Agency
26. Executive Ethics Commission
27. Governor's Office of Management and Budget
28. Guardianship and Advocacy Commission
29. Human Rights Commission
30. Illinois Arts Council
31. Illinois Civil Service Commission
32. Illinois Commerce Commission
33. Illinois Council on Developmental Disabilities
34. Illinois Deaf and Hard of Hearing Commission
35. Illinois Educational Labor Relations Board
36. Illinois Emergency Management Agency
37. Illinois Gaming Board
38. Illinois Independent Tax Tribunal
39. Illinois Labor Relations Board
40. Illinois Law Enforcement Training and Standards Board
41. Illinois Liquor Control Commission
42. Illinois Power Agency
43. Illinois Prisoner Review Board*

Provided by the Department of Innovation and Technology

44. Illinois Procurement Policy Board
45. Illinois Racing Board
46. Illinois State Toll Highway Authority
47. Illinois Workers' Compensation Commission
48. Office of the Executive Inspector General
49. Office of the Governor
50. Office of the Lieutenant Governor
51. Office of the State Fire Marshal*
52. Property Tax Appeal Board
53. Sex Offender Management Board*
54. State Police Merit Board

*Went live on January 1, 2020

ACRONYM GLOSSARY

AD – Active Directory
API – Application Program Interface
AR – Accounts Receivable
ATSR – Agency Technology Service Requestor
CHIRP – Criminal History Information Response Process
CIO – Chief Information Officer
CISO – Chief Information Security Officer
CJIS – Criminal Justice Information Services
CMS – Central Management Services
CO – Controlling
DCMS – Department of Central Management Services
Department – Department of Innovation and Technology
DIM – Department's Identity Management
DoIT – Department of Innovation and Technology
EAT – Expenditure Adjustment Transmittal
ECC – ERP Central Component
ERP – Enterprise Resource Planning
FEIN – Federal Employer Identification Number
FI – Financial Accounting
FM – Funds Management
FTI – Federal Tax Information
GL – General Ledger
GOMB – Governor's Office of Management and Budget
GRC – Governance, Risk, and Compliance
HPQC – Hewitt Packard Quality Control
HR – Human Resources
HRIS – Human Resources Information System
ID – Identification
ILCS – Illinois Compiled Statutes
ILTA – Illinois State Toll Highway Authority
IOC – Illinois Office of the Comptroller
IOCA – Illinois Office of the Comptroller Accounts
IP – Internet Protocol
IT – Information Technology
JE – Journal Entry
LHF – Locally Held Funds
M&O – Maintenance and Operational
MIM – Microsoft Identity Management
MS-ISAC – Multi-State Information Sharing and Analysis Center
NIST – National Institute of Standards and Technology
PAR – Personnel Action Request
PCI – Payment Card Industry
PHI – Protected Health Information
PSC – Personal Service Contractor

PSCD – Public Sector Collection & Disbursements
RDT – Receipt Deposit Transmittal
SAMS – Statewide Accounting Management System
SAP – Systems, Applications and Products
SKF – Statistical Key Figure
SOC – System and Organization Controls
SOD – Segregation of Duties
SRM – Supplier Relationship Management
SSN – Social Security Number
STIL – State of Illinois
WBS – Work Breakdown Structure