STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY

REPORT ON THE DESCRIPTION OF SYSTEM, SUITABILITY OF DESIGN, AND OPERATING EFFECTIVENESS OF CONTROLS FOR THE PERIOD JULY 1, 2021, THROUGH JUNE 30, 2022

ENTERPRISE RESOURCE PLANNING SYSTEM FOR THE IT GENERAL CONTROLS AND APPLICATION CONTROLS

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

Chicago Office:

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

Office of the Auditor General
Frank J. Mautino

INDEPENDENT SERVICE AUDITOR'S REPORT ON THE STATE OF ILLINOIS, DEPARTMENT OF INNOVATION AND TECHNOLOGY'S DESCRIPTION OF ITS 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 for 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, 2021 to June 30, 2022, (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. a subservice organization to provide cloud hosting services for the State of Illinois, Enterprise Resource Planning System; the Department of Central Management Services, a subservice organization to provide building maintenance activities of Department occupied facilities; Okta, Inc., a subservice organization to provide cloud-based service for the Department's identity and access management;

BMC Software, Inc. a subservice organization to provide hosting services for the Department's service management tool, Remedy on Demand; and ServiceNow, Inc., a subservice organization to provide cloud-based service for managing the Department's Information Technology services, including help desk ticketing 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 organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information about the corrective action plan and user entity listing 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's description of the State of Illinois, Enterprise Resource Planning System for the IT General Controls and Application Controls made available to user entities during the period from July 1, 2021 to June 30, 2022. Information about the State of Illinois, Department of Innovation and Technology's corrective action plan and user entity listing has not been subjected to procedures applied in the examination of the description of the State of Illinois, Enterprise Resource Planning System for the IT General Controls and Application Controls 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 for the IT General Controls and Application Controls and, accordingly, we express no opinion on these items.

Service Organization Responsibilities

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

Service Auditor's Responsibilities

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in *Government Auditing Standards,* issued by the Comptroller General of the United States and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on criteria in management's assertions, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period from July 1, 2021 to June 30, 2022. We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 Qualified Opinion

Our examination disclosed:

1) Page 13 of the accompanying description of the information technology general controls and application controls for its Enterprise Resource Planning System system states the Department conducts risk assessments for customer agencies. Our testing determined the Department is to conduct risk assessments for all agencies, boards, and commissions under the Governor, not just agencies utilizing the Enterprise Resource Planning System.

2) Page 15 of the accompanying description of the information technology general controls and application controls for its Enterprise Resource Planning System system states the Department's Division of Information Security is responsible for ensuring the Department's compliance with enterprise information security policies. Our testing determined the Division of Information Security is not ensuring compliance for all of the enterprise information security policies.

3) Page 27 of the accompanying description of the information technology general controls and application controls for its Enterprise Resource Planning System system states access creation or modification to Department resources (users and administrators) requires submission of a service request approved by an authorized Agency Technology Service Requestor (ATSR). The Department did not provide a population of new network administrator access requests and a population of Active Directory access modifications. As a result, we were unable to determine whether the controls were suitably designed and operating effectively to achieve the control objective, "Controls provide reasonable assurance that logical access to applications, data, and the environment relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions."

In our opinion, except for the matters referred to in the preceding paragraph, 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, 2021 to June 30, 2022.

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, 2021 to June 30, 2022; 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, 2021 to June 30, 2022.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period from July 1, 2021 to June 30, 2022 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, 2021 to June 30, 2022.

Other Reporting Required by Government Auditing Standards

In accordance with *Government Auditing Standards*, we have also issued our report dated August 3, 2022 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, 2021 to June 30, 2022, 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, 2021 to June 30, 2022 (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, 2021 to June 30, 2022, 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 3, 2022
Springfield, Illinois

SECTION II

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

Illinois Department of Innovation & Technology

JB Pritzker, Governor
Jennifer Ricker, Secretary and State CIO

Assertion of the Management of the Department of Innovation and Technology

We have prepared the description of the Department of Innovation and Technology's information technology general controls and application controls for 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, 2021 to June 30, 2022, 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 misstatement of user entities' financial statements. 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 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 made available to user entities of the system during some or all of the period July 1, 2021 to June 30, 2022 for the IT 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 was designed and implemented, including, if applicable:

      i) The types of services provided.

      ii) The procedures, within both automated and manual systems, by which requests for those services are provided, including, as appropriate, procedures by which services are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

      iii) How the system captures and addresses significant events and conditions.

      iv) The process used to prepare reports and other information for user entities.

      v) 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.

      vi) Other aspects of our control environment, risk assessment process, information and communication systems, control activities, and monitoring activities that are relevant to the services provided.

b) Includes relevant details of changes to the State of Illinois, Enterprise Resource Planning 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 a broad range of 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 that each individual user entity of the system and its auditor may consider important in its own particular environment.

