STATE OF ILLINOIS
DEPARTMENT OF INNOVATION AND TECHNOLOGY

INFORMATION TECHNOLOGY HOSTING SERVICES

REPORT ON THE DESCRIPTION OF THE INFORMATION TECHNOLOGY HOSTING SERVICES AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF THE CONTROLS RELEVANT TO SECURITY AND AVAILABILITY
FOR THE PERIOD JULY 1, 2020 TO JUNE 30, 2021

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

Honorable Frank J. Mautino
Auditor General, State of Illinois

Scope

We have examined the State of Illinois, Department of Innovation and Technology's (Department) accompanying description of its Information Technology (IT) hosting services titled "State of Illinois, Information Technology Hosting Services" throughout the period July 1, 2020 through June 30, 2021, (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2020 through June 30, 2021**,** to provide reasonable assurance that the Department's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability *(applicable trust services criteria)* set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Trust Services Criteria).*

The information included in Section V, "Other Information Provided by the Department That is Not Covered by the Service Auditor's Report", is presented by the Department's management to provide additional information and is not part of the Department's description. Information about the Department's corrective action plan has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve the Department's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

The Department uses the Department of Central Management Services, a subservice organization to provide building maintenance activities; Zayo Group, LLC, a subservice organization to provide an alternate data center for off-site storage and replication of the production environment; Microsoft, LLC, a subservice organization to provide cloud hosting services; BMC Software, Inc., a subservice organization to provide hosting services for service management tool; NICUSA, Inc., a subservice organization to provide hosting services and software as a service; Google LLC, a subservice organization to provide a web-based solution; Micro Focus Software, Inc., a subservice organization to provide project and portfolio management tools; Docusign, Inc., a subservice organization to provide software as a service; Okta, Inc., a subservice organization to provide identity as a services; RiskSense, Inc., a subservice organization to provide vulnerability management system; ServiceNow,Inc., a subservice organization to provide hosting services; Splunk, Inc., a subservice organization to provide cloud hosting services; and Salesforce, Inc., a subservice organization to provide hosting services and software as a service. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Department, to achieve the Department's service commitments and system requirements based on the applicable trust services criteria. The description presents the Department's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Department's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Department, to achieve the Department's service commitments and system requirements based on the applicable trust services criteria. The description presents the Department's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the Department's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

The Department is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Department's service commitments and system requirements were achieved. The Department has provided the accompanying assertion, titled "Assertion of the Department of Innovation and Technology's Management" (assertion), about the description and the suitability of design and operating effectiveness of controls stated therein. The Department is also 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; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls 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 our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.

- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.

- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

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

Controls That Did Not Operate During Period

1) The Department's description of system discusses its request for administrative account access, which include controls related to the access provisioning process. However, during the period July 1, 2020 through June 30, 2021, the Department did not have a request for new administrative accounts. Because these controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criterion CC6.2, *Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*

2) The Department's description of system discusses the backup process, which include controls related to remediation of failed backups. However, during the period July 1, 2020 through June 30, 2021, the Department did not encounter failed backups. Because these controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criterion A1.2, *The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.*

Basis for Qualified Opinion

Our examination disclosed:

1) The Department states in the description of its system that it has controls in place to complete employee performance evaluations annually and at varying intervals for probationary employees. However, as noted on page 46 of the description of tests of controls and the results thereof, controls related to performance evaluations were not annually performed or were not performed in accordance to the applicable intervals and, therefore, were not operating effectively throughout the period July 1, 2020 to June 30, 2021. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC1.5, *The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*

2) The Department states in the description of its system that it has controls in place to conduct risk assessments for each agency. However, as noted on page 51 of the description of tests of controls and the results thereof, controls related to risk assessments were not consistently performed and, therefore, were not operating effectively throughout the period July 1, 2020 to June 30, 2021. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC3.1, *The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*

3) The Department states in the description of its system that it has controls in place to require access modifications to the State of Illinois, Department of Innovation and Technology's resources begins with the submission of a Remedy service request approved by an Agency Technology Service Requestor. However, as noted on page 58 of the description of tests of controls and the results thereof, a population of Active Directory access modifications to the State of Illinois, Department of Innovation and Technology's resources could not be provided, and therefore, tests of the operating effectiveness of this control could not be performed for the period. Consequently, we were unable to determine whether the Department's controls operated effectively during the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC6.2, *Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*

4) The Department states in the description of its system that it has controls in place to require security software access modifications to the State of Illinois, Department of Innovation and Technology's mainframe resources begin with the submission of a Remedy service request or Mainframe Request. However, as noted on page 59 of the description of tests of controls and the results thereof, a population of security software access modifications to the State of Illinois, Department of Innovation and Technology's mainframe resources could not be provided, and therefore, tests of the operating effectiveness of this control could not be performed for the period. Consequently, we were unable to determine whether the Department's controls operated effectively during the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC6.2, *Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*

5) The Department states in the description of its system that physical access is deactivated after official notice of separation or termination. However, as noted on page 62 of the description of tests of controls and the results thereof, documentation demonstrating the terminated individuals' access badges were deactivated could not be provided, and therefore, tests of the operating effectiveness of this control could not be performed for the

period. Consequently, we were unable to determine whether the Department's controls operated effectively during the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC6.4, *The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.*

6) The Department states in the description of its system that changes with significant or extensive impact require test, implementation and backout plans. In addition, approval is required prior to being placed into production. However, as noted on page 74 of the description of tests of controls and the results thereof, test, implementation and backout plans were not consistently provided. Additionally, approvals prior to be placed into production were not consistently obtained. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion CC8.1, *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objective.*

Opinion

In our opinion, except for the effects of the matters giving rise to the modification described in the preceding paragraph, in all material respects,

a. the description presents the State of Illinois, Information Technology Hosting Services that was designed and implemented throughout the period July 1, 2020 to June 30, 2021 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period July 1, 2020 to June 30, 2021 to provide reasonable assurance that the Department's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Department's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period July 1, 2020 to June 30, 2021, to provide reasonable assurance that the Department's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of the Department's controls operated effectively throughout that period.

Emphasis of Matter

As noted in the Description of the State of Illinois, Information Technology Hosting Services for the IT hosting services, effective March 21, 2020, the Governor of the State of Illinois signed

Executive Order 2020-10 requiring all individuals currently living within the State of Illinois to stay at home or at their place of residence, as a result of the global pandemic related to the COVID-19 outbreak. The Description of the State of Illinois, Information Technology Hosting Services for the IT hosting services documents the changes to the Department's internal controls due to the requirements of Executive Order 2020-10.

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

Other Reporting Required by Government Auditing Standards

In accordance with *Government Auditing Standards*, we have also issued our report dated August 4, 2021, on our consideration of the State of Illinois, Department of Innovation and Technology's internal control over (1) fairly presenting the State of Illinois, Department of Innovation and Technology's description of its State of Illinois, Information Technology Hosting Services throughout the period July 1, 2020 to June 30, 2021, and (2) establishing and maintaining effective internal control over the suitable design and operating effectiveness of the controls related to the control objectives within the State of Illinois, Department of Innovation and Technology's description of its IT hosting services throughout the period July 1, 2020 to June 30, 2021 (internal control over reporting), and on our tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, and other matters, limited to the scope of this report. The purpose of that report is solely to describe the scope of our testing of internal control over reporting and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the State of Illinois, Department of Innovation and Technology's internal control over reporting or on compliance. That report is an integral part of an examination performed in accordance with *Government Auditing Standards* in considering the State of Illinois, Department of Innovation and Technology's internal control over reporting and compliance.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the State of Illinois, Department of Innovation and Technology, user entities of the State of Illinois, Department of Innovation and Technology's Information Technology Hosting Services during some or all of the period from July 1, 2020 to June 30, 2021, and user entities of the Department subject to risk arising from interactions with the report, including the description of tests of controls and results thereof in Section IV, and is intended solely for the information and use of the State of Illinois, Information Technology Hosting Services, practitioners providing services to such user entities, and prospective user entities who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than the specified parties.

SIGNED ORIGINAL ON FILE
Jane Clark, CPA
Director of Financial and Compliance Audits

SIGNED ORIGINAL ON FILE
Mary Kathryn Lovejoy, CPA, CISA
Principal of IS Audits

August 4, 2021
Springfield, Illinois

SECTION II

ASSERTION OF THE MANAGEMENT OF THE STATE OF ILLINOIS, DEPARTMENT OF INNOVATION AND TECHNOLOGY

Illinois Department of
Innovation & Technology

JB Pritzker, Governor
Jennifer Ricker, Acting Secretary

Assertion of the Management of the State of Illinois,
Department of Innovation and Technology

Honorable Frank J. Mautino
Auditor General, State of Illinois

We have prepared the accompanying description of the State of Illinois, Department of Innovation and Technology's Information Technology (IT) hosting services system titled "State of Illinois, Information Technology Hosting Services" throughout the period July 1, 2020, to June 30, 2021, (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the IT hosting services system that may be useful when assessing the risks arising from interactions with the State of Illinois, Department of Innovation and Technology's system, particularly information about system controls that the State of Illinois, Department of Innovation and Technology has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The State of Illinois, Department of Innovation and Technology uses subservice organizations to provide building maintenance activities of Department occupied facilities, hosting services, software as a service, identity as a service, vulnerability management system, web-based solution, project and portfolio management tool, and an alternate data center. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the State of Illinois, Department of Innovation and Technology to achieve the State of Illinois, Department of Innovation and Technology's service commitments and system requirements based on the applicable trust services criteria. The description presents the State of Illinois, Department of Innovation and Technology's, controls the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the State of Illinois, Department of Innovation and Technology, to achieve the State of Illinois, Department of Innovation and Technology's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

1. The description presents the State of Illinois, Department of Innovation and Technology's State of Illinois, Information Technology Hosting Services system that was designed and implemented throughout the period July 1, 2020, to June 30, 2021, in accordance with the description criteria.

2. The controls stated in the description were suitably designed throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that the State of Illinois, Department of Innovation and Technology's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls throughout that period.

3. Except for the matters described below, the controls stated in the description operated effectively throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that the State of Illinois, Department of Innovation and Technology's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of the State of Illinois, Department of Innovation and Technology's controls operated effectively throughout that period.

    a. The description states on page 46 there are controls in place to complete employee performance evaluations annually and at varying intervals for probationary employees. However, performance evaluations were not annually performed or were not performed in accordance to the applicable intervals. As a result, the State of Illinois, Department of Innovation and Technology's controls were not operating effectively to provide reasonable assurance that the State of Illinois, Department of Innovation and Technology's service commitments and system requirements were achieved based on trust services criterion CC1.5, *The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*

    b. The description states on page 51 there are controls in place to conduct risk assessments for each agency. However, risk assessments were not consistently performed. As a result, the State of Illinois, Department of Innovation and Technology's controls were not operating effectively to provide reasonable assurance that the State of Illinois, Department of Innovation and Technology's service commitments and system requirements were achieved based on trust services criterion CC3.1, *The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*

    c. The description states on page 58 there are controls in place to require access modifications to the State of Illinois, Department of Innovation and Technology's resources begins with the submission of a Remedy service request approved by an Agency Technology Service

Requestor. However, a population of Active Directory access modifications to the State of Illinois, Department of Innovation and Technology's resources could not be provided. As a result, the State of Illinois, Department of Innovation and Technology's controls were not operating effectively to provide reasonable assurance that the State of Illinois, Department of Innovation and Technology's service commitments and system requirements were achieved based on trust services criterion CC6.2, *Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*

d. The description states on page 59 there are controls in place to require security software access modifications to the State of Illinois, Department of Innovation and Technology's mainframe resources begin with the submission of a Remedy service request or Mainframe Request. However, a population of security software access modifications to the State of Illinois, Department of Innovation and Technology's mainframe resources could not be provided. As a result, the State of Illinois, Department of Innovation and Technology's controls were not operating effectively to provide reasonable assurance that the State of Illinois, Department of Innovation and Technology's service commitments and system requirements were achieved based on trust services criterion CC6.2, *Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*

e. The description states on page 62 there are controls in place to require physical access be deactivated after official notice of separation or termination. However, documentation demonstrating the terminated individuals' access badges were deactivated could not be provided. As a result, the State of Illinois, Department of Innovation and Technology's controls were not operating effectively to provide reasonable assurance that the State of Illinois, Department of Innovation and Technology's service commitments and system requirements were achieved based on trust services criterion CC6.4, *The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.*

f. The description states on page 74 there are controls in place that changes with significant or extensive impact require test, implementation and backout plans. In addition, approval is required prior to being placed into productions. However, test, implementation and backout plans were not consistently provided. Additionally, approvals prior to be placed into productions were not consistently obtained. As a result, the State of Illinois, Department of Innovation and Technology's controls were not operating effectively to provide reasonable assurance that the State of Illinois, Department of Innovation and Technology's service commitments and system requirements were achieved based on trust services criterion CC8.1, *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objective.*

SIGNED ORIGINAL ON FILE

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

SECTION III

DESCRIPTION OF THE STATE OF ILLINOIS, INFORMATION TECHNOLOGY HOSTING SERVICES

Scope and Boundaries of the System

This is a System and Organization Controls ("SOC") 2 Type 2 report and includes a description of the Department of Innovation and Technology's (Department) IT hosting services, and the controls in place to provide reasonable assurance the Department's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) (applicable trust services criteria), throughout the period July 1, 2020 through June 30, 2021, which may be relevant to users of the Department's IT hosting services. It does not encompass all aspects of the services provided or procedures followed for other activities performed by the Department.

The Description is intended to provide information for client agencies and their independent auditors to understand the systems and controls in place for the Department's IT hosting services. The client agencies are responsible for and maintain the design, implementation, security, and operation of their applications and data.

Background

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

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

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

Subservice Organizations

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

Subservice Organization	Subservice Organization Description
The Department of Central Management Services (DCMS)	Provides building maintenance activities of Department occupied facilities.
BMC Software, Inc.	Provides hosting services for the Department's service management tool, Remedy On Demand.
Docusign, Inc.	Provides a cloud-based software as a service for managing

	the Department's electronic agreements.
Google, LLC	Provides a web-based software as a service solution.
Microsoft, LLC	Provides cloud hosting services related to the production environment.
Micro Focus Software, Inc.	Provides a project and portfolio management tool.
NICUSA, Inc.	Provides hosting services and a web-based Statewide Permits and Licensing Solution.
Okta, Inc.	Provides a cloud-based service for the Department's identity and access management.
RiskSense, Inc.	Provides a cloud-based service for risk-based vulnerability management.
Salesforce, Inc.	Provides hosting services and a web-based solution.
ServiceNow, Inc.	Provides a cloud-based service for managing the Department's Information Technology services, including help desk ticketing services.
Splunk, Inc.	Provides hosting services and a web-based interface for the Department data analytics.
Zayo Group LLC	Provides an alternate data center for off-site data storage and replication of the production environment.

Services Provided

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

- management of the procurement, retention, installation, maintenance, and operation of information technology 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.