2) Except for the matter described in paragraph 3, the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period July 1, 2021 to June 30, 2022 to achieve those control objectives if user entities applied the complementary controls assumed in the design of the Department of Innovation and Technology's controls throughout the period July 1, 2021 to June 30, 2022. 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 service organization.

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

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

3) Description of Deficiency in Fair Personation, Suitability of Design, or Operating Effectiveness

a. We state in the accompanying description of the information technology general controls and application controls for its Enterprise Resource Planning System the Department is to conduct risk assessments for customer agencies. However, the Department is to conduct risk assessments for all agencies, boards, and commissions under the Governor, not just agencies utilizing the Department's Shared Services.

b. We state in the accompanying description of the information technology general controls and application controls for its Enterprise Resource Planning System the Department's Division of Information Security is responsible for ensuring the Department's compliance with enterprise information security policies. However, the Department's Division of Information Security is not ensuring compliance for all of the enterprise information security policies.

c. We state in the accompanying description of the information technology general controls and application controls for its Enterprise Resource Planning System access creation or modification to Department resources (users and administrators) requires submission of a service request approved by an authorized Agency Technology Service Requestor (ATSR). However, the Department did not provide a population of new network administrator access request and a population of Active Directory access modifications. As a result, controls were suitably designed and operating effectively to achieve the control objective, "Controls provide reasonable assurance that logical access to applications, data, and the environment relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.”

SIGNED ORIGINAL ON FILE

Jennifer Ricker, Secretary
Department of Innovation and Technology
August 3, 2022

SECTION III

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

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

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

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

Subservice Organizations

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

Subservice Organization	Subservice Organization Description
Department of Central Management Services (DCMS)	Provides building maintenance activities of Department occupied facilities.
BMC Software, Inc.	Provides hosting services for the Department's service management tool, Remedy on Demand.
Okta, Inc.	Provides a cloud-based service for the Department's identity and access management.
Virtustream, Inc.	Provides cloud hosting services for the State of Illinois Enterprise Resource Planning (ERP) System.
ServiceNow, Inc.	Provides a cloud-based service for managing the Department's Information Technology services, including help desk ticketing services. ServiceNow went live on July 28, 2021 as the Department's service management system

Overview of Service Provided

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

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

- installation and operation of IT systems.

Internal Control Framework

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

- Control Environment,
- Risk Assessment,
- Information and Communication,
- Control Activities, and
- Monitoring.

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

Control Environment

The Department's organizational hierarchy supports internal controls starting with the Department's Secretary. The Secretary is a member of the Governor's Cabinet and is the "Chief Information Officer for the State and the steward of State data with respect to those agencies under the jurisdiction of the Governor" per Section 1-15 of 20 ILCS 1370. During the examination period, one individual served in this capacity as the Acting Secretary.

The Acting Assistant Secretary (vacant) directly supervises the Department's 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, Enterprise Resource Planning (ERP) Program Director, and six Chief Information Officers (CIOs) grouped into service delivery taxonomies. (The seventh Group CIO, the Transportation Group CIO position has been vacant since its establishment and has been abolished effective October 29, 2021.)

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

The Chief Administrative Officer consults with the Secretary and senior management to facilitate functional compatibility and alignment of Department objectives. Subordinate managers oversee the Department's Human Resources, Procurement and Property Control.

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) plans, coordinates, reviews, and directs long and short-term strategic goals, policies, and procedures based on the Department's mission and initiatives with the ultimate goals of understanding, satisfying, and exceeding, if possible, customer expectations.

The Chief of Staff advises the Secretary on the transformation status of legacy agency resources (personnel and equipment) to meet the requirements of the Act and provides the authority for transferring State resources into the Department. The Chief of Staff also supervises functional areas of the Department's General Counsel, 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 projects are aligned to the Department's mission, long-term strategic goals, and business objectives.

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

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

The 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 six 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 six (6) groups reflecting Statewide agency services. Categories are (1) health and human services (vacant November 13, 2021 to present); (2) government and public employees; (3) business and workforce; (4) natural and cultural resources; (5) public safety (vacant July 1-15, 2021); and (6) education. (As stated previously, the vacant Transportation Group CIO was abolished October 29, 2021.)

Human Resources (HR)

The Department's hiring practices adhere to legal requirements as published in the State Personnel Code, Personnel Rules, union contracts, *Rutan/Shakman* decisions, court orders, the Governor's Comprehensive Employment Plan (CEP) For Agencies under the Jurisdiction of the Governor, and applicable state/federal laws.

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

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

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

Performance evaluations are completed annually for employees on DoIT payroll. Additionally, for employees' service probationary periods, performance evaluations are completed at varying intervals.

- Four-month probationary period, performance evaluations are completed two weeks prior to the end of the probationary period.
- Six-month probationary period, performance evaluations are completed at the end of three months and again at two weeks prior to the end of the probationary period.