Principal Service Commitments and System Requirements

The Department's principle service commitments and system requirements are documented and communicated to agencies within the Service Catalog, published on the Department's website. Service commitments and system requirements vary based on the services being provided; however, common commitments and system requirements in place include the following:

- Server deployment and management,
- Mainframe management,
- System monitoring,
- System patching and configuration,
- Data replication and storage, and
- Logical and physical security.

System Incidents

The Department defines a system incident as an occurrence that would lead to the loss of, or disruption to, operations, services, or functions and result in the Department's failure to achieve its service commitments or system requirements. Such an occurrence may arise from a security event, security incident, failure to comply with applicable laws and regulations, error or by other means. In determining whether a system incident occurred, criteria may include, but are not limited to, the following:

- Whether the occurrence resulted from one or more controls that were not suitably designed or operating effectively.
- Whether the occurrence resulted in a significant failure in the achievement of one or more of the Department's service commitments and system requirements.
- Whether public disclosure of the occurrence was required (or is likely to be required) by laws or regulations.
- Whether the occurrence had a material effect on the Department's financial position or results of operations.
- Whether the occurrence resulted in sanctions by any legal or regulatory agency.

Incidents and events relevant to security and availability are important in monitoring, identifying and evaluating if a system incident has occurred, however incidents and events relevant to security and availability do not always rise to the level of a system incident. An evaluation of an incident or event relevant to security and availability will make that determination.

The Department did not identify any system incidents that occurred during the period based on these criteria.

Components of the System Used to Provide the Services

The State of Illinois' IT environment is housed in the Department's secured Central Computing Facility (CCF) and Communications Building.

Infrastructure

Midrange

The Department's midrange configuration consists of physical and virtual devices. These midrange devices host the various services the Department offers. The midrange primary operating systems software includes:

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

Mainframe

The Department's mainframe configuration consists of multiple CMOS processors (Complementary Metal Oxide Semiconductor processors) segregated into logical 'production' and 'test' partitions. Partitions are configured in a [redacted] platform, IBM's systems complex coupling environment.

The primary operating system software includes:

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

Primary z/OS subsystems include:

- The Customer Information Control System (CICS) is a software product that enables online transaction processing. CICS allows numerous transaction types, entered from multiple terminals, to be processed concurrently by user written application programs. CICS acts as an interface between the operating system and application programs.
- Information Management System (IMS), which is an online database software subsystem, used as the control architecture under which online database system applications process. An IMS system is capable of running many different applications within a single definition of one or more "Message Processing Region" and one "Control Region".
- DataBase 2 (DB2) is a relational database management system for z/OS environments.
- The primary z/VM subsystem is [redacted] which is a database software system.

<u>Software</u>

The software consists of application programs and IT system software that supports application programs (operating systems, middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain and monitor the infrastructure include:

Network Monitoring Tools

- [redacted] - Network monitoring until February 2021
- [redacted] - Network monitoring –began utilization in March 2021
- [redacted] Network monitoring - began utilization in February 2021

Infrastructure Monitoring Tools

- [redacted] - Infrastructure monitoring and management tool
- [redacted] Center Configuration Manager - System management tool
- [redacted] - Database server monitoring
- z/OS System Console - Mainframe monitoring
- [redacted] - Mainframe monitoring

Network Security Tools

- [redacted] - Network access control management tool
- [redacted] - Network access control management tool

Change Management Tools

- Remedy On Demand - Change ticketing system

Service Management Tool

- Remedy On Demand - Service ticketing system,

Vulnerability Management Tools

- [redacted] - Vulnerability scanning

Data Backup and Replication Tools

- [redacted] - Backup tool
- [redacted] - Backup tool
- [redacted] - Backup tool

<u>People</u>

The Department's organizational hierarchy supports internal controls starting with the Department's Secretary. The Secretary is a member of the Governor's Cabinet and is the "Chief Information Officer for the State and the steward of State data with respect to those agencies under the jurisdiction of the Governor" per Section 1-30 of 20 ILCS 1370. During the examination period, two individuals have served in this capacity, one as Secretary through September 4, 2020, and one as Acting Secretary beginning September 5, 2020 to present.

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

The Department's organizational hierarchy promotes separation of duties, monitoring of controls, and customer support through staff positions of: Affirmative Action/Equal Employment Opportunity Officer, Chief Administrative Officer, Chief Internal Auditor, Chief Information Security Officer, Chief Service Officer, Chief of Staff, Chief Enterprise Architect, Chief Technology Officer, Chief Data Officer, Enterprise Resource Planning (ERP) Program Director, and seven CIOs grouped into service delivery taxonomies.

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

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

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

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

The Chief Service Officer (vacant from July 1, 2020 to present) plans, coordinates, reviews, and directs long and short-term strategic goals, policies, and procedures based on the Department’s mission and initiatives with the ultimate goals of understanding, satisfying, and exceeding, if possible, customer expectations.

The Chief of Staff advises the Secretary on the transformation status of legacy agency resources (personnel and equipment) to meet the requirements of the Act and provides the authority for transferring State resources into the Department. The Chief of Staff also supervises functional areas of the Department’s fiscal officer, budget director, legislative liaison, communications and General Counsel (reporting structure moved here effective December 16, 2020).

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

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

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

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

The seven Group CIOs promote quality of service and enhance the effectiveness of the Department's internal control environment through information exchange, general oversight of agency information processing, and strategic planning participation. The Group CIOs enhance agency awareness of Department policies, procedures, objectives, and new initiatives as well as providing a channel to communicate agency concerns and recommendations. These responsibilities have been categorized into seven (7) groups reflecting Statewide agency services. Categories are (1) family, children, elderly, and veterans (through March 31, 2021 at which time the name of the group was clarified to reflect health and human services effective April 1, 2021); (2) government and public employees; (3) business and workforce; (4) natural and cultural resources; (5) public safety (vacant March 1, 2021 to present); (6) education; and (7) transportation. The Transportation Group CIO position has not yet been filled.

Processes and Procedures

The Department enterprise information security policies and procedures provide guidance to all State of Illinois agencies, boards, commissions, trusted partners and information technology service providers and serve as a foundation for detailed divisional and departmental policies and procedures. The automated and manual procedures involved in the operation of the system, including how services are initiated, authorized, performed and delivered in a secure manner, are included in the system description.

The policies located on the Department's website (https://www2.illinois.gov/sites/doit/support/policies/Pages/default.aspx) 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 enterprise information security policies are reviewed by the Department every three years, or more frequently when significant changes to the environment warrant an update.

Data

Client agencies' data is managed and stored in accordance with the relevant data protection and other regulations and with specific requirements established by the client agencies. The client agencies define and control the data loaded on the Department's infrastructure.

Data is monitored and security hardened. Department storage appliances have encryption at rest in place and self-encrypted drives where available. The agencies are responsible for encrypting sensitive data in motion.

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

Description of the Controls Relevant to the Security Trust Services Category

Control Environment

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. *(CC1.1.A*)

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 (*CC1.3.D, CC1.4.E*) 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. (*CC1.3.A*) Each State employee position (job protected or at will) is identified on the organizational chart. (*CC1.3.B, CC1.4.D*) 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). (*CC1.3.C*)

New employee and Personal Service Contractors (PSC) must pass applicable background checks prior to being offered employment. (*CC1.1.B, CC1.4.A*)

Annually, performance evaluations are completed. Additionally, for employees' service probationary periods, performance evaluations are completed at varying intervals. (*CC1.5.A*)

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

Newly-hired employees are provided the DCMS Policy Manual during New Employee Orientation. They are required to sign an acknowledgment form stating the individual is bound to act in accordance with the DCMS Policy Manual and all updates provided or be subject to discipline, up to and including discharge. (*CC1.1.C, CC2.2.G*) New Employee Orientation is being conducted virtually due to COVID-19 remote work directives.

Newly-hired PSCs are governed by the terms, conditions, and duties outlined in their legally-binding contract. (*CC1.1.D*) 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." (*CC1.1.E, CC2.2.H, CC2.3.F*)

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

- Harassment and Discrimination Prevention Training as required by the State Officials and Employees Ethics Act (5 ILCS 430/1).
- Illinois Department of Revenue, Information Safeguarding Training regarding the protection of Federal Tax Information (FTI).
- Ethics Training Program for State of Illinois Employees and Appointees.
- Security Awareness Training as required by the Illinois Data Security on State Computers Act (20 ILCS 450/25). (*CC1.1.F, CC1.4.B, CC1.5.B, CC2.2.I*)

In addition, newly-hired employees and PSCs are provided the Acceptable Use Policy and are required to complete the Acceptable Use Policy Certification stating the individual will comply with the State's policies and regulations. This Acceptable Use Policy Certification is completed once, at the time of hire. (*CC1.1.H, CC1.5.D, CC2.2.K)*

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

Annually, employees and PSCs are required to complete the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training Program for State of Illinois Employees and Appointees, and Security Awareness Training via paper or OneNet and complete the acknowledgement of participation. (*CC1.1.G, CC1.4.C, CC1.5.C, CC2.2.J*)

Communication and Information

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. (*CC2.2.A, CC2.3.E, CC5.3.A*)

The Department has implemented various policies and procedures relevant to security. *(CC2.1.B)* The Department has published its security related policies and procedures on its website. (*CC5.3.D*) A list of these policies has been provided in the section entitled "Policies and Procedures" above.

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. (*CC2.2.F*) The Department's Division of Information Security is responsible for ensuring Department's compliance with enterprise information security policies. (*CC2.2.E)*

The website also provides links to the DoIT Digest content, which informs the reader of new initiatives, business applications, ongoing projects, administrative information, and Departmental news. (*CC2.2.B*)

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. (*CC2.2.C*)

Due to COVID-19 and State employees working remotely, Remote Work Reminders are published on the Employee Portal when there is remote work news or information to share to facilitate work from home. A Remote Work webpage was published on the Department's website to provide guidelines and additional resources to support employees working remotely. (*CC2.2.D, CC5.3.B*)

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. (*CC2.3.A*) 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. (*CC2.3.B*)

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. (*CC2.3.C)*

Risk Assessment

The Department has established a Risk Management Program (RMP) to offer guidelines on how to reduce risk across the enterprise. (*CC2.1.A*) The RMP includes several components that leverage the National Institute of Standards and Technology (NIST) framework as a foundation. NIST provides a comprehensive series of technical and non-technical (i.e., administrative) controls that act as safeguards and countermeasures prescribed to protect the confidentiality, integrity, and availability of data and information systems. (*CC3.3.A*)

An Enterprise Information Security Risk Assessment Policy has been published on the Department's website. (*CC3.1.C*)

The Department conducts risk assessment for each agency based on the RMP. (*CC3.1.B, CC5.1.B*) For the RMP to be effective, it is a team effort involving the participation and support of key stakeholders of the organization who interact with State of Illinois data and information systems. To ensure the accuracy of the results, the respondent must have an intimate knowledge of processes relative to applications and day-to-day business operations. The Organization Risk Assessment Questionnaire (ORAQ) is designed to gain an overall holistic view of the organization.

Risks and mitigation plans are captured and tracked in the Department's risk register. (*CC3.2.B, CC5.1.D*) 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. (*CC3.2.C, CC3.4.B, CC5.1.E*)

Managerial, operational and technical changes are discussed during the risk assessment process. (*CC5.1.F, CC5.3.C*)

In addition, the Department receives threat, vulnerability, and incident intelligence from multiple sources, including the MS-ISAC and the Illinois Statewide Terrorism and Intelligence Center.

(CC3.1.A, CC3.4.A, CC5.1.A) Risks from potential and newly discovered vulnerabilities are assessed through interaction with the Department's security staff and vendor subscription services. (CC3.2.A, CC3.4.C, CC5.1.C) The Department also maintains contact with vendors to receive vulnerability information.

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. (CC1.2.A) 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. (CC1.2.B) The Committee is to meet four times per calendar year, with the authority to convene more frequently if requested. (CC1.2.C)

Internal Audit provides the Department independent, objective assurance and consulting services by performing risk assessment exercises to create the annual audit plan. (CC4.1.B) Furthermore, internal audit performs system pre-implementation reviews to evaluate system controls. (CC4.1.C) External and internal audits' results are communicated to senior management, and management response is documented. (CC4.2.C) 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. (CC4.2.D)

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. (CC4.1.A) Critical and high level Remedy tickets that did not meet the performance metrics are discussed for potential service improvement going forward. (CC4.2.A) 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. (CC4.2.B)

Control Activities

The Department selects logical and physical security, change management, and incident monitoring control activities to manage the technology infrastructure and security access risks identified during the annual risk assessment process. (CC5.2.A)

Logical and Physical Access

In order to access the State's information technology environment, an Active Directory ID and password are required. (CC6.1.A) 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. (*CC6.1.B)*

The Department is in the process of moving from Active Directory Federal Services (ADFS) to Okta Single SignOn (SSO). As of June 30, 2021, half of the agencies' applications have been moved to Okta SSO. ADFS and Okta SSO utilize the same Active Directory credentials, in addition to two-factor authentication. (*CC6.1.P)*

Access Creation, Modification, and Revocation

Access creation or modification to Department resources (users and administrators) requires the submission of a Remedy service request from a Remedy submitter or an authorized Agency Technology Service Requestor (ATSR). (*CC6.2.A*) Only ATSR can approve the request, and the IT Service Processing team assigns Remedy tasks to support groups to satisfy the request.

For voluntary separations of an employee or a contractor, an Employee Exit form and a Remedy service request are completed to initiate and ensure the removal of access and the retrieval of equipment. (*CC6.5.A*)

Revoking access to Department resources is initiated upon receipt of a Remedy service request or under special or emergency circumstances, network access is disabled at the instruction of the Department senior management. (*CC6.2.B*) A Remedy service request is created by the ATSR or Remedy submitter after the special or emergency access revocation has occurred. The Department does not have a time frame for ensuring the access is revoked timely.

Password Resets

Active Directory accounts are reset by users calling the IT Service Desk or by one of the Department's self-service options – Microsoft Identity Management (MIM) or the Department's Identity Management (DIM) tool. (*CC6.1.C*) IT Service Desk encourages use of the self-service option.

When a call is received by the IT Service Desk for an Active Directory password reset, IT Service Desk staff will determine if the caller is eligible to use MIM/DIM and if they have previously registered. If registered, users will be directed to reset their password via this method. If they are unsuccessful, have not previously registered or are not eligible to use MIM/DIM, IT Service Desk staff will create a Remedy ticket. The IT Service Desk staff will then proceed with the reset after verification of two of three pieces of information; phone number, email address and physical address. (*CC6.1.D*) 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. (*CC6.3.A*) 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. (*CC6.3.B*) Account deletion is processed upon receipt of the Remedy request.