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

Newly-hired PSCs on the Department's payroll are governed by the terms, conditions, and duties outlined in their legally-binding contract. PSCs acknowledge and accept compliance with Department policies and procedures, as each contract states the "Contract Employee agrees to be bound by and comply with policies and procedures of the Agency."

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

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

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

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

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

For an employee voluntarily separating from the Department (transferring, resigning, or retiring), once Human Resources 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 terminated from the Department, once Human Resources receives either written or verbal direction from the Secretary or her/his designee, HR initiates a PAR, obtains appropriate Department authorizations from the Chief Fiscal Officer and the Secretary and generates the Exit Form. For a contractor, the separation process begins upon expiration or termination of the contract at which time an Exit Form is generated. Once the 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 service request to disable access and return equipment.

Risk Assessment Process

The Department has established a Risk Management Program (RMP) to offer guidelines on how to reduce risk across the enterprise.

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

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

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

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

Information and Communication

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

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

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

Acceptable Use Policy
Access Control Policy
Accountability, Audit, and Risk Management Privacy Policy
Audit and Accountability Policy
Awareness and Training Policy
CJIS Security Supplemental Policy
Configuration Management Policy
Contingency Planning Policy
Data Minimization and Retention Privacy Policy
Data Quality and Integrity Privacy Policy
FTI Supplemental Policy
Identification and Authentication Policy
Individual Participation and Redress Privacy Policy
Information Security Incident Management Policy
Media Protection Policy
Overarching Enterprise Information Security Policy
PCI Data Security Policy
Personnel Security Policy
PHI Supplemental
Physical and Environmental Protection Policy
Privacy Security Policy

Program Management Policy
Risk Assessment Policy
Security Assessment and Authorization Policy
Security Planning Policy
System and Communication Protection Policy
System and Information Integrity Policy
System and Services Acquisition Policy
System Maintenance Policy
Transparency, Authority, and Purpose Privacy Policy
Use Limitation Privacy Policy
Identity Protection Policy
Mobile Device Security Policy
Wireless Communication Device Policy

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

Internal Communication

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

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

External Communication

In addition to the Department's website, client agencies are kept informed through direct correspondence and face-to-face meetings.

The Department's Communication Office sends email correspondence to appropriate agency groups (directors, CIOs, Telecom Coordinators, Agency Technology Service Requestors (ATSR)) documenting new services/processes/outages/etc. Group CIOs discuss with agency leadership personnel relevant subjects that may include significant events, service issues, improvements, processes, and strategic goals. Group CIOs meet with agency CIOs when business needs require or when instructed by Department management to update and gather information from agencies. Group CIO communication occurs at an individual agency level. State-wide level agency communication is accomplished through CIO Council meetings which are held at the Secretary's request to update and inform agency CIOs of news and information.

Agency CIOs, along with Department leadership and support staff are invited to attend "DoIT Daily" meetings (Mondays through Fridays). DoIT Daily is a forum to share high-level and high-risk operational issues with a team equipped to discuss steps for resolution.

The Department communicates ERP information via:

- 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. Effective September 2021, the descriptions of all functional releases are published on the ERP Website and are no longer sent via email.
- 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 an incident ticket for all problems experienced with the ERP.
- Individual ERP team members via email or phone for any business process questions.

In addition, ERP policies and procedures are maintained on SharePoint.

Monitoring Activities

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

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

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

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

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

<u>Enterprise Resource Planning System</u>
The Department implemented the 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 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 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 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 ERP 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 ERP utilizes 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 should complete recording of all transactions. In addition, it is recommended the agency complete the various reconciliations with IOC system in a timely manner and ensure all transactions are accurately reflected in the General Ledger.

Company Code STIL maintains a 6-month rolling window of open periods, which includes the current month and previous five months. 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 oldest prior period open, thus maintaining the 6-month window of open periods.

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.

The quarterly and year-end closing also includes tasks for required reporting requirements.

Periods one through six for fiscal year 2022 and special periods 13 through 16 for fiscal year 2021 are open for STIL. Periods 11 and 12 for calendar year 2021 are open for ILTA. As of June 30, 2022, periods eight through twelve for fiscal year 2022, period 1 for fiscal year 2023, and special periods 13 through 16 for fiscal year 2022 are open for STIL. Periods 6 and 7 for calendar year 2022 are 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/ServiceNow incident ticket to ERP Production Support. The General Ledger Functional Expert will reopen the closed periods that need posted to and work with the agency to make the needed corrections. The General Ledger Functional Expert will then reclose the periods once the corrections are complete.

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 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). A HANA interface runs against the SAMS warehouse payment table to identify the payments which are ERP vouchers. This process creates a text file which pulls against the ERP vouchers that are open in the system. It is the agencies' responsibility to investigate any issues identified by the reconciliation between the two systems.

Interface reports are sent to each agency daily. The interface reports document high-level detail of the various interfaces run overnight, including the success/error records of each interface. If there is an error identified on the report, the agency will receive an additional email with additional information on the error.

The Department of Healthcare and Family Services and the Illinois Tollway utilizes the Locally Held Funds (LHF) functionality for payments that are not sent through Office of 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. The Department of Healthcare and Family Services submits a file with check information to the ERP Production Support for processing to clear checks. The Illinois Tollway manually clears checks in SAP. It is the responsibility of each agency to ensure the processing was completed and the reconciliation of the LHF was completed.

The Department of Human Services utilizes ERP to process payments to providers in the form of a debit card. The AP Master Data role has access to maintain a debit card table that interfaces with a 3rd party vendor who establishes the debit card accounts. The Department of Human Services is responsible for monitoring the status of vendors paid via a debit card.

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 Tollway), a second batch job is run for the monthly depreciation on new, disposed-of and transferred assets. The 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 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 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. Additionally, the warehouse management functionality 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.

The STO process for STIL is also available for orders from DHS warehouse plants HSSW and HSCW. STOs can be made within the DHS business area or from an approved external business areas. A business area requests approval via a Remedy/ServiceNow incident request and the Production Support team coordinates approval from DHS via email. Once approved, the Stock Transport Processor at the receiving plant creates the STO using an INV cost center, functional area, and funded program. The supplying plant processes the order and goods issue. The receiving plan will enter a goods receipt once the goods are received. If the goods are to a plant that is not within the supplying plant business area, the stock will show as stock in transit until the goods receipt is processed.

Procurement Business Case
Procurement Business Case (PBC) functionality is used by agencies to launch an exempt procurement request and capture procurement information prior to obligation. A Procurement Business Case is required for:

- Capturing all exempt procurements to be created with a dollar value of $10,000 or more, and
- Tracking multi-level PBC approvals across agencies.

The agency RFx/PBC Requestor creates the PBC document in SRM and the agency RFx/PBC Approver approves the document. Further approvals from Central Management Services, Department of Innovation and Technology, the Governor's Office of Management and Budget or the Office of the Governor are routed via workflow based on the nature of request and PBC total dollar value.

Contract Obligations
Contracts are obligated through Supplier Relationship Management (SRM). Upon execution of a contract, the Strategic Buyer enters obligation data required to populate information required in the Contract Obligation Document (COD). There are fields that require manual entry of data that then derive information needed for the Office of the Comptroller (IOC). Attachments can be added to contract record.

Once entered, the Strategic Buyer will release the document. The Contract Approver is required to review and approve the contract obligation. Once approved, an Earmarked Funds Reservation is generated, and the obligation consumes budget

A nightly batch run which generates the COD and Agency Balancing Report (ABR) documenting approved obligations. Upon receiving ABR, agencies will review and forward to the Comptroller IOC within five days. In addition, with the execution of MOU with IOC, users have the capability to submit contract attachments electronically via SRM. It is the responsibility of the users to reconcile and correct data between the IOC and SRM.

Some business areas have interfaces that populate data that is otherwise entered manually by the Strategic Buyer. Grant agreement obligations are interfaced from Amplifund to SRM. These contracts are interfaced in awaiting approval status and must be approved. Several agencies, including DHS and DCFS interface contracts from their legacy systems in awaiting approval status as well. IDOT interfaces contracts from their legacy system in approved status. Contract obligations generated from the BidBuy are interfaced to SRM in saved status. The Strategic Buyer will update all interfaced contract obligation information and release for approval.

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. As receivables age, some agencies utilize the dunning functionality to escalate collections efforts at various age levels. In addition, DHS utilizes auto-referral functionality to send qualified receivables to Office of the Comptroller's IDROP system and to a 3rd party collections agency.

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.

Once the Treasurer's draft is received, the applicable Receipt Deposit Transmittal (RDT) or Expenditure Adjustment Transmittal (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 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.

The reversal of payments is routed through the same process as receivables.

In the instance an agency misclassifies a payment remitted to the Office of the Comptroller, agencies utilize the Receipt Transfer Request process. In addition to recording the reclassification, a paper SCO-102 is generated for submission to the Office of the Comptroller.

Monthly, agencies utilize the General Ledger Balance Report in order to balance with the Office of

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 Comptroller.

There are several receivable and receipt reports available to the agencies, including, receivables aging, payment transactions, and customer detail. In addition, the HANA PSCD Enterprise report is available that merges all agency activity.

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 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 and Functional Area. In the event a new fund needs to be established, a request from the Office of 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 the 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 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. *(C1.1)*

Controlling
The Controlling process 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 agency 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.