Administrative Access

Department staff and vendors with a business need to access or modify network devices are added to a designated Active Directory access group (for role based and least privileges) and setup with a two-factor authentication token. (*CC6.3.C*)

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

Tokens serve as a secondary confirmation and in conjunction with validated AD credentials. If the AD account is disabled or deactivated, the token is rendered ineffective and useless for authentication purposes. Token remains inactive until a challenge/response procedure is successfully completed. This procedure requires the Department's Two-Factor Authentication Administrator communicate certain information to the technician in real time to activate the token.

Mainframe Resources

The Department utilizes security software as a method of controlling and monitoring access to the mainframe resources. The security software requires an established ID and password to verify the identity of the individual. (*CC6.1.E*) The primary means of defining an individual's level of access is the security software profile. (*CC6.1.F*)

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

- Minimum password length;
- Password complexity;
- Password history;
- Minimum password age; and
- Number of invalid login attempts. (*CC6.1.G*)

Additionally, the security software passwords are maintained as encrypted values within the system security database. (*CC6.1.H*)

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

Mainframe Access Creation, Modification and Revocation

For the creation and modification of a security software account, agencies are responsible for the submission of an approved service request or Mainframe Request Form if Remedy service request is not available for the agency. Once the Remedy service request is created, or Mainframe Request Form is submitted, the Department's Software Security Coordinator will receive the Remedy ticket, and follow the Security Software ID Creation procedures to create an account as specified. (*CC6.2.C*)

On an annual basis, the Department's Security Software Coordinator sends proxy agencies and the Department a listing of security software IDs assigned to their agency and the Department for review. (*CC6.3.D*) The agencies and the Department are to review the listing and provide a response back to the Department's Security Software Coordinator stating the IDs are appropriate or indication which IDs are to be revoked, re-assigned or deleted. Additionally, on a monthly basis, the Department's Security Software Coordinator or designee runs a report documenting the Department and the proxy agencies' security software IDs which have not been utilized in the past 90-days; upon review, the IDs are revoked. (*CC6.3.E*)

The Department's Security Software Coordinator or designee runs a weekly violation report which is reviewed for invalid and unauthorized access attempts of the Department and proxy agency security software IDs. The Department's Security Software Coordinator follows up with the review results as stated in the Security Violation Report Procedure. The Department's SecuritySoftware Coordinator or designee contacts the individual or their supervisor to determine the reason for the violation. (*CC6.3.F, CC7.1.B*)

Semi-monthly, the Department's Security Software Coordinator receives a separation report documenting the separations for the month. The Department's Security Software Coordinator or designee reviews the separation reports, noting separation of individuals from the Department and proxy agencies. If a separation is noted, the Security Software Coordinator will revoke the individual's security software ID. (*CC6.3.G*)

Mainframe Password Resets

In the event a user requires a reset of their mainframe password, they are required to either submit the request via email to the IT Service Desk or use the Department's self-service option: DoIT Identity Management tool. (*CC6.1.I*) Email reset requests are to include the user's name, mainframe ID and a contact phone number. The IT Service Desk staff creates a Remedy ticket and contact the user at the number provided and reset the mainframe ID password. If the IT Service Desk staff are not able to reach the user, a message is left for the user that includes the Remedy ticket number and instructing them to contact the IT Service Desk, at which time the password will be reset.

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

In the event the IT Service Desk does not have appropriate rights to reset a mainframe password, the user is instructed to contact their Agency System Software Coordinator. In the event the Department is the agency's proxy, a Remedy ticket is assigned to the Department's Security Software Coordinator or the Department's Security Software Administrator. Using information from the Remedy ticket, the Department's Security Software Coordinator or the Security Software Administrator contacts the user to reset the password. (*CC6.1.J*) If unable to contact the user on the first attempt, a message is left asking the user to call back. No password is left in the message. Passwords used in the resetting process are temporary, one-time use only. The Remedy ticket remains open until the password has been successfully reset after which the Remedy ticket is closed.

Administrative Accounts

Access to the operating system configurations is limited to system support staff. (*CC6.2.D*) Access with powerful privileges, high-level access and access to sensitive system functions is restricted to authorized personnel. (*CC6.2.E*) To request administrative account access, the Department access provisioning process is to be followed. (*CC6.2.F*)

The System Coordinator and Mainframe manager review a high-level systems programmer user ID listing on an annual basis. (*CC6.3.J*) It is signed off on by both after the listing is deemed to be correct, or modifications have been made to the Mainframe System Security Software user IDs.

Network Security Services

Network Services is comprised of three areas of responsibilities;

- Local Area Network Services is responsible for managing firewalls, switches, servers, and software that are the components to the local area network.
- Agency Wide Area Network Services is responsible for managing firewalls, routers, switches, servers, and software that are the components to the wide area network and virtual private network infrastructures.
- Backbone Wide Area Network Services is responsible for managing wave equipment, firewalls, routers, switches, cabling, servers, and software that are the components to the backbone, wide area network as well as peering and internet access (Illinois Century Network).

Common Controls

The Department maintains network diagrams depicting common connectivity configurations. Additionally, network segmentation permits unrelated portions of the agencies' information system to be isolated from each other. Further, enterprise wide, agencies' traffic is segmented to be isolated from each other. (*CC6.6.A*)

Detailed design and configuration standards and guides are maintained to ensure the integrity of the design, security and configuration of the network. (*CC6.1.K)* Additionally, access level controls are applied through the use of Access Control Lists and Authentication Servers. Further, Access Control Lists reside [redacted]. (*CC6.6.B*)

Authentication servers control access through assignment of access right privileges (read only or update) based on Department-defined group profiles. (*CC6.3.H*) A security banner also serves as a security awareness mechanism and is displayed at initial network connection warning of prosecution for unauthorized access. (*CC6.1.L*)

Self-monitoring network routers and switches record all events, notifies [redacted] and forwards to multiple logging servers. These servers use filters to automatically generate alerts when a network services' configured parameter or condition occurs. (*CC6.8.A, CC7.1.C*)

Distributed denial of service platform is utilized to monitor and mitigate network threats. Threats are reviewed and appropriate action is taken based on the individual threat. (*CC6.8.B*)

Firewalls are in place and configured with denial rules. (*CC6.6.C*) Additionally, an intrusion detection system is in place to monitor for malicious and unauthorized activity. (*CC6.6.D*)

Local Area Network (LAN) Services
Network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to LAN Services Support staff and a console display alert when a predefined event occurs, or a threshold is reached. LAN Services Support staff follow up on these alerts and engage operational teams for resolution as necessary. (*CC6.8.C, CC7.1.D*) Alerts are tracked in the network monitoring system.

The authentication server records failed login attempts to the network equipment. (*CC6.8.D*, *CC7.1.E*) Logs are imported into the Department's security information and event management tool for archival, historical, or investigative purposes upon request.

Agency Wide Area Network (WAN) Services
Network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / or console display alert when a predefined event occurs, or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. The 24x7x365 Network Operation Center staff reviews each occurrence and engage operation teams for resolution. (*CC6.8.E, CC7.1.F*)

The authentication server records failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to the Network Design and Engineering staff to determine, on a case by case basis, if further action is required. (*CC6.8.F, CC7.1.G*)

WAN encryption technologies are utilized to protect data. (*CC6.7.H*) Encryption technologies or secured communication channels are used to protect transmission of data across public network providers as requested by agencies for security compliance when agency applications do not transmit encrypted data. When data travels across a public network, it is encrypted at the access router and while in transit across the public network until it reaches the distribution router and enters the private network. (*CC6.1.O*)

Virtual Private Networks (VPN) provide controlled and trusted connections between devices when required for data traversing public networks including the Internet. (*CC6.1.M, CC6.6.E)* The

Department's Enterprise VPN Standard provides guidance when establishing a VPN connection. (*CC6.1.N*)

Backbone Wide Area Network (WAN) Services
Network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / or console display alert when a predefined event occurs or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. Alerts are tracked in the Network monitoring system. (*CC6.8.G, CC7.1.H*)

Authentication Servers record failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to Network Design and Engineering staff to determine, on a case by case basis, if further action is required. (*CC6.8.H, CC7.1.I*)

Endpoint Protection

Workstations
The Endpoint Protection Group is responsible for management of the [redacted] is used to detect, investigate security incidents, and provide guidance for remediation to the endpoint cyber threats. [redacted] continuously monitors endpoint telemetry, to detect and respond to malware and exploits. (*CC6.8.J*) The Endpoint Protection group, following the Department's Change Management Process, ensures all the systems are operating with a vendor supported version of the [redacted] Additionally, agencies are responsible for notifying the Department of actual or suspected information security breaches, compromised accounts, or unauthorized access.

As of June 30, 2021, only one agency is still in process of migrating from definitions-based antivirus software to the [redacted] for their workstations. (*CC6.8.K*)

Servers
The Endpoint Protection Group is responsible for pushing antivirus definitions and antivirus software updates out. Antivirus software is applied to manage definitions and software updates. Antivirus software is used to automatically push virus definition files to all systems after receipt from antivirus vendors. (*CC6.8.I*) The Endpoint Protection Group monitors the state of systems and detect systems which fail to load updates and are not running the latest supported version. The Endpoint Protection Group follows the Department's Change Management Process to bring these systems up to date. Additionally, agencies are responsible for notifying the Department of actual or suspected information security breaches, compromised accounts, or unauthorized access.

Data Transmission Protection
The secure, encrypted transfer of mainframe data is achieved using the File Transfer Protocol Secure (FTPS). (*CC6.7.A*) The software MOVEit is used to transmit midrange data between servers and applications and provides email alerts for any failures to Department and agency support staff. (*CC6.7.B, A1.2.W*)

Access to MOVEit systems are reviewed and followed up on an annual basis by the Department's Midrange Wintel Group. (*CC6.3.I*)

Another option available to valid Illinois.gov users for the secure transmission of data is the file transfer utility 'FileT'. (*CC6.7.C*) This utility uses random key generation to access files stored on a server. (*CC6.7.D*) Only those with a valid key may download files from the server. Files are automatically purged from the server after five days. (*CC6.7.E*) The sender must acknowledge a warning of unauthorized access message by clicking a box before transfer is allowed. (*CC6.7.F*) The sender receives a confirmation message containing a link to the transfer status as well as a link to remove the file from the server if necessary. A valid Illinois.gov email address is required to use this utility for State resources; either as the recipient or the sender. (*CC6.7.G*)

The Department also utilizes outgoing email encryption technology in both on-premises and cloud email exchange servers. The email encryption technology is configured to utilize [redacted] by default, and user can specify that encryption be utilized. (*CC6.7.I*)

Physical Security Access Controls
The CCF and Communications Building house the State's infrastructure. The following security controls are implemented at the facilities:

- The CCF and the Communications Building are monitored 24x7x365 by security guards. (*CC6.4.A*)

- The CCF and Communications Building are monitored by security cameras located at various interior and exterior points. The security cameras are monitored by the security guards. (*CC6.4.B*)

- The CCF and Communications Building maintain building access and perimeter monitoring. (*CC6.4.C*)

- The interior and exterior of the CCF and Communications Building access are enforced by card key access. (*CC6.4.D*)

- To obtain a card key (badge) for access to the CCF and Communications Building, an ID Badge Request Form is submitted by an authorized individual to HR. In the event the individual requires access to the CCF secured area, additional authorization is required. (*CC6.4.E*) The Department's HR enters the applicable access rights into the Velocity system (card key (badge) system), obtains valid proof of identity and a photo to obtain a card key (badge). (*CC6.4.F*) In order for non-state employees to obtain a card key (badge) documentation of a clear background check, performed in the past five years, must be provided prior to initial badge issuance. (*CC6.4.G*) The card key (badge) is then created with approved access rights.

The card key (badge) access is revoked at the expiration date or upon official notice of separation or termination. (*CC6.4.H*) An ID Badge Request Form is submitted by an authorized individual documenting the request for deactivation.

- The Department's Midrange Wintel Manager or designee conducts monthly reviews of individuals who were granted access or had access removed in the prior month to the CCF secured area. (*CC6.4.I*) In addition, the Department's Security team conducts quarterly access reviews of all individuals with access to the CCF (starting in December 2020), and Communication Building. (*CC6.4.J*) Further, the Department's Security team conducts monthly reviews of all individuals with access to the CCF secured area. (*CC6.4.K*)

- Visitors are required to provide identification and sign the visitor log in order to gain access to the CCF and Communications Building. (*CC6.4.L*) The visitors are provided a visitor badge, with no access rights. The visitor is required to be escorted at all time. (*CC6.4.M*)

- In the event an individual does not have their card key (badge) readily available, the security guards may issue a temporary access card key (badge). The access rights, as documented in Velocity, are associated with the card key (badge). (*CC6.4.N*)

  In addition, temporary badges are issued to authorized vendors once identification has been validated. (*CC6.4.O*) The temporary badges allow the vendor access without escort.

System Operations

The Cyber Threat Intel Team employs a vulnerability scanning process to assess servers identified through server discovery scan for each agency. Vulnerability scans are scheduled weekly. The Department shares vulnerability scanning results with Group CIO's and agency CIO's via email weekly. (*CC7.1.A*) The Department provides client agencies with the Agency Instructional Guide for Submitting Vulnerability and Remediation Tickets to mitigate identified server vulnerabilities. (*CC7.2.A*) Unremediated vulnerabilities will continue to be reported in the weekly scan reports.

Lost or Stolen Equipment

As published in the Acceptable Use Policy, agencies or users are responsible for reporting lost or stolen equipment to the IT Service Desk. Upon notification, the IT Service Desk will initiate a Remedy ticket to track and document the event.

An encryption protection feature is installed as part of laptop imaging prior to deployment. The Department's End User Computing (EUC) Image Management verifies encryption status. If the device was encrypted, the Remedy ticket is assigned to Property Control unit for disposition.

If encryption is inactive or was not installed as part of the device imaging process prior to deployment, EUC Image Management will assign the Remedy ticket to the Security Operations Center (SOC) who will enact a breach investigation that consists of steps outlined in their

Security Incident Playbook. (CC6.7.J, CC7.3.D) If it is determined no sensitive or confidential data resided on the device, the SOC will update the Remedy ticket and assign to Property Control unit for disposition. Otherwise, the SOC assists with the investigation to mitigate the impact of the potentially compromised data and affected users. Documentation, correspondence, and resolution actions are recorded and captured in the SOC's incident reporting tool. If further investigation is required, the Property Control unit forwards a copy of the police report to the Illinois State Police.

Security Operations Center

The Security Operations Center monitors the network for the detection and analysis of potential security intrusions, cybersecurity threats, and incidents. (CC7.2.F) Depending on the threat, the Security Operation Center has established Standard Operating Procedures to assist with the detection, analysis and resolution. (CC7.2.G) The Security Operations Center is available 7 days a week during normal business hours, longer during periods of elevated risk. Security incidents are monitored by the Communication Management Center during non-business hours.