HANA Analytics
The HANA Analytics functionality provides agencies with enhanced reporting capabilities. Agencies can query their own data against views that have been built. Based on defined roles, agencies 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. The following reconciliation reports are available to end users based on appropriate role assignment:

- SB01 Expenditure Reconciliation
- SB04 Revenue Reconciliation
- SC14 Contract Reconciliation
- SC15 FY Obligation Reconciliation
- SC15 FY-Lapse Obligation Reconciliation

Tableau Dashboards use views developed in HANA to provide a real-time interactive overview using visualizations to provide insight into information such as an Agency’s budget appropriations, consumption, budget availability, obligation spend and supporting details behind obligations. Filtering is available based on various master data and cost elements such as Fund, Funded Program, Fund Center, etc. Dashboards can be used for analysis and spending patterns, and can be downloaded or printed in easy-to-read format(s)

Information Technology General Controls

Change Control
Changes to the ERP follow the processes defined in the IL ACTS ERP Change Control Process Guide - Finance. *(C2.1)*

The change management process begins with either the submission of an Incident Ticket via the service management system 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. An Incident Ticket or Change Request can originate from an ERP staff, ERP system integrator, or agency user.

For Incident Tickets, these parties enter the description of their issue and the Incident Tickets are assigned to an ERP group in the service management system 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 appropriate ERP staff or ERP system integrator, that individual becomes 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. A Change Advisory Board consisting of agency Chief Fiscal / Financial Officers was formed and tasked with prioritizing implementation of change requests. As a result of the COVID-19 stay at home order, the Change Advisory Board has not met during fiscal 2022. In the interim, the Change Requests were being prioritized by the ERP Program Manager for Work Management and the Functional Experts.

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. *(C2.2*) ERP Program Managers approve all transports to production. *(C2.3)* 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 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. *(C2.4)* 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.

Incident Tickets or Change Requests that are technical in nature, such as patches, are handled by the ERP's hosting service provider and applied to production based upon an agreed upon schedule with the State or after alignment with an ERP Program Manager. Patches are applied to the ACTS SAP team's non-production servers first. The ERP Production Support team, together with the responsible ERP Program Manager, review overall system performance over a two week period. If patches are successfully working at the end of the two week period the patches are scheduled and applied to the ACTS SAP Production servers. The existing Change Control Process Guide is followed.

The Incident Ticket or Change Request is considered resolved upon completion of configuration, and 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). *(C2.5)*

Batch Jobs
The ERP Team uses [redacted] to manage every batch process, including all of the various interfaces run. A limited number of approved ERP team members have access. *(C2.6)* Any new job will be created in development environment and moved to higher environment in accordance to release management process.

Any job chain hold/restart/re-run/reschedule will be performed by the Basis team with ERP Manager or State Functional Expert approval.

Logical Access
In order to access the State's information technology environment, an Active Directory ID and password are required. (*C4.1*) Password security parameters have been established and configured to ensure access to resources is appropriate:

- Minimum password length;
- Password complexity;
- Password history;
- Minimum password age; and
- Number of invalid login attempts. (*C4.2)*

The Department has implemented OKTA for Single Sign-On (SSO). Single-sign on allows users to utilize their Active Directory credentials to authenticate to cloud services. Several services have been integrated and further integrations will be completed as appropriate. OKTA SSO is configured to pass authentication requests to ADFS for authentication and has been configured for all users. (C4.9) OKTA also provides multi-factor authentication.

Access Creation, Modification, and Revocation
Access creation or modification to Department resources (users and administrators) requires the submission of a service request approved by an authorized Agency Technology Service Requestor (ATSR). (*C4.3*) IT Service Processing team assigns tasks to support groups to satisfy the request until July 27th, 2021. Starting July 28th, 2021, the tasks are automatically assigned to appropriate working groups based on ServiceNow's automated workflow.

For voluntary separations of an employee or a contractor, an Employee Exit form and a service request are completed to initiate and ensure the removal of access. The Department revokes the access on the employee's last working day. (*C4.4*)

Under special or emergency circumstances, network access is disabled at the instruction of the Department senior management. A service request is approved by the ATSR after the special or emergency access revocation has occurred.

Password Resets
Active Directory accounts are reset by users calling the IT Service Desk or by one of the

Department's self-service options – Microsoft Identity Management (MIM) or the Department's Identity Management (DIM) tool. (*C4.5*) 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 service ticket. The IT Service Desk staff will then proceed with the reset after verification of two of three pieces of information; phone number, email address and physical address. (*C4.6*) Once a successful reset has taken place, users will be instructed to either register or re-register for MIM/DIM if eligible.

Reviews
On an annual basis, the Department's Security Compliance team sends a list of the technical accounts to appropriate supervisors. (*C4.7*) The supervisor of the technical account owner is requested to review and update continued access. In the event the technical account is no longer required, a Remedy ticket is submitted by the immediate supervisor or their designee to remove the account. Additionally, accounts with 60 days of inactivity are disabled.

The Department performs a monthly review of Illinois.gov Active Directory accounts and disables accounts which have been dormant for 60 days. (*C4.8*) Account deletion is processed upon receipt of the Remedy request.