Upon notification of a threat, the Department follows the Cyber Security Incident Response Plan. (CC7.3.E) For identified high or medium risk incidents, an executive summary is sent from the Incident Response Case Management to the Deputy CISO and CISO upon closure for their awareness. (CC7.4.C) The Security Operations Center's incident response details are available in the System Operations Center's Incident Response Case Management system for management to review. (CC7.5.A)

Network Operations Center

The Network Operations Center monitors 24x7x365 for network devices and bandwidth for outages and alerts from the network monitoring systems. (CC7.2.J) When the Network Operations Center receives alerts, the Network Operations Center staff determines if further action is required and engages operational teams for resolution as necessary. A service ticket is created as necessary to track the alert until remediation is completed.

Computer Operations

The Computer Operations Center utilizes software and the Automated Operations Console to continuously monitor the mainframe and midrange environment 24x7x365. (CC7.2.B) Problems, issues, and incidents are recorded via the Daily Shift Reports and a Remedy ticket is created. (CC7.2.C, CC7.3.F) The problem, issue or incident is tracked via Remedy until resolution.

The Daily Shift Report documents the activity conducted on mainframe production systems and incident calls received at the Computer Operations Center. The Report contains the date, time, and system involved in the incident, along with a narrative providing any necessary information regarding the incident. The Report is forwarded to Enterprise Infrastructure management and supervisors for awareness and follow-up of outstanding issues. (CC7.2.D, CC7.3.B)

The Operator Shift Change Checklist (an action list shared between shifts) is completed at the beginning of each shift to ensure the production systems are operating appropriately and any open items are passed on to the next shift and to identify any changes which need to be made. The Operator Shift Change Checklist is signed off by Operations Center supervisors. (CC7.2.E)

IT Service Desk

An incident is defined as an unplanned interruption to an IT service, reduction in the quality of an IT service, or a failure of a configured item. Agencies are responsible for reporting incidents to the IT Service Desk.

The Incident Management Process Guide documents Department workflow and remediation processes for incidents reported to the IT Service Desk. (*CC7.3.A, CC7.4.F, CC7.5.B*)

When the IT Service Desk receives a report of an incident, a Remedy ticket is opened, documenting the user's name, agency, and contact information along with a detailed description of the incident. (*CC7.4.A*) Each incident is categorized based on the service, system, or application impacted by the incident. Tickets are also prioritized based on the impact (the number of affected users) and urgency (how quickly the resolution is needed) of the incident. (*CC7.4.B*) The IT Service Desk then assigns the Remedy ticket to the applicable service group for remediation and closure of the ticket. Reported incidents are tracked via a Remedy ticket until appropriate remediation efforts are completed. (*CC7.4.D*)

The IT Service Desk follows a Major Incident Process for incidents that meet the criteria as documented in the Incident Management Process Guide. The Major Incident Process provides a method for escalated handling of an incident to help facilitate a quicker resolution time, as well as provide notifications/updates to Department staff. (*CC7.4.E*)

Due to COVID-19 and State employees working remotely, the Department has experienced a large increase in the volume of reported incidents. The response to incidents requiring on-site visits was delayed. At the same time, priority was given to those incidents that were related to remote access. The backlog of unassigned incidents has been addressed by engaging additional Department staff.

Change Management

Control over changes to the network, mainframe, mainframe patching, and midrange infrastructures as well as to data storage devices are documented in the Change Management Process Guide, ROD Change Management Guide, and the Change Management User Guide which provides a quick reference of the Department's change processes. (*CC8.1.A*) z/OS production systems are updated quarterly and when patches become available, all other mainframe software components (IMS, CICS, DB2, ISV, etc) are updated. (*CC8.1.B)*

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

The Change Advisory Committee (CAC) supports the authorization of changes and assists Department managers and technicians in assessing and prioritizing changes and makes recommendations regarding significant impacts. The CAC consists of individuals from the Department as well as from multiple agencies and is chaired by the Enterprise Change Manager. Minutes, along with reports, are posted to the Change Management SharePoint site, accessible by authorized agency personnel.

Changes with a significant or extensive impact require test, implementation, and back out information be provided within the change request. (*CC8.1.C*) Change requests are classified into class and impact categories with the level of approval is based on the assigned impact. Approval is required prior to being placed into production. (*CC8.1.D*)

In the event of an emergency, only verbal approval by a supervisor is required to begin remediation. Remedy documentation is finalized once the emergency has subsided. Emergency changes require a Post Implementation Review be provided within the change request. (*CC8.1.E*)

The Department follows the Server Patch Management procedures for receiving and deploying Microsoft Windows patches monthly. *(CC8.1.F)* The patches are first tested with the technical staff, a pilot group, and then pushed out to the general population. The Department utilizes [redacted] to push and monitor Windows patches after obtaining approval. *(CC8.1.G)*

The Department follows the applicable patching procedures for the Linux, VMware and Unix (AIX) patches are implemented when provided by the vendor. (*CC8.1.H*) The patches are reviewed and tested by technicians and follow the Department's change management process. (*CC8.1.I*)

Risk Mitigation

Monitoring of Subservice Providers

The GRC group collects and reviews subservice providers' System and Organization Controls (SOC) reports from BMC Software, Inc., Docusign, Inc., Microsoft, LLC, Micro Focus Software, Inc., NICUSA, Inc., Google, LLC, Okta, Inc., RiskSense, Inc., Salesforce, Inc., ServiceNow, Inc., Splunk, Inc., and Zayo Group, LLC for alignment with the State of Illinois enterprise information system security policies. *(CC9.2.C)* The Department's baseline controls are utilized to evaluate subservice organizations' SOC reports to ensure compliance with the State of Illinois enterprise information system security policies. The Department's baseline controls include the following: access control, awareness and training, system and information integrity, malicious code protection, contingency planning, configuration management, risk assessment, incident response, security assessment and authorization.

Written review of subservice organization controls and exceptions noted in the SOC reports are presented to the system business owner for their review. Complementary User Entity Controls are also documented and provided to the system business owner for them to provide attestation of compliance. Artifacts to support the system business owner's affirmation are collected. If follow-up is needed to address identified weaknesses in attestation form, quarterly follow-up with system business owner is conducted.

In addition, the Department's project management team conducts daily meetings with Splunk, Inc., weekly meetings to ensure compliance with contractual requirement with NICUSA, Inc., Google, LLC (starting July 9th, 2020), Salesforce, Inc. (starting September 15th 2020), ServiceNow, Inc. (with more frequency if requested), Mircro Focus (starting August 17, 2020 with more frequency if requested) and Okta, Inc. (starting September 22, 2020). Meetings with

BMC Software, Inc. (starting on October 19, 2020) and Docusign, Inc. are scheduled every two weeks, while meeting with RiskSense, Inc. is scheduled quarterly (starting January 2021). A monthly meeting is held with Microsoft, LLC. The Department communicates with Zayo Group, LLC management regarding existing services as stated in the contracts. (*CC9.2.A*)

The subservice providers' contracts require them to contact the Department in the event of a security incident or information breach which impacts the State's data. (*CC2.3.D, CC9.2.D*)

The Department annually monitors the DCMS managed CCF and Communications Building to ensure appropriate physical and environmental controls are in place. (*CC9.2.B*) The Department reviews the CCF and Communications Building related contracts and validates deliverables with a checklist and walkthrough to ensure contractual compliance. Identified weaknesses and recommendations are provided to the Department's Chief of Enterprise Infrastructure and DCMS facility manager for corrective action responses. Corrective action items are followed up with the business owners via meetings and emails.

Description of the Controls Relevant to the Availability Trust Services Category

Network

The Department has implemented redundancy in the Data Center LANs and at agency locations where technically, fiscally, and operationally feasible. (*CC9.1.C, A1.2.V*) Additionally, device configurations are saved on a network management server, which verifies device configuration revisions daily, and new configurations are backed up when detected. (*A1.2.A*) Configurations saved on the network management server are backed up daily to the CCF and the Alternate Data Center (ADC) through the midrange backup system. (*A1.2.B*)

Mainframe

The Department is responsible for the scheduling and monitoring of the backup process except for the agency database data and applications. Agencies are responsible for scheduling the backups of their applications and database data. Agencies are also responsible for informing the Department of their business needs. Data on mainframe systems are backed up daily and weekly utilizing [redacted] (*A1.2.C*) The Department utilizes [redacted] to schedule and verify the completion of the backups. (*A1.2.D*)

The Department has implemented mainframe backup procedures to assist staff in the event of failures. (*A1.1.I*)

Daily, the Department's Storage staff review the output of the daily backup jobs for any failures. In the event of a mainframe daily backup job failure, the Department's Operations Center staff records the incident in the Shift Report. (*A1.2.E*) The next working day, the Department's Storage staff review the Shift Report to identify the problem, correct and resubmit the failed portion of the backup job.

The Department's Storage staff review the output of the weekly backup jobs for success or failure. The failure is researched and corrected, and then the failed portion of the backup job is resubmitted for completion. (*A1.2.F*)

Data replication is performed between the CCF and the ADC. Mainframe data replication occurs every [redacted] between the CCF and the ADC [redacted]. The monitoring software sends the Enterprise Storage and Backup group an alert if the data is out of sync for more than 24 hours. (*A1.2.G*) If there is an issue, a Remedy ticket is submitted to track the Enterprise Storage and Backup group's progress on resolution of the issue.

The [redacted] Replicated Status log keeps a log of replication between the two [redacted] and tracks library replication outcomes for [redacted] replication activity. (*A1.2.H*) These logs document the status of the replicated Data Domain pool and the time of the last sync and are maintained for seven days. The Storage staff reviews and corrects any issues.

Midrange

[redacted] are used to back up the midrange environment. (*A1.2.I*) [redacted] is used to monitor and report on midrange backups. (*A1.1.D*) Midrange server backups are performed daily or weekly and are either incremental or full. (*A1.2.J*) [redacted] automatically generate daily reports indicating the backup status of scheduled jobs from the prior day. These daily reports are emailed to the Enterprise Storage and Backup group who then investigates the cause of failures and works to resolve the problem. (*A1.2.K*)

Backed up server data is written to a Data Domain storage system and then replicated to another Data Domain storage system at the ADC. The Data Domain storage systems generate a daily status report which is emailed to the Enterprise Storage and Backup group. (*A1.2.L*) The Data Domain storage systems also send email alerts to the Enterprise Storage and Backup group when issues arise that may need additional attention. (*A1.2.M*) The Enterprise Storage and Backup group investigate the issue until a satisfactory conclusion is reached. The Data Domain systems automatically alert vendor support in the event of hardware or system failures. (*A1.2.N*)

The Data Domain storage systems are also a target for SQL, DB2, and Oracle backups. The database backups are written to the Data Domain storage systems via Common Internet File System or Network File System and then replicated to the ADC. (*A1.2.O*) It is the responsibility of the database administrators to perform and monitor the success of the database backups.

A [redacted] goes through the production SQL servers and creates a report with the latest backup date and it is sent to the SQL team daily. The SQL team reviews it and follows up for any failures. (*A1.2.P*) The SQL team also gets alerts from the SQL servers when backup jobs fail. (*A1.2.Q*) Additionally, the SQL team receives alerts from the [redacted] monitoring software if a database has missed a backup. (*A1.2.R*)

Any data, including, but not limited to SQL, Access, DB2 databases, user shared documents and user profiles are located on tier 2 storage device via the Network File System or the Service Message Block shares. The Enterprise Storage and Backup group has policies on the [redacted] that take daily snapshots of all shares which are then retained up to 60 days. (*A1.2.S*) The tier 2 storage also has daily synchronization with the ADC to another [redacted] storage system. The [redacted] generates a daily report showing successful and failed synchronization attempts with the ADC. (*A1.2.T*) Enterprise Storage and Backup group investigate failed synchronization attempts until a satisfactory conclusion is reached. The [redacted] has a call home feature that notifies vendor support. For critical issues, the [redacted] call home feature additionally notifies the Enterprise Storage and Backup group. (*A1.2.U*)

Mainframe

The mainframe environment is monitored through the z/OS systems console for errors and issues. (*CC7.2.H*)The Operations Center staff continuously monitors the system console.

Mainframe system performance and capacity is monitored by System Software programming personnel, via Resource Measurement Facility reports which are run daily and monthly. (*CC7.2.I*) Additionally, performance and capacity monitoring are documented via internal memorandum distributed via email to Enterprise Infrastructure management monthly. (*A1.1.E)*

The Department has implemented system options to protect resources and data. The System Management Facility records operating system activities. The System Coordinator runs a System Management Facility violation report weekly for review and signs off on the report after resolving any unusual violations. (*CC7.3.C*)

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

Midrange

Midrange availability is monitored by the Operations Command Center via the [redacted] system. (*A1.1.F*) Command Center technicians notify System and/or Storage technicians of [redacted]lerts.

Structured Query Language (SQL) database servers use the [redacted] tool set for additional monitoring. The [redacted] system alerts have been set up to generate emails to SQL support staff. (*A1.1.G*) The SQL support staff use the [redacted] tools to help trouble shoot SQL issues.

The Active Directory Domain Controllers use [redacted] for additional monitoring. [redacted] alerts have been set up to email alerts to AD support staff. (*A1.1.H*) The AD staff uses [redacted] to help trouble shoot AD issues.

Data Storage

Data Storage performance and capacity are monitored using vendor specific toolsets. *(A1.1.A*) When there is an equipment outage or performance issues, Data Storage technicians contact the equipment or software vendor. Automated alerts are sent via email to Data Storage technicians and management when capacity is reached or exceeds 80%. (*A1.1.B*) Midrange data backups are monitored by [redacted]t. (*A1.1.C*)

Recovery

A Business Impact Analysis (BIA) has been completed to provide an understanding of the Department's critical business functions and the IT tools and systems utilized by those functions, along with the business need for recovery priorities, along with determining the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

The Resiliency Planning Model outlines the adoption of the NIST 800-34 layered approach in contingency planning for the various services, systems, and infrastructure provided and supported by the Department. The Recovery Activation and Response plan outlines roles and responsibilities and the transition of efforts and teams as incident response moves into recovery. The Recovery Activation and Response Plan is reviewed for accuracy annually and after each effort supporting incident responses. (*CC9.1.A*)

Disaster recovery tests are performed annually via one of the following methods of either tabletop simulations, walk-throughs of plans, proof of concept testing, or functional exercises. (*CC9.1.B, A1.3.A*)

During the fiscal year the Department conducted testing involving the mainframe and critical infrastructure plans and shared service system contingency plans. Testing of the State of Illinois Cyber Disruption Plan was also conducted in partnership with the Illinois Emergency Management Agency (IEMA), Illinois State Police (ISP), Illinois National Guard (ING), and Statewide Terrorism and Intelligence Center (STIC).