ERP Access Provisioning
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.

There are five types of users: dialog, system, service, reference 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 and reference type used to configure the firefighter roles. 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.

There is also a service ID type which facilitates an agency's ability to connect its databases to the 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 Director makes the final decision on the creation of any new ID's. (C4.10) The ERP Program monitors the ID usage on a monthly basis. (C4.11) 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.

The initial upload of a 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 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. (C4.12) Any exceptions to this process are documented in implementation deliverables. Single sign on functionality with Illinois.gov Active Directory is enabled using Okta as the authentication tool. Users are still sent an email with login instructions; however there is no longer a separate password for ERP. Additionally, users must be added to a special Active Directory group to enable the single sign on functionality if they are on the Illinois.gov domain. Adding users to this group is accomplished using a service request in the service management system. For users outside of the Illinois.gov domain, their authentication occurs either (1) by having an individual account established in Okta which then does not facilitate a single sign on; (2) by having their agency Active Directory system connected to Okta which does facilitate single sign on or (3) have the agency Okta instance connected to the DOIT Okta instance.

For ERP, once an agency is live, the process for creating a new ERP ID is as follows:

- For agencies that utilized Human Capital Management (HCM) functionality, an ERP ID is automatically created for all new employees by the ERP HCM Production Support Team based on service requests, or in certain cases a help desk incident, submitted by an agency in the service management system.

For agencies that did not utilize HCM, a request to create a new ERP ID is initiated by the agency using a service request in the service management 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 is responsible for adding 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. *(C4.13)* No access is granted when segregation of duties conflicts exist and a mitigating control is not applied.

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

ERP 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.

ERP 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. *(C4.14)* 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.

ERP Administrative Access
The Firefighter ID provides access to administrative rights and is limited to ERP functional experts and authorized Production Support staff. *(C4.15)* 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. ERP management subsequently reviews the log of work completed. (C4.16)

ERP Help Desk

ERP end users can help desk tickets; an online portal that includes a form for users to fill out.

Information gathered from this channel is entered into the service management system by the ERP Program staff, which creates an incident ticket that would follow the same process as an incident ticket created by the IT Service Desk. This channel was discontinued September 30, 2021.

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.

Upon receipt, an incident ticket gets routed to the appropriate group in the service management system based on the nature of the request. At this point, Production Support triages the ticket 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 ticket to "Resolved", which in turn automatically notifies the user of resolution via email.

If the incident ticket is determined to be a defect that requires a fix, the incident ticket 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. The defect follows the Incident Management process flow where the fix is first tested in the development environment before moving to the quality environment for UAT. Testing approvals for the two environments, testing documentation, request for transport to production, and production transport approval are all maintained in HPQC for each defect. *(C3.1)* Incidents deemed to be critical/high impact also require a root cause analysis to be submitted to the State for review and approval. (*C3.2*)

If Production Support determines 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 the incident management system, 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. *(C3.3)*

Infrastructure

The Department utilizes a subservice organization to host the ERP application. Accordingly, the controls over the infrastructure are the responsibility of the subservice organization.

Backups and Monitoring of Backups

Backups and recovery are executed by the subservice organization. Backups are conducted:

- 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. *(C5.1)*

The ERP team receives daily operational reports documenting the success/failure of the backup process. Those reports are reviewed on a daily basis by the ERP team. *(C5.2)* Any issues are addressed directly with the service organization.

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.

	Complementary User Agency Controls
#1	The agencies are responsible for the complete, accurate, and timely entry of data into the ERP.
#2	It is the agencies' responsibility to investigate any issues identified by the reconciliation between the two systems.
#3	Agencies are responsible for reviewing and rectifying the errors noted on the discrepancy report.
#4	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.
#5	Agencies are responsible for ensuring proper segregation of duties in the assignment of user access rights.
#6	Agencies are responsible for informing the Department of business needs.
#7	Agencies are responsible for the timely completion of the various reconciliations and ensure all transactions are reflected in the General Ledger.
#8	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.
#9	Agencies are responsible for entering and approving an access termination request into GRC.
#10	Agencies are responsible for reviewing the user access rights to the ERP System.
#11	Agencies in possession of an ERP HANA Interface ID are responsible for communicating any business need or staffing changes related to ID usage.

SECTION IV

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

Information Provided by the Service Auditor

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

Our examination was limited to the control objectives and related controls specified by the Department of Innovation and Technology in Sections III and IV of the report, and did not extend to controls in effect at the client agencies. The examination was performed in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. It is each client agencies' responsibility to evaluate this information in relation to the internal control structure in place at each client agency in order to assess the total internal control structure. If an effective internal control structure is not in place at client agencies, the Department's controls may not compensate for such weaknesses.