Complementary Subservice Organization Controls

The Department's controls related to the IT hosting services cover only a portion of the overall control environment required to provide reasonable assurance that the service commitments and system requirements were achieved. It is not feasible that the service commitments and system requirements can be achieved solely by the Department's controls. The complementary subservice organization controls in the table below are expected to be implemented and operating effectively:

Number	Complementary Subservice Organization Control ("CSOC")	Applicable Criteria
1.	Controls are implemented to provide IT managed services which are performed in accordance with contracts.	CC9.2
2.	Controls are implemented to provide assurance that access to networks and applications is approved, reviewed periodically, and access is terminated timely.	CC6.2
3.	Controls are implemented to provide reasonable assurance that only authorized personnel are able to make changes to network and applications.	CC6.3
4.	Controls are implemented to provide reasonable assurance that updates to networks and applications are documented, approved, and tested prior to implementation.	CC8.1
5.	Control are implemented to provide adequate security around the network and application operations.	CC6.6
6.	Controls are implemented to address incidents that are identified, tracked, resolved and closed in a timely manner.	CC6.8

User Entity Responsibilities

The Department's system is designed with the assumption that certain responsibilities fall to the users of the system. The procedures listed below are the responsibility of users of the system. These controls are expected to be in operation at user entities to complement the Department's controls.

Number	User Entity Responsibilities
1.	Controls are implemented to ensure an authorized ATSRs submits an approved Remedy service request for the creation, modification, and termination of user access.
2.	Controls are implemented to ensure the proxy agency reviews the appropriateness of their security software accounts and respond to the Security Software Coordinator or designee.
3.	Control are implemented to ensure the agency reviews AD accounts that have been dormant for 60 or more days and take appropriate actions to keep accounts active.
4.	Controls are implemented to ensure the agency is scheduling the backups of their applications and database data.

5.	Controls are implemented to ensure the agency notifies the Department of actual or suspected information security breaches, compromised accounts, or unauthorized access.

The list of user-organization responsibilities presented above do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations.

SECTION IV

TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, TESTS OF CONTROLS AND RESULTS OF TESTS

Information Provided by the Independent Service Auditor

This report is intended to provide information to the management of the Department, user entities of the Department's IT hosting services, and prospective user entities, independent auditors and practitioners providing services to those entities, who have a sufficient understanding to consider it, along with other information including information about the controls implemented by the user entity. This report is intended to provide information about the suitability of the design and operating effectiveness of the controls implemented to achieve the service commitments and system requirements based on the criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*, throughout the period July 1, 2020 through June 30, 2021.

Although the applicable trust services criteria and related controls are presented in this section, they are an integral part of the Department' description of its IT hosting services throughout the period July 1, 2020 through June 30, 2021.

The examination was performed in accordance with attestation standards established by the American Institute of Certified Public Accountants, Statement on Standards for Attestation Engagements ("SSAE") 18, specifically AT-C sections 105 and 205, the guidance contained in the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy* and the standards applicable to attestation engagements contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. It is each user entity's responsibility to evaluate this information in relation to the internal control structure in place at each user entity in order to assess the total internal control structure. If an effective internal control structure is not in place at user entities, the Department's controls may not compensate for such weaknesses.

This description is intended to focus on the Department's controls surrounding the IT hosting services throughout the period July 1, 2020 through June 30, 2021; it does not encompass all aspects of the services provided or controls performed by the Department. Unique processes or control situations not described in the report are outside the scope of this report.

Tests of Controls

Our examination of the description of the service organization's IT hosting services and the suitability of the design and operating effectiveness of the controls to achieve the related service commitments and system requirements based on the services criteria stated in the description involved performing procedures to obtain evidence about the presentation of the description of the system in accordance with the description criteria and the suitability of the design and operating effectiveness of those controls to achieve the related service commitments and system requirements based on the services criteria stated in the description. Our procedures included assessing the risks that the description is not presented in accordance with the description criteria and that the controls were not suitably designed or operating effectively to achieve the related service commitments and system requirements based on the services stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related service commitments and system requirements based on the applicable trust services criteria stated in the description were achieved throughout the period July 1, 2020 through June 30, 2021.

Our tests of controls were designed to cover a representative number of activities throughout the period July 1, 2020 through June 30, 2021, for each of the controls listed in Section IV, which are designed to achieve the related service commitments and system requirements based on the applicable trust services criteria. In selecting particular tests of controls, we considered: (a) the nature of the controls being tested, (b) the types and competence of available evidential matter, (c) the criteria to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

The Office of the Auditor General'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 user locations or other controls which were not documented as tested under each control criteria listed in Section IV. The description of the Office of the Auditor General'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 Office of the Auditor General and should be considered information provided by the Office of the Auditor General.

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

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

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

Information Provided by the Department

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

Criterial Related to the Security (Common Criteria) Category

Criteria Number	Trust Services Criteria	Control Number	Controls Specified by the Department	Tests of Controls Performed by the Office of the Auditor General	Results of Tests
	Common Criteria Related to Control Environment				
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	CC1.1.A	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.	Reviewed 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 to determine the hiring practices.	No deviations noted.
		CC1.1.B	New employee and Personal Service Contractors (PSC) must pass applicable background checks prior to being offered employment.	Selected a sample of new employees and PSCs to determine if applicable background checks were performed prior to employment offer.	No deviations noted.
		CC1.1.C	Newly-hired employees are provided the DCMS Policy Manual during New Employee Orientation. They are required to sign an acknowledgment form stating the individual is bound to act in accordance with the DCMS Policy Manual and all updates provided or be subject to discipline, up to and including discharge.	Selected a sample of new employees to determine if the new employee signed the acknowledgment form.	No deviations noted.
		CC1.1.D	Newly-hired PSCs are governed by the terms, conditions, and duties outlined in their legally-binding contract.	Selected a sample of newly hired PSCs to determine if the contracts detailed the terms, conditions, and duties of the PSC.	No deviations noted.
		CC1.1.E	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."	Selected a sample of PSC contracts to determine if the contracts required the PSC to comply with the Department's policies and procedures.	No deviations noted.
		CC1.1.F	Newly-hired employees and PSCs are required to complete an acknowledgement of participation form for each of the following required trainings within 30 days of hire: Harassment and Discrimination Prevention Training, Illinois Department of Revenue, Information Safeguarding Training, Ethics Training, and Security Awareness Training.	Selected a sample of new employees and PSCs to determine if the new employee and PSC completed the Acknowledge of Participation for the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training, and Security Awareness Training within 30 days of hiring.	No deviations noted.
		CC1.1.G	Annually, employees and PSCs are required to complete the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training Program for State of Illinois Employees and Appointees, and Security Awareness Training via paper or OneNet and complete the acknowledgement of participation.	Reviewed the annual training report for employees and PSCs to determine if they had completed the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training Program for State of Illinois Employees and Appointees, and Security Awareness Training and completed the acknowledgement of participation annually.	1 of 801 employees and PSCs did not complete the Ethics Training Program.

					4 of 796 employees and PSCs completed the Security Awareness Training 6 to 62 days late.
					1 of 801 employees and PSCs completed the Ethics training Program 5 days late.
		CC1.1.H	Newly-hired employees and PSCs are provided the Acceptable Use Policy and are required to complete the Acceptable Use Policy Certification stating the individual will comply with the State's policies and regulation. This Acceptable Use Policy Certification is completed once, at the time of hire.	Selected a sample of new employees and PSCs to determine if the new employee and PSC had completed the Acceptable Use Policy Certification upon hiring.	No deviations noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC1.2.A	The Audit Committee assists the Secretary in fulfilling their responsibilities for effectively and efficiently managing and maintaining an effective system of internal control.	Reviewed the Internal Audit Committee charter to determine their responsibilities.	No deviations noted.
		CC1.2.B	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.	Reviewed the Internal Audit Committee charter and Internal Audit Committee meeting minutes to determine if they assisted the Secretary in oversight and reporting responsibilities.	No deviations noted.
		CC1.2.C	The Committee is to meet four times per calendar year, with the authority to convene more frequently if requested.	Reviewed Internal Audit Committee meeting minutes to determine if they met four times throughout the year.	No deviations noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC1.3.A	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.	Reviewed the organizational chart to determine if the organizational chart documented the Department's organizational structure, reporting lines, authorities, responsibilities and had been reviewed annually.	No deviations noted.
		CC1.3.B	Each State employment position (job protected or at will) is identified on the organizational chart.	Reviewed the organizational chart to determine if each State employment position was identified.	No deviations noted.
		CC1.3.C	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).	Selected a sample of job descriptions to determine if the job description documented the employee's duties, responsibilities, qualifications, minimum acceptable competency education requirements, and experience levels.	No deviations noted.
		CC1.3.D	Vendor contractors are hired based on contract requirements which follow Illinois procurement regulations.	Selected a sample of vendor contractors to determine if vendor contract was hired based on contract requirements.	No deviations noted.

CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC1.4.A	New employee and Personal Service Contractors (PSC) must pass applicable background checks prior to being offered employment.	Selected a sample of new employees and PSCs to determine if applicable background checks were performed prior to employment offer.	No deviations noted.
		CC1.4.B	Newly-hired employees and PSCs are required to complete an acknowledgement of participation form for each of the following required trainings within 30 days of hire: Harassment and Discrimination Prevention Training, Illinois Department of Revenue, Information Safeguarding Training, Ethics Training, and Security Awareness Training.	Selected a sample of new employees and PSCs to determine if the new employee and PSC completed the Acknowledge of Participation for the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training, and Security Awareness Training within 30 days of hiring.	No deviations noted.
		CC1.4.C	Annually, employees and PSCs are required to complete the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training Program for State of Illinois Employees and Appointees, and Security Awareness Training via paper or OneNet and complete the acknowledgement of participation.	Reviewed the annual training report for employees and PSCs to determine if they had completed the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training Program for State of Illinois Employees and Appointees, and Security Awareness Training and completed the acknowledgement of participation annually.	1 of 801 employees and PSCs did not complete the Ethics Training Program.
					4 of 796 employees and PSCs completed the Security Awareness Training 6 to 62 days late.
					1 of 801 employees and PSCs completed the Ethics training Program 5 days late.
		CC1.4.D	Each State employment position (job protected or at will) is identified on the organizational chart.	Reviewed the organizational chart to determine if each State employment position was identified.	No deviations noted.
		CC1.4.E	Vendor contractors are hired based on contract requirements which follow Illinois procurement regulations.	Selected a sample of vendor contractors to determine if vendor contractors were hired based on contract requirements.	No deviations noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC1.5.A	Performance evaluations are completed. Additionally, for employees' service probationary periods, performance evaluations are completed at varying intervals.	Selected a sample of employees to determine if performance evaluations were completed at the proper interval.	28 of 32 four month probationary evaluations selected were completed 1 to 203 days late.
					21 of 28 three and six month probationary evaluations selected were completed 1 to 212 days late.
					20 of 60 annual evaluations selected were completed 3 to 220 days late.

		CC1.5.B	Newly-hired employees and PSCs are required to complete an acknowledgement of participation form for each of the following required trainings within 30 days of hire: Harassment and Discrimination Prevention Training, Illinois Department of Revenue, Information Safeguarding Training, Ethics Training, and Security Awareness Training.	Selected a sample of new employees and PSCs to determine if the new employee and PSC completed the Acknowledge of Participation for the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Orientation for State of Illinois Employees, and Security Awareness Training within 30 days of hiring.	No deviations noted.
		CC1.5.C	Annually, employees and PSCs are required to complete the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training Program for State of Illinois Employees and Appointees, and Security Awareness Training via paper or OneNet and complete the acknowledgement of participation.	Reviewed the annual training report for employees and PSCs to determine if they had completed the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training Program for State of Illinois Employees and Appointees, and Security Awareness Training and completed the acknowledgement of participation annually.	1 of 801 employees and PSCs did not complete the Ethics Training Program. 4 of 796 employees and PSCs completed the Security Awareness Training 6 to 62 days late. 1 of 801 employees and PSCs completed the Ethics training Program 5 days late.
		CC1.5.D	Newly-hired employees and PSCs are provided the Acceptable Use Policy and are required to complete the Acceptable Use Policy Certification stating the individual will comply with the State’s policies and regulation. This Acceptable Use Policy Certification is completed once, upon hiring.	Selected a sample of new employees and PSCs to determine if the new employee and PSC had completed the Acceptable Use Policy Certification upon hiring.	No deviations noted.

Criterial Related to the Security (Common Criteria) Category					
Criteria Number	**Trust Services Criteria**	**Control Number**	**Controls Specified by the Department**	**Tests of Controls Performed by the Office of the Auditor General**	**Results of Tests**
	Common Criteria Related to Communication and Information				
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC2.1.A	The Department has established a Risk Management Program (RMP) to offer guidelines on how to reduce risk across the enterprise.	Reviewed the RMP to determine if the RMP provided guidelines to reduce risk across the enterprise.	No deviations noted.
		CC2.1.B	The Department has implemented various policies and procedures relevant to security.	Reviewed the various security polices and procedures to determine the security posture.	No deviations noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC2.2.A	The Department's website delivers information to client agencies and to Department staff covering: Initiatives and accomplishments, Policies, Service Catalog (which describes services available to user agencies), and Instructions on how to order services and products as well as how to report operational problems.	Reviewed the Department's website to determine information provided to client agencies and Department staff.	No deviations noted.
		CC2.2.B	The website also provides links to the DoIT Digest content, which informs the reader of new initiatives, business applications, ongoing projects, administrative information, and Departmental news.	Reviewed the Department's website to determine if the DoIT Digest had been posted.	No deviations noted.
		CC2.2.C	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.	Reviewed the Department's website, Employee Portal, and emails to determine if employees were informed.	No deviations noted.
		CC2.2.D	A Remote Work webpage was published on the Department's website to provide guidelines and additional resources to support employees working remotely.	Reviewed the Remote Work webpage to determine if the webpage provided guidelines and resources to employees working remotely.	No deviations noted.
		CC2.2.E	The Department's Division of Information Security is responsible for ensuring Department's compliance with enterprise information security policies.	Observed various tools utilized for ensuring compliance with enterprise information security policies.	No deviations noted.

CC2.2.F	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.	Reviewed policies and procedures to determine if the policies and procedures had been reviewed by the GRC Group every three years or when changes were noted.	The Department did not have a policy or procedure documenting the frequency in which policies and procedures published on its website were to be reviewed.
CC2.2.G	Newly-hired employees are provided the DCMS Policy Manual during New Employee Orientation. They are required to sign an acknowledgment form stating the individual is bound to act in accordance with the DCMS Policy Manual and all updates provided or be subject to discipline, up to and including discharge.	Selected a sample of new employees to determine if the new employee complied the acknowledgment form.	No deviations noted.
CC2.2.H	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."	Selected a sample of PSC contracts to determine if the contracts required the PSC to comply with the Department's policies and procedures.	No deviations noted.
CC2.2.I	Newly-hired employees and PSCs are required to complete an acknowledgement of participation form for each of the following required trainings within 30 days of hire: Harassment and Discrimination Prevention Training, Illinois Department of Revenue, Information Safeguarding Training, Ethics Training, and Security Awareness Training.	Selected a sample of new employees and PSCs to determine if the new employee and PSC completed the Acknowledge of Participation for the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training, and Security Awareness Training within 30 days of hiring.	No deviations noted.
CC2.2.J	Annually, employees and PSCs are required to complete the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training Program for State of Illinois Employees and Appointees, and Security Awareness Training via paper or OneNet and complete the acknowledgement of participation.	Reviewed the annual training report for employees and PSCs to determine if they had completed the Harassment and Discrimination Prevention Training, Information Safeguarding Training, Ethics Training Program for State of Illinois Employees and Appointees, and Security Awareness Training and completed the acknowledgement of participation annually.	1 of 801 employees and PSCs did not complete the Ethics Training Program. 4 of 796 employees and PSCs completed the Security Awareness Training 6 to 62 days late. 1 of 801 employees and PSCs completed the Ethics training Program 5 days late.