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

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

Tests of Controls

Our test of the operational effectiveness of controls were designed to cover a representative number of activities throughout the period of July 1, 2021 to June 30, 2022, for each of the controls, which are designed to achieve the specific control objectives. In selecting particular tests of operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the examination objectives to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

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

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

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

Type	**Description**
Observation	Observed the application, performance, or existence of the specific control(s) as represented by management.
Selected/Reviewed	Selected/reviewed documents and records indicating performance of the control.

Information Provided by the Department

When using information produced by the Department, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Control Objective 1: Controls provide reasonable assurance that invalid transactions and errors that are relevant to user entities' internal control over financial reporting are identified and rejected that are relevant to user entities' internal control over financial reporting.

	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.	No deviations noted.

Control Objective 2: Controls provide reasonable assurance that application programs and infrastructure changes that are relevant to user entities' internal control over financial reporting are properly authorized, tested, approved and implemented to result in complete, accurate, and timely processing and 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-Finance.	Reviewed the IL ACTS (ERP) Change Management Policy & Procedures to determine the change management process.	No deviations noted.
C2.2	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.	Selected a sample of change requests to determine if testing and approvals had been completed.	1 of 31 changes selected did not have a fully completed change request form.
C2.3	ERP Program Managers approve all transports to production.	Selected a sample of transports to determine if they were approved by the ERP Program Manager.	No deviations noted.
C2.4	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.	Selected a sample of configuration changes to determine if testing had been conducted and an authorized ERP team member made the configuration change.	No deviations noted.
C2.5	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).	Selected a sample of emergency releases to determine if proper authorization and approval was obtained and the emergency release was documented in HPQC or GRC.	No deviations noted.
C2.6	The ERP Team uses [redacted] to manage every batch process, including all of the various interfaces run. A limited number of approved ERP team members have access.	Reviewed the [redacted] Job Chain schedule to determine the interfaces ran and the frequency.	No deviations noted.

		Reviewed the ERP team members with access to [redacted] to determine whether access was restricted to a limited number and appeared	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	Testing approvals for the two environments, testing documentation, request for transport to production, and production transport approval are all maintained in HPQC for each defect.	Selected a sample of defects to determine if testing documentation and approvals were obtained.	No deviations noted.
C3.2	Incidents deemed to be critical/high impact also require a root cause analysis to be submitted to the State for review and approval.	Selected a sample of critical/high impact incident tickets to determine if they were submitted to the State for review and approval.	No deviations noted.
C3.3	Production Support provides ERP management with written weekly updates and monthly reports.	Selected a sample of weekly and monthly reports to determine if status updates were provided to the ERP management.	No deviations noted.

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

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C4.1	In order to access the State's information technology environment, an Active Directory ID and password are required.	Observed an Active Directory ID and password were required to gain access to the environment.	No deviations noted.
C4.2	Password security parameters have been established and configured to ensure access to resources is appropriate: • Minimum password length; • Password complexity; • Password history; • Minimum password age; and • Number of invalid login attempts.	Reviewed the password parameters to determine whether parameters had been established.	The Active Directory password syntax did not conform to the Credential Standards password requirements.
C4.3	Access creation or modification to Department resources (users and administrators) requires the submission of a service request approved by an authorized Agency Technology Service Requestor (ATSR).	Selected a sample of new users to determine if an ATSR approved service request was submitted.	7 of 36 new users selected did not have an ATSR approved service request.
		Inquired with Department staff to obtain the population of new network administrator access requests.	The Department did not provide a population of new network administrator access requests. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
		Inquired with Department staff to obtain the populations of access modifications.	The Department did not provide a population of Active Directory access modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.

C4.4	For voluntary separations of an employee or a contractor, an Employee Exit form and a service request are completed to initiate and ensure the removal of access. The Department revokes the access on the employee’s last working day.	Selected a sample of separated employees and contractors to determine if an Exit form and service request was completed.	7 of 30 separated employees and contractors selected did not have a completed service request.
			2 of 30 service requests selected were completed late.
		Selected a sample of separated employees and contractors to determine if their access was revoked on the last working day.	Documentation was not provided for 17 of 30 separated employees and contractors selected demonstrating their access had been revoked.
			9 of 30 employees and contractors selected did not have access revoked on their last working day.
C4.5	Active Directory accounts are reset by users calling the IT Service Desk or by one of the Department’s self-service options – Microsoft Identity Management (MIM) or the Department’s Identity Management (DIM) tool.	Reviewed the Department's website to determine solution to reset passwords.	No deviations noted.
C4.6	The IT Service Desk staff will then proceed with the reset after verification of two of three pieces of information; phone number, email address and physical address.	Observed the IT Service Desk staff to determine if an individual's identity was verified prior to reset.	No deviations noted.
C4.7	On an annual basis, the Department’s Security Compliance team sends a list of the technical accounts to appropriate supervisors.	Reviewed the annual review to determine if the Security Compliance Team conducted a review of technical accounts.	No deviations noted.
C4.8	The Department performs a monthly review of Illinois.gov Active Directory accounts and disables accounts which have been dormant for 60 days.	Selected a sample of monthly reviews to determine if dormant accounts had been reviewed and disabled.	No deviations noted.
C4.9	OKTA Single Sign-on (SSO) is configured to pass authentication request to Active Directory Federation Services (ADFS) for authentication and has been configured for all users.	Reviewed OKTA configuration to determine if authentication requests were passed to ADFS for authentication for all users and provided multi-factor authentication.	No deviations noted.