		CC2.2.K	Newly-hired employees and PSCs are provided the Acceptable Use Policy and are required to complete the Acceptable Use Policy Certification stating the individual will comply with the State's policies and regulation. This Acceptable Use Policy Certification is completed once, at the time of hiring.	Selected a sample of new employees and PSCs to determine if the new employee and PSC had completed the Acceptable Use Policy Certification upon hiring.	No deviations noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC2.3.A	Group CIOs discuss with agency leadership personnel relevant subjects that may include significant events, service issues, improvements, processes, and strategic goals.	Reviewed Group CIOs' communications to determine if Group CIOs were communicating with agencies.	No deviations noted.
		CC2.3.B	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.	Reviewed CIO Council meeting agendas to determine if agency CIOs were informed.	No deviations noted.
		CC2.3.C	DoIT Daily is a forum to share high-level and high-risk operational issues with a team equipped to discuss steps for resolution.	Reviewed DoIT Daily agendas to determine if high-level and high-risk operational issues were discussed.	No deviations noted.
		CC2.3.D	The subservice providers' contracts require them to contact the Department in the event of a security incident or information breach which impacts the State's data.	Reviewed subservice providers' contracts to determine if the contracts require the subservice providers to contact the Department in the event of a security incident or information breach.	2 of 12 subservice providers' contracts did not contain the requirement for the subservice provider to contact the Department in the event of a security incident or information breach.
		CC2.3.E	The Department's website delivers information to client agencies and to Department staff covering: Initiatives and accomplishments, Policies, Service Catalog (which describes services available to user agencies), and Instructions on how to order services and products as well as how to report operational problems.	Reviewed the Department's website to determine information provided to client agencies and Department staff.	No deviations noted.
		CC2.3.F	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."	Selected a sample of PSC contracts to determine if the contracts required the PSC to comply with the Department's policies and procedures.	No deviations noted.

Criterial Related to the Security (Common Criteria) Category					
Criteria Number	**Trust Services Criteria**	**Control Number**	**Controls Specified by the Department**	**Tests of Controls Performed by the Office of the Auditor General**	**Results of Tests**
	Common Criteria Related to Risk Assessment				
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC3.1.A	The Department receives threat, vulnerability, and incident intelligence from multiple sources, including the MS-ISAC and the Illinois Statewide Terrorism and Intelligence Center.	Reviewed notifications the Department received from various sources to determine if threat, vulnerability, and incident intelligence was communicated.	No deviations noted.
		CC3.1.B	The Department conducts risk assessment for each agency based on the RMP.	Selected a sample of agencies to determine if risk assessments had been conducted based on RMP.	5 of 8 agencies' risk assessments selected were not conducted.
		CC3.1.C	An Enterprise Information Security Risk Assessment Policy has been published on the Department’s website.	Reviewed the Department's website to determine if the Enterprise Information Security Risk Assessment Policy had been published.	No deviations noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CC3.2.A	Risks from potential and newly discovered vulnerabilities are assessed through interaction with the Department’s security staff and vendor subscription services.	Reviewed correspondence between the Department and vendors to determine if risks from potential and newly discovered vulnerabilities were assessed.	No deviations noted.
		CC3.2.B	Risks and mitigation plans are captured and tracked in the Department's risk register.	Reviewed the Department's risk register to determine if risks and mitigation plans were captured and tracked.	No deviations noted.
		CC3.2.C	The Department conducts quarterly mitigation plan follow-up review to keep track of progress until mitigation plans are completed.	Reviewed quarterly correspondence with agencies and the risk register to determine if quarterly mitigation plan follow-up reviews were conducted.	No deviations noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC3.3.A	The RMP includes several components that leverage the National Institute of Standards and Technology (NIST) framework as a foundation. NIST provides a comprehensive series of technical and non-technical (i.e., administrative) controls that act as safeguards and countermeasures prescribed to protect the confidentiality, integrity, and availability of data and information systems.	Reviewed the RMP to determine if the RMP documented technical and non-technical controls to protect the confidentiality, integrity, and availability of data and information systems.	No deviations noted.

CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	CC3.4.A	The Department receives threat, vulnerability, and incident intelligence from multiple sources, including the MS-ISAC and the Illinois Statewide Terrorism and Intelligence Center.	Reviewed correspondence from multiple sources to determine if threat, vulnerability, and incident intelligence was received.	No deviations noted.
		CC3.4.B	The Department conducts quarterly mitigation plan follow-up review to keep track of progress until mitigation plans are completed.	Reviewed quarterly correspondence with agencies and the risk register to determine if quarterly mitigation plan follow-up reviews were conducted.	No deviations noted.
		CC3.4.C	Risks from potential and newly discovered vulnerabilities are assessed through interaction with the Department's security staff and vendor subscription services.	Reviewed correspondence between the Department and vendors to determine if risks from potential and newly discovered vulnerabilities were assessed.	No deviations noted.

Criterial Related to the Security (Common Criteria) Category					
Criteria Number	Trust Services Criteria	Control Number	Controls Specified by the Department	Tests of Controls Performed by the Office of the Auditor General	Results of Tests
	Common Criteria Related to Monitoring Activities				
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC4.1.A	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.	Reviewed quarterly meeting documentation to determine if performance metrics were discussed.	No deviations noted.
		CC4.1.B	Internal Audit provides the Department independent, objective assurance and consulting services by performing risk assessment exercises to create the annual audit plan.	Reviewed the annual audit plan to determine if its creation was based on risk assessments.	No deviations noted.
		CC4.1.C	Internal Audit performs system pre-implementation reviews to evaluate system controls.	Reviewed system pre-implementation review reports to determine if system controls were evaluated.	No deviations noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	CC4.2.A	Critical and high level Remedy tickets that did not meet the performance metrics are discussed for potential service improvement going forward.	Reviewed quarterly meeting documentation to determine if critical and high level Remedy tickets were discussed.	No deviations noted.
		CC4.2.B	Service level metrics showing the Department's customer service performance are posted on the Department's website.	Reviewed the Department's website to determine if service level metrics were posted.	No deviations noted.
		CC4.2.C	External and internal audits' results are communicated to senior management, and management response is documented.	Reviewed external and internal audits reports to determine if audit reports were communicated to senior management and management responded.	No deviations noted.
		CC4.2.D	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.	Reviewed the annual report to determine if the report detailed significant findings and status of the recommended changes.	No deviations noted.

Criterial Related to the Security (Common Criteria) Category

Criteria Number	Trust Services Criteria	Control Number	Controls Specified by the Department	Tests of Controls Performed by the Office of the Auditor General	Results of Tests
	Common Criteria Related to Control Activities				
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC5.1.A	The Department receives threat, vulnerability, and incident intelligence from multiple sources, including the MS-ISAC and the Illinois Statewide Terrorism and Intelligence Center.	Reviewed notifications the Department received from various sources to determine if threats, vulnerabilities, and incident intelligences were communicated.	No deviations noted.
		CC5.1.B	The Department conducts risk assessment for each agency based on the RMP.	Selected a sample of agencies to determine if risk assessments had been conducted based on RMP.	5 of 8 agencies' risk assessments selected were not conducted.
		CC5.1.C	Risks from potential and newly discovered vulnerabilities are assessed through interaction with the Department's security staff and vendor subscription services	Reviewed correspondence between the Department and vendors to determine if risks from potential and newly discovered vulnerabilities were assessed.	No deviations noted.
		CC5.1.D	Risks and mitigation plans are captured and tracked in the Department's risk register.	Reviewed the Department's risk register to determine if risks and mitigation plans were captured and tracked.	No deviations noted.
		CC5.1.E	The Department conducts quarterly mitigation plan follow-up review to keep track of progress until mitigation plans are completed.	Reviewed quarterly correspondence with agencies and the risk register to determine if quarterly mitigation plan follow-up reviews were conducted.	No deviations noted.
		CC5.1.F	Managerial, operational and technical changes are discussed during the risk assessment process.	Reviewed the RMP to determine if managerial, operational, and technical changes were part of the risk assessment process.	No deviations noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC5.2.A	The Department selects logical and physical security, change management, and incident monitoring control activities to manage technology infrastructure and security access risks identified during the annual risk assessment process.	Reviewed logical and physical security, change management, and incident monitoring controls to determine if identified risks were managed.	No deviations noted.

CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CC5.3.A	The Department’s website delivers information to client agencies and to Department staff covering: Initiatives and accomplishments, Policies, Service Catalog (which describes services available to user agencies), and Instructions on how to order services and products as well as how to report operational problems.	Reviewed the Department's website to determine if information was provided to client agencies and Department staff.	No deviations noted.
		CC5.3.B	A Remote Work webpage was published on the Department’s website to provide guidelines and additional resources to support employees working remotely.	Reviewed the Remote Work webpage to determine if the webpage provided guidelines and resources to employees working remotely.	No deviations noted.
		CC5.3.C	Managerial, operational and technical changes are discussed during the risk assessment process.	Reviewed the RMP to determine if managerial, operational, and technical changes were part of the risk assessment process.	No deviations noted.
		CC5.3.D	The Department has published its security related policies and procedures on its website.	Reviewed the Department's website to determine if security related policies and procedures had been published.	No deviations noted.

Criterial Related to the Security (Common Criteria) Category					
Criteria Number	**Trust Services Criteria**	**Control Number**	**Controls Specified by the Department**	**Tests of Controls Performed by the Office of the Auditor General**	**Results of Tests**
	Common Criteria Related to Logical and Physical Access				
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1.A	In order to access the State's information technology environment, an Active Directory ID and password are required.	Observed an AD ID and password were required to gain access to the environment.	No deviations noted.
		CC6.1.B	Password security parameters have been established and configured to ensure access to resources is appropriate: • Minimum password length; • Password complexity; • Password history; • Minimum password age; and • Number of invalid login attempts.	Reviewed the password parameters to determine whether parameters had been established.	No deviations noted.
		CC6.1.C	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.
		CC6.1.D	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.
		CC6.1.E	The security software requires an established ID and password to verify the identity of the individual.	Observed security software ID and password were required to access the mainframe environment.	No deviations noted.
		CC6.1.F	The primary means of defining an individual's level of access is the security software profile.	Observed a security software profile to determine if the profile defined the level of access.	No deviations noted.
		CC6.1.G	Password security parameters have been established and configured to ensure access to mainframe resources is appropriate: • Minimum password length; • Password complexity; • Password history; • Minimum password age; and • Number of invalid login attempts.	Reviewed the systems options to determine if password standards had been established.	No deviations noted.
		CC6.1.H	The security software passwords are maintained as encrypted values within the system security database.	Reviewed the system options to determine if security software passwords were maintained as encrypted values within the system security database.	No deviations noted.

		CC6.1.I	In the event a user requires a reset of their mainframe password, they are required to either submit the request via email to the IT Service Desk or use the Department’s self-service option: DoIT Identity Management tool.	Reviewed the DoIT Identity Management Website to determine solution to reset passwords.	No deviations noted.
		CC6.1.J	In the event the Department is the agency’s proxy, a Remedy ticket is assigned to the Department’s Security Software Coordinator or the Department’s Security Software Administrator. Using information from the Remedy ticket, the Department’s Security Software Coordinator or the Security Software Administrator contacts the user to reset the password.	Observed the Security Software Coordinator reset the mainframe password upon receipt of a Remedy ticket.	No deviations noted.
		CC6.1.K	Detailed design and configuration standards and guides are maintained to ensure the integrity of the design, security and configuration of the network.	Reviewed the design and configuration standards and guides to determine if the standards and guides were maintained.	No deviations noted.
		CC6.1.L	A security banner also serves as a security awareness mechanism and is displayed at initial network connection warning of prosecution for unauthorized access.	Reviewed configurations to determine if a security banner was displayed upon initial connection to the network.	No deviations noted.
		CC6.1.M	Virtual Private Networks (VPN) provide controlled and trusted connections between devices when required for data traversing public networks including the Internet.	Reviewed VPN configurations to determine if security settings were configured to allow for secure remote connections.	No deviations noted.
		CC6.1.N	The Department’s Enterprise VPN Standard provides guidance when establishing a VPN connection.	Reviewed the Enterprise VPN Standard to determine if the Standards provided guidance on establishing VPN connections.	No deviations noted.
		CC6.1.O	When data travels across a public network, it is encrypted at the access router and while in transit across the public network until it reaches the distribution router and enters the private network.	Reviewed configurations to determine if data traversing the network was encrypted.	No deviations noted.
		CC6.1.P	ADFS and Okta SSO utilize the same Active Directory credentials, in addition to two-factor authentication.	Observed Okta and ADFS to determine if it utilized AD credentials and two-factor authentication.	No deviations noted.

CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC6.2.A	Access creation or modification to Department resources (users and administrators) requires the submission of a Remedy service request from a Remedy submitter or an authorized Agency Technology Service Requestor (ATSR).	Selected a sample of new employees and contractors to determine if an ATSR approved Remedy service request was submitted.	No deviations noted.
				Selected a sample of access modifications to determine if an ATSR approved Remedy service request was submitted.	The Department did not provide a population of access modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
		CC6.2.B	Revoking access to Department resources is initiated upon receipt of a Remedy service request or under special or emergency circumstances, network access is disabled at the instruction of the Department senior management.	Selected a sample of separated users to determine if network access was disabled.	2 of 27 selected separated employees' and contractors' access revocation documentation was not provided.
					The Department did not have a policy documenting the required timeframe for revocation of logical access upon termination.
		CC6.2.C	Once the Remedy service request is created, or Mainframe Request Form is submitted, the Department's Software Security Coordinator will receive the Remedy ticket, and follow the Security Software ID Creation procedures to create an account as specified.	Selected a sample of new security software accounts to determine if the Software Security Coordinator followed the Security Software ID Creation procedures to create an account.	5 of 35 new security software accounts selected were not approved by an ATSR.
					4 of 35 new security software accounts selected did not have an approved Remedy ticket or Mainframe Access Request Form.

				Selected a sample of modified security software accounts to determine if the Software Security Coordinator followed the Security Software ID Creation procedures to modify the account.	The Department did not provide a population of security software ID modifications. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
		CC6.2.D	Access to the operating system configurations is limited to system support staff.	Reviewed access rights to the mainframe operating system configurations to determine if access was limited to system support staff.	No deviations noted.
		CC6.2.E	Access with powerful privileges, high-level access and access to sensitive system functions is restricted to authorized personnel.	Reviewed access rights to powerful privileges, high-level access to sensitive system functions to determine if access was limited to authorized personnel.	No deviations noted.
		CC6.2.F	To request administrative account access, the Department access provisioning process is to be followed.	Selected a sample of new administrative accounts to determine if new administrative accounts followed the Department's access provisioning process.	The Department did not have a request for a new system administrator. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.

CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	CC6.3.A	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.
		CC6.3.B	The Department performs a monthly review of Illinois.gov Active Directory accounts and disables accounts which have been dormant for 60 days.	Selected a sample of monthly reviews to determine if dormant accounts were reviewed.	No deviations noted.
		CC6.3.C	Department staff and vendors with a business need to access or modify network devices are added to a designated Active Directory access group (for role based and least privileges) and setup with a two-factor authentication token.	Selected a sample of individuals with a business need to access or modify network devices to determine if staff and vendors were added to designated Active Directory access groups and set up with a two-factor authentication token.	1 of 20 network administrators did not require administrative rights to the environment.
		CC6.3.D	On an annual basis, the Department's Security Software Coordinator sends proxy agencies and the Department a listing of security software IDs assigned to their agency and the Department for review.	Reviewed the annual review of security software IDs to determine if the review had been conducted.	The Department did not conduct the Security Software Annual Reconciliation.
		CC6.3.E	On a monthly basis, the Department's Security Software Coordinator or designee runs a report documenting the Department and the proxy agencies' security software IDs which have not been utilized in the past 90-days; upon review, the IDs are revoked.	Selected a sample of monthly reports to determine if the IDs had been revoked.	No deviations noted.
		CC6.3.F	The Department's Security Software Coordinator or designee runs a weekly violation report which is reviewed for invalid and unauthorized access attempts of the Department and proxy agency security software IDs. The Department's Security Software Coordinator follows up with the review results as stated in the Security Violation Report Procedure. The Department's Security Software Coordinator or designee contacts the individual or their supervisor to determine the reason for the violation.	Selected a sample of weekly reports to determine if the Security Software Coordinator or designee had reviewed and followed up on invalid and unauthorized access attempts.	No deviations noted.
		CC6.3.G	Semi-monthly, the Department's Security Software Coordinator receives a separation report documenting the separations for the month. The Department's Security Software Coordinator or designee reviews the separation reports, noting separation of individuals from the Department and proxy agencies. If a separation is noted, the Security Software Coordinator will revoke the individual's security software ID.	Selected a sample of semi-monthly reports to determine if the Security Software Coordinator had reviewed and revoked individual accounts which had separated.	No deviations noted.
		CC6.3.H	Authentication servers control access through assignment of access right privileges (read only or update) based on Department-defined group profiles.	Reviewed configurations to determine if authentication servers controlled access.	No deviations noted.

		CC6.3.I	Access to MOVEit systems are reviewed and followed up on an annual basis by the Department’s Midrange Wintel Group.	Reviewed the annual review of access to MOVEit by the Department's Midrange Wintel Group.	No deviations noted.
		CC6.3.J	The System Coordinator and Mainframe manager review a high-level systems programmer user ID listing on an annual basis.	Reviewed the annual review of high-level system programmers by the System Coordinator and Mainframe manage.	No deviations noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives.	CC6.4.A	The CCF and the Communications Building are monitored 24x7x365 by security guards.	Observed security guards at the CCF and the Communications Building.	No deviations noted.
		CC6.4.B	The CCF and Communications Building are monitored by security cameras located at various interior and exterior points. The security cameras are monitored by the security guards.	Observed security cameras were located at interior and exterior points and were monitored by the security guards.	No deviations noted.
		CC6.4.C	The CCF and Communications Building maintain building access and perimeter monitoring.	Observed building access and perimeter monitoring controls.	No deviations noted.
		CC6.4.D	The interior and exterior of the CCF and Communications Building access are enforced by card key access.	Observed card key readers at interior and exterior points.	No deviations noted.
		CC6.4.E	To obtain a card key (badge) for access to the CCF and Communications Building, an ID Badge Request Form is submitted by an authorized individual to HR. In the event the individual requires access to the CCF secured area, additional authorization is required.	Selected a sample of new employees and contractors to determine if an authorized ID Badge Request Form was completed and if access to the CCF secured area was properly authorized.	3 of 26 new employee and contractor ID Badge Request Forms selected did not have all required fields properly completed.
		CC6.4.F	The Department’s HR enters the applicable access rights into the Velocity system (card key (badge) system), obtains valid proof of identity and a photo to obtain a card key (badge).	Selected a sample of new access requests to determine if a valid proof of identity and a photo were provided.	No deviations noted.
		CC6.4.G	In order for non-state employees to obtain a card key (badge) documentation of a clear background check, performed in the past five years, must be provided prior to initial badge issuance.	Selected a sample of access requests for new non-State employees to determine if a clear background check had been completed in the last five years and was provided prior to the initial badge issuance.	No deviations noted.

CC6.4.H	The card key (badge) access is revoked at the expiration date or upon official notice of separation or termination.	Selected a sample of terminations to determine if card key access was timely deactivated.	The Department did not provide documentation demonstrating the terminated individuals' access badge had been deactivated. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
CC6.4.I	The Department’s Midrange Wintel Manager or designee conducts monthly reviews of individuals who were granted access or had access removed in the prior month to the CCF secured area.	Selected a sample of monthly reviews to determine if the Midrange Wintel Manager had reviewed individuals who were granted access or had access removed in the prior month to the CCF secured area.	No deviations noted.
CC6.4.J	The Department’s Security team conducts quarterly access reviews of all individuals with access to the CCF (starting in December 2020), and Communication Building.	Selected a sample of quarterly access reviews to determine if the Security team had reviewed individuals' access to the CCF (starting in December 2020) and the Communication Building.	No deviations noted.
CC6.4.K	The Department’s Security team conducts monthly reviews of all individuals with access to the CCF secured area.	Selected a sample of monthly reviews to determine if the Security team conducted monthly reviews of individuals with access to the CCF secured area.	No deviations noted.
CC6.4.L	Visitors are required to provide identification and sign the visitor log in order to gain access to the CCF and Communications Building.	Observed visitors were required to sign the visitor's log and provide identification to gain access to the CCF and Communications Building.	No deviations noted.
CC6.4.M	The visitors are provided a visitor badge, with no access rights. The visitor is required to be escorted at all time.	Observed visitors were required to sign the visitor's log, provide identification, and be escorted.	No deviations noted.
CC6.4.N	In the event an individual does not have their card key (badge) readily available, the security guards may issue a temporary access card key (badge). The access rights, as documented in Velocity, are associated with the card key (badge).	Observed individuals were provided temporary access card keys with access rights as documented in Velocity.	No deviations noted.

		CC6.4.O	Temporary badges are issued to authorized vendors once identification has been validated.	Selected a sample of the Building Admittance Registers to determine if individuals were provided a temporary badge with appropriate access.	In the 30 Building Admittance Registers selected there were 7 individuals with 13 instances which were not provided a temporary badge with appropriate access.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	CC6.5.A	For voluntary separations of an employee or a contractor, an Employee Exit form and a Remedy service request are completed to initiate to ensure the removal of access and the retrieval of equipment.	Selected a sample of separated employees and contractors to determine if an Employee Exit form and Remedy service request had been completed.	2 of 27 terminated employees selected did not have a Remedy Service Request completed.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC6.6.A	The Department maintains network diagrams depicting common connectivity configurations. Network segmentation permits unrelated portions of the agencies' information system to be isolated from each other. Enterprise wide, agencies' traffic is segmented to be isolated from each other.	Reviewed network diagrams to determine connectivity configurations.	No deviations noted.
				Reviewed device configurations to determine if networks were segmented.	No deviations noted.
		CC6.6.B	Access level controls are applied through the use of Access Control Lists and Authentication Servers. Access Control Lists reside o[redacted]	Reviewed configurations to determine if ACLs restricted communications.	No deviations noted.
		CC6.6.C	Firewalls are in place and configured with denial rules.	Selected a sample of firewalls to determine if the firewalls were configured with denial rules.	No deviations noted.
		CC6.6.D	An intrusion detection system is in place to monitor for malicious and unauthorized activity.	Selected a sample of egress firewalls to determine if the egress firewalls were configured to monitor malicious and unauthorized activity.	No deviations noted.

		CC6.6.E	Virtual Private Networks (VPN) provide controlled and trusted connections between devices when required for data traversing public networks including the Internet.	Reviewed VPN configurations to determine if security settings were configured to allow for secure remote connections.	No deviations noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	CC6.7.A	The secure, encrypted transfer of mainframe data is achieved using the File Transfer Protocol Secure (FTPS).	Observed the file transfer protocol to determine if the mainframe data was secure and encrypted during transfer.	No deviations noted.
		CC6.7.B	The software MOVEit is used to transmit midrange data between servers and applications and provides email alerts for any failures to Department and agency support staff.	Reviewed the MOVEit software configurations to determine if MOVEit was used to transmit data between servers and applications and if email alerts were sent for failures to Department and agency support staff.	No deviations noted.
		CC6.7.C	Another option available to valid Illinois.gov users for the secure transmission of data is the file transfer utility 'FileT'.	Reviewed the FileT configurations to determine the security over the transmission of the data.	No deviations noted.
		CC6.7.D	This utility uses random key generation to access files stored on a server.	Reviewed file transfer protocol configurations to determine if random key generation was utilized.	No deviations noted.
		CC6.7.E	Files are automatically purged from the server after five days.	Reviewed filed transfer protocol configurations to determine if files were purged after five days.	No deviations noted.
		CC6.7.F	The sender must acknowledge a warning of unauthorized access message by clicking a box before transfer is allowed.	Observed the sender must acknowledge a warning of unauthorized access message.	No deviations noted.
		CC6.7.G	A valid Illinois.gov email address is required to use this utility for State resources; either as the recipient or the sender.	Observed a valid Illinois.gov address was required.	No deviations noted.
		CC6.7.H	WAN encryption technologies are utilized to protect data.	Reviewed configurations to determine if data traversing the network was encrypted.	No deviations noted.
		CC6.7.I	The email encryption technology is configured to utilize [redacted] by default, and user can specify that encryption be utilized.	Reviewed encryption technology configurations to determine if [redacted] was utilized.	No deviations noted.
		CC6.7.J	If encryption is inactive or was not installed as part of the device imaging process prior to deployment, EUC Image Management will assign the Remedy ticket to the Security Operations Center (SOC) who will enact a breach investigation that consists of steps outlined in their Security Incident Playbook.	Selected a sample of lost or stolen laptops in which encryption was not installed to determine if the SOC enacted a breach investigation as outlined in the Security Incident Playbook.	No deviations noted.

CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CC6.8.A	Self-monitoring network routers and switches record all events, notifies [redacted] and forwards to multiple logging servers. These servers use filters to automatically generate alerts when a network services' configured parameter or condition occurs.	Reviewed network routers and switches to determine if they were encoded with filters and if the Network Operations Center was reviewing and resolving alerts received.	No deviations noted.
		CC6.8.B	Distributed denial of service platform is utilized to monitor and mitigate network threats. Threats are reviewed and appropriate action is taken based on the individual threat.	Reviewed the distributed denial of services platform configurations and alerts to determine if threats were mitigated and reviewed.	No deviations noted.
		CC6.8.C	LAN Services network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to LAN Services Support staff and a console display alert when a predefined event occurs, or a threshold is reached. LAN Services Support staff follow up on these alerts and engage operational teams for resolution as necessary.	Reviewed software configurations to determine if emails and alerts were sent and LAN Services Support staff followed up on the alerts.	No deviations noted.
		CC6.8.D	The authentication server records failed login attempts to the network equipment.	Reviewed configurations to determine if failed login attempts were logged.	No deviations noted.
		CC6.8.E	WAN Services network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / or console display alert when a predefined event occurs, or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. The 24x7x365 Network Operation Center staff reviews each occurrence and engage operation teams for resolution.	Reviewed software configurations to determine if emails and alerts were sent to the 24x7x365 Network Operations Center when predefined events or thresholds were reached and the 24x7x365 Network Operations Center followed up on the alerts.	No deviations noted.
		CC6.8.F	WAN Services authentication server records failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to Network Design and Engineering staff to determine, on a case by case basis, if further action is required.	Reviewed configurations to determine if failed login attempts were logged and if an email notification was sent to Network Design and Engineering staff.	No deviations noted.

CC6.8.G	Backbone WAN Services network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / or console display alert when a predefined event occurs or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. Alerts are tracked in the Network monitoring system.	Reviewed software configurations to determine if emails and alerts were sent to the 24x7x365 Network Operations Center when predefined events or thresholds were reached and the 24x7x365 Network Operations Center followed up on the alerts.	No deviations noted.
CC6.8.H	Backbone WAN Services authentication servers record failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to Network Design and Engineering staff to determine, on a case by case basis, if further action is required.	Reviewed configurations to determine if failed login attempts were logged and if email notification was sent to Network Design and Engineering staff.	No deviations noted.
CC6.8.I	Antivirus software is used to automatically push virus definition files to all systems after receipt from antivirus vendors.	Reviewed antivirus compliance reports to determine if definitions and updates were configured.	7 of 233 servers' DAT versions were out of compliance. 15 of 2,760 servers' AMCore Content versions were out of compliance.
CC6.8.J	[redacted] is used to detect, investigate security incidents, and provide guidance for remediation to the endpoint cyber threats. [redacted] continuously monitors endpoint telemetry, to detect and respond to malware and exploits.	Reviewed AMP Connector version compliance reports to determine if the Connector versions were compliant.	7 of 14 MAC operating systems AMP Connector version was out of compliance. 62 of 43,377 Windows operating systems AMP Connector versions were out of compliance.

		CC6.8.K	One agency is still in process of migrating from definitions-based antivirus software to the [redacted] for their workstations.	Reviewed antivirus compliance reports to determine if definitions and updates were configured.	21 of 218 Department of Children and Family Services (DCFS) workstations' [redacted] versions were out of compliance.
					28 of 218 DCFS workstations' AMCore Content versions were out of compliance.