C4.10	There is a service ID type which facilitates an agency’s ability to connect its databases to the 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 Director makes the final decision on the creation of any new ID’s.	Selected a sample of service ID types to determine if the ERP Program Director had approved the creation of the service ID type.	No deviations noted.
C4.11	The ERP Program monitors the ID usage on a monthly basis.	Selected a sample of months to determine if the ID usage was monitored.	No deviations noted.
C4.12	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.	Selected a sample of initial upload of users' access to determine if a segregation of duties analysis had been conducted and approved by the agency.	No deviations noted.
C4.13	The ERP Program staff ensures mitigating controls are applied prior to access being granted.	Selected a sample of new access requests to ensure segregation of duties conflicts were reviewed.	No deviations noted.
C4.14	Annually, the ERP security team sends User Access Reports to the agencies documenting their users and the associated rights, which are to be reviewed.	Reviewed the User Access Reports to determine if agencies were sent User Access Reports for review.	No deviations noted.
C4.15	The Firefighter ID provides access to administrative rights and is limited to ERP functional experts and authorized Production Support staff.	Reviewed Firefighter ID to determine if access was limited to ERP functional experts and authorized Production Support staff.	No deviations noted.
C4.16	If approved by ERP Program Management, the user will receive an email stating the request has been approved. ERP management subsequently reviews the log of work completed.	Reviewed the log of work to determine if ERP management had reviewed.	No deviations noted.

Control Objective 5: Controls provide reasonable assurance that applications, data, and the environment relevant to user entities' internal control over financial reporting is backed up and stored offsite.

	CONTROLS SPECIFIED BY THE DEPARTMENT	TESTS OF CONTROLS	RESULTS OF TESTS
C5.1	Full data backups are performed weekly, and differential data backups are performed daily.	Reviewed backup schedules to determine if daily and weekly backups were performed.	No deviations noted.
C5.2	The ERP team receives daily operational reports documenting the success/failure of the backup process. Those reports are reviewed on a daily basis by the ERP team.	Selected a sample of operational reports to determine if the reports were reviewed daily by the ERP Team.	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)

1. The Department is in the process of conducting risk assessments for all customer agencies. The Department will continue to make risk assessments available to all agencies.

2. The Department will work to clarify the description of system and ensure the procedures are documented and communicated.

3. The Department will continue to implement advanced tools and improve procedures to audit and log account changes.

Provided by the Department of Innovation and Technology

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

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

Provided by the Department of Innovation and Technology

44 Illinois Liquor Control Commission
45 Illinois Pollution Control Board
46 Illinois Power Agency
47 Illinois Prisoner Review Board
48 Illinois Procurement Policy Board
49 Illinois Racing Board
50 Illinois State Police
51 Illinois State Toll Highway Authority
52 Illinois Workers' Compensation Commission
53 Judicial Inquiry Board
54 Office of the Attorney General
55 Office of the Auditor General
56 Office of the Executive Inspector General
57 Office of the Governor
58 Office of the Lieutenant Governor
59 Office of the State Appellate Defender
60 Office of the State Fire Marshal
61 Office of the Treasurer
62 Property Tax Appeal Board
63 Sex Offender Management Board
64 State Board of Elections
65 State Police Merit Board
66 State University Civil Service System

ACRONYM GLOSSARY

AD – Active Directory
ADFS – Active Directory Federal Services
API – Application Program Interface
AR – Accounts Receivable
ATSR – Agency Technology Service Requestor
CHIRP – Criminal History Information Response Process
CEP – Comprehensive Information Plan
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
FI – Financial Accounting
FM – Funds Management
FTI – Federal Tax Information
GL – General Ledger
GRC – Governance, Risk, and Compliance
HCM – Human Capital Management
HPQC – Hewitt Packard Quality Control
HR – Human Resources
HRIS – Human Resources Information System
ICN – Illinois Century Network
ID – Identification
ILCS – Illinois Compiled Statutes
ILTA – Illinois Tollway
IOC – Illinois Office of Comptroller
IOCA – Illinois Office of the Comptroller Accounts
IP – Internet Protocol
IT – Information Technology
JE – Journal Entries
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
ORAQ – Organizational Risk Assessment Questionnaire
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
RMP – Risk Management Program
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
SSO – Single SignOn
STIL – State of Illinois