Criterial Related to the Security (Common Criteria) Category					
Criteria Number	**Trust Services Criteria**	**Control Number**	**Controls Specified by the Department**	**Tests of Controls Performed by the Office of the Auditor General**	**Results of Tests**
	Common Criteria Related to System Operations				
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CC7.1.A	Vulnerability scans are scheduled weekly. The Department shares vulnerability scanning results with Group CIO's and agency CIO's via email weekly.	Selected a sample of weekly vulnerability scans to determine if they were completed and shared with the Group CIOs and Agency CIOs.	5 of 5 weeks selected did not have vulnerability scans communicated to all Group CIOs and Agency CIOs.
		CC7.1.B	The Department's Security Software Coordinator or designee runs a weekly violation report which is reviewed for invalid and unauthorized access attempts of the Department and proxy agency security software IDs. The Department's Security Software Coordinator follows up with the review results as stated in the Security Violation Report Procedure. The Department's Security Software Coordinator or designee contacts the individual or their supervisor to determine the reason for the violation.	Selected a sample of weekly reports to determine if the Security Software Coordinator or designee had reviewed and followed up on invalid and unauthorized access attempts.	No deviations noted.
		CC7.1.C	Self-monitoring network routers and switches record all events, notifies [redacted] and forwards to multiple logging servers. These servers use filters to automatically generate alerts when a network services' configured parameter or condition occurs.	Reviewed network routers and switches to determine if they were encoded with filters and if the Network Operations Center was reviewing and resolving alerts received.	No deviations noted.
		CC7.1.D	LAN Services network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to LAN Services Support staff and a console display alert when a predefined event occurs, or a threshold is reached. LAN Services Support staff follow up on these alerts and engage operational teams for resolution as necessary.	Reviewed software configurations to determine if emails and alerts were sent and LAN Services Support staff followed up on the alerts.	No deviations noted.
		CC7.1.E	The authentication server records failed login attempts to the network equipment.	Reviewed configurations to determine if failed login attempts were logged.	No deviations noted.

		CC7.1.F	WAN Services network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / or console display alert when a predefined event occurs, or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. The 24x7x365 Network Operation Center staff reviews each occurrence and engage operation teams for resolution.	Reviewed software configurations to determine if emails and alerts were sent to the 24x7x365 Network Operations Center when predefined events or thresholds were reached and the 24x7x365 Network Operations Center followed up on the alerts.	No deviations noted.
		CC7.1.G	WAN Services authentication server records failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to the Network Design and Engineering staff to determine, on a case by case basis, if further action is required.	Reviewed configurations to determine if failed login attempts were logged and if an email notification was sent to Network Design and Engineering staff.	No deviations noted.
		CC7.1.H	Backbone WAN Services Network monitoring software collects and analyzes operational metrics of device connectivity, traffic bandwidth, and processor utilization. The software generates an email to the 24x7x365 Network Operations Center and / or console display alert when a predefined event occurs or a threshold is reached. The 24x7x365 Network Operations Center determines if further action is required and engages operational teams for resolution as necessary. Alerts are tracked in the Network monitoring system.	Reviewed software configurations to determine if emails and alerts were sent to the 24x7x365 Network Operations Center when predefined events or thresholds were reached and the 24x7x365 Network Operations Center followed up on the alerts.	No deviations noted.
		CC7.1.I	Backbone WAN Services authentication servers record failed login attempts to the network equipment. Failed attempts are stored and recorded within the authentication server. This server automatically generates an email notification which is forwarded to Network Design and Engineering staff to determine, on a case by case basis, if further action is required.	Reviewed configurations to determine if failed login attempts were logged and if email notification was sent to Network Design and Engineering staff.	No deviations noted.

CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	CC7.2.A	The Department provides client agencies with the Agency Instructional Guide for Submitting Vulnerability and Remediation Tickets to mitigate identified server vulnerabilities.	Reviewed the Agency Instructional Guide for Submitting Vulnerability and Remediation Tickets to determine if it provided guidance to agencies.	No deviations noted.
		CC7.2.B	The Computer Operations Center utilizes software and the Automated Operations Console to continuously monitor the mainframe and midrange environment 24x7x365.	Observed the software and the AOC to determine if it monitored the mainframe and midrange environment.	No deviations noted.
		CC7.2.C	Problems, issues, and incidents are recorded via the Daily Shift Reports and a Remedy ticket is created.	Selected a sample of Daily Shift Reports to determine if problems, issues and incidents were recorded and if a Remedy ticket was created.	No deviations noted.
		CC7.2.D	The Daily Shift Report documents the activity conducted on mainframe production systems and incident calls received at the Computer Operations Center. The Report contains the date, time, system involved in the incident, along with a narrative providing any necessary information regarding the incident. The Report is forwarded to Enterprise Infrastructure management and supervisors for awareness and follow-up of outstanding issues.	Selected a sample of Daily Shift Reports to determine if they documented activity conducted on the mainframe production environment, recorded incident calls received, and were forwarded to the Enterprise Infrastructure management for follow-up.	No deviations noted.
		CC7.2.E	The Operator Shift Change Checklist (an action list shared between shifts) is completed at the beginning of each shift to ensure the production systems are operating appropriately and any open items are passed on to the next shift and to identify any changes which need to be made. The Operator Shift Change Checklist are signed off by Operations Center supervisors.	Selected a sample of the Operator Shift Change Checklists to determine if they were completed at the beginning of each shift and reviewed by the Operations Center supervisors.	No deviations noted.
		CC7.2.F	The Security Operations Center monitors the network for the detection and analysis of potential intrusions, cybersecurity threats, and incidents.	Observed tools to monitor network for the detection and analysis of potential intrusions, cybersecurity threats and incidents.	No deviations noted.
		CC7.2.G	Depending on the threat, the Security Operation Center has established Standard Operating Procedures to assist with the detection, analysis and resolution.	Reviewed the Security Operating Procedures to determine if the Security Operating Procedures assisted with the detection, analysis and resolution of potential threats.	No deviations noted.
		CC7.2.H	The mainframe environment is monitored through the z/OS systems console for errors and issues.	Observed the z/OS system console to determine if errors and issues were documented.	No deviations noted.
		CC7.2.I	Mainframe system performance and capacity is monitored by System Software programming personnel, via Resource Measurement Facility reports which are run daily and monthly.	Selected a sample of Resource Measurement Facility reports to determine if they were ran daily and monthly and monitored by System Software programming personnel.	No deviations noted.

		CC7.2.J	The Network Operations Center monitors 24x7x365 for network devices and bandwidth for outages and alerts from the network monitoring systems.	Reviewed software configurations to determine if emails and alerts were sent to the 24x7x365 Network Operations Center when predefined events or thresholds were reached and the 24x7x365 Network Operations Center followed up on the alerts.	No deviations noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CC7.3.A	The Incident Management Process Guide documents Department workflow and remediation processes for incidents reported to the IT Service Desk.	Reviewed the Incident Management Process Guide to determine if it documented the workflow and remediation process of reported incidents.	No deviations noted.
		CC7.3.B	The Daily Shift Report documents the activity conducted on mainframe production systems and incident calls received at the Computer Operations Center. The Report contains the date, time, system involved in the incident, along with a narrative providing any necessary information regarding the incident. The Report is forwarded to Enterprise Infrastructure management and supervisors for awareness and follow-up of outstanding issues.	Selected a sample of Daily Shift Reports to determine if they documented activity conducted on the mainframe production environment, recorded incident calls received, and were forwarded to the Enterprise Infrastructure management for follow-up.	No deviations noted.
		CC7.3.C	The System Coordinator runs a System Management Facility violation report weekly for review and signs off on the report after resolving any unusual violations.	Reviewed a sample of weekly System Management Facility violation reports to determine if unusual violations were resolved and the reports were signed off on by the System Coordinator.	No deviations noted.
		CC7.3.D	If encryption is inactive or was not installed as part of the device imaging process prior to deployment, EUC Image Management will assign the Remedy ticket to the Security Operations Center (SOC) who will enact a breach investigation that consists of steps outlined in their Security Incident Playbook.	Selected a sample of lost or stolen laptops in which encryption was not installed to determine if the SOC enacted a breach investigation as outlined in the Security Incident Playbook.	No deviations noted.
		CC7.3.E	Upon notification of a threat, the Department follows the Cyber Security Incident Response Plan.	Selected a sample of threats to determine if the Cyber Security Incident Response Plan was followed.	8 of 25 medium and high priority incidents selected did not have an Executive Summary sent to the CISO or DCISO upon closing of the incident.
					1 of 6 medium incidents selected did not contain the agency's notification upon determination of user impact.

					2 of 25 medium and high priority incidents selected did not have an Executive Summary sent to the CISO upon opening of the incident.
		CC7.3.F	Problems, issues, and incidents are recorded via the Daily Shift Reports and a Remedy ticket is created.	Selected a sample of Daily Shift Reports to determine if problems, issues and incidents were recorded and if a Remedy ticket was created.	No deviations noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CC7.4.A	When the IT Service Desk receives a report of an incident, a Remedy ticket is opened, documenting the user’s name, agency, and contact information along with a detailed description of the incident.	Observed the receipt of an incident report by the IT Service Desk to determine if the Remedy ticket documented the user's name, agency, and contact information.	No deviations noted.
		CC7.4.B	Each incident is categorized based on the service, system, or application impacted by the incident. Tickets are also prioritized based on the impact (the number of affected users) and urgency (how quickly the resolution is needed) of the incident.	Selected a sample of incident tickets to determine if the incident ticket was categorized and prioritized.	No deviations noted.
		CC7.4.C	For identified high or medium risk incidents, an executive summary is sent from the Incident Response Case Management to the Deputy CISO and CISO upon closure for their awareness.	Selected a sample of medium and high reported incidents to determine if an executive summary was to the Deputy CISO and CISO upon closure.	8 of 25 medium and high priority incidents selected did not have an Executive Summary sent to the CISO or DCISO upon closing of the incident.
		CC7.4.D	Reported incidents are tracked via a Remedy ticket until appropriate remediation efforts are completed.	Selected a sample of Remedy tickets to determine if they had been tracked until remediation efforts were completed.	No deviations noted.
		CC7.4.E	The Major Incident Process provides a method for escalated handling of an incident to help facilitate a quicker resolution time, as well as provide notifications/updates to Department staff.	Reviewed the Major Incident Process to determine if it provided a method for the handling of escalated incidents and providing notifications and updates to Department staff.	No deviations noted.
		CC7.4.F	The Incident Management Process Guide documents Department workflow and remediation processes for incidents reported to the IT Service Desk.	Reviewed the Incident Management Process Guide to determine if it documented the workflow and remediation process of reported incidents.	No deviations noted.

CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	CC7.5.A	The Security Operations Center’s incident response details are available in the System Operations Center’s Incident Response Case Management system for management to review.	Selected a sample of incidents to determine if incident response details were available in the Incident Response Case Management system for management to review.	No deviations noted.
		CC7.5.B	The Incident Management Process Guide documents Department workflow and remediation processes for incidents reported to the IT Service Desk.	Reviewed the Incident Management Process Guide to determine if it documented the workflow and remediation process of reported incidents.	No deviations noted.

Criterial Related to the Security (Common Criteria) Category

Criteria Number	Trust Services Criteria	Control Number	Controls Specified by the Department	Tests of Controls Performed by the Office of the Auditor General	Results of Tests
	Common Criteria Related to Change Management				
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC8.1.A	Control over changes to the network, mainframe, mainframe patching, and midrange infrastructures as well as to data storage devices are documented in the Change Management Process Guide, ROD Change Management Guide, and the Change Management User Guide which provides a quick reference of the Department's change processes.	Reviewed the Change Management Process Guide, ROD Change Management Guide, and the Change Management User Guide to determine if controls were documented.	The required approvals documented in the Remedy on Demand User Guide contradicted the required approvals documented in the Change Management Guide.
		CC8.1.B	z/OS production systems are updated quarterly and when patches become available, all other mainframe software components (IMS, CICS, DB2, ISV, etc) are updated.	Reviewed z/OS production system patches to determine if they were updated quarterly.	No deviations noted.
				Reviewed other mainframe components patches to determine if they were patched when available.	No deviations noted.
		CC8.1.C	Changes with a significant or extensive impact require test, implementation, and back out information be provided within the change request.	Selected a sample of significant or extensive impact changes to determine if test, implementation, and backout information was provided with the change request.	6 of 60 significant or extensive impact changes selected did not contain a test plan.
					6 of 60 significant or extensive impact changes selected did not contain a backout plan.
					6 of 60 significant or extensive impact changes selected did not contain a implementation plan.
		CC8.1.D	Change requests are classified into class and impact categories with the level of approval is based on the assigned impact. Approval is required prior to being placed into production.	Reviewed a sample of changes to determine if the change was properly approved based on its class and impact categories and approved prior to being placed into production.	4 of 60 medium, high and critical impact changes selected were not approved by the Change Advisory Committee.
					4 of 60 low and high impact changes selected were not approved by a group manager.
					16 of 60 low impact changes selected were not approved by the Enterprise Change Manager.
					3 of 60 low impact changes selected were not reviewed.

		CC8.1.E	Emergency changes require a Post Implementation Review be provided within the change request.	Reviewed a sample of emergency changes to determine if a Post Implementation Review was provided within the change request.	3 of 16 emergency changes selected did not have a Post Implementation Review conducted.
					6 of 16 emergency changes selected did not have a Post Implementation Review completed within two business days after implementation.
		CC8.1.F	The Department follows the Server Patch Management procedures for receiving and deploying Microsoft Windows patches monthly.	Selected a sample of monthly Microsoft Window patches to determine if they followed the Server Patch Management procedures.	No deviations noted.
		CC8.1.G	The Department utilizes [redacted] to push and monitor Windows patches after obtaining approval.	Reviewed the [redacted] patch schedule to determine if Window patches are pushed out and monitored.	No deviations noted.
		CC8.1.H	The Department follows the applicable patching procedures for the Linux, VMware and Unix (AIX) patches are implemented when provided by the vendor.	Selected a sample of Linux, VMWare, and Unix patches to determine if they followed the applicable patching procedures.	4 of 4 VMWare patches selected did not have documentation of testing completed prior to implementation.
		CC8.1.I	The patches are reviewed and tested by technicians and follow the Department's change management process.	Selected a sample of Linux, VMWare, and Unix patches to determine if they were reviewed and tested by technicians and followed the Department's change management process.	4 of 4 VMWare patches selected did not have documentation of testing completed prior to implementation.
					1 of 2 Unix patches selected did not have documentation of testing being completed prior to implementation.

Criterial Related to the Security (Common Criteria) Category					
Criteria Number	Trust Services Criteria	Control Number	Controls Specified by the Department	Tests of Controls Performed by the Office of the Auditor General	Results of Tests
	Common Criteria Related to Risk Mitigation				
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC9.1.A	The Recovery Activation and Response plan outlines roles and responsibilities and the transition of efforts and teams as incident response moves into recovery. The Recovery Activation and Response Plan is reviewed for accuracy annually and after each effort supporting incident responses.	Reviewed the Recovery Activation and Response plan to determine if roles and responsibilities were defined and it had been reviewed annually or after each effort supporting an incident response.	No deviations noted.
		CC9.1.B	Disaster recovery tests are performed annually via one of the following methods of either tabletop simulations, walk-throughs of plans, proof of concept testing, or functional exercises.	Reviewed recovery testing documentation to determine if testing was conducted annually.	No deviations noted.
		CC9.1.C	The Department has implemented redundancy in the Data Center LANs and at agency locations where technically, fiscally, and operationally feasible.	Review configurations to determine if they had been configured for redundancy.	No deviations noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	CC9.2.A	The Department's project management team conducts daily meetings with Splunk, Inc., weekly meetings to ensure compliance with contractual requirement with NICUSA, Inc., Google, LLC (starting July 9th, 2020), Salesforce, Inc. (starting September 15th 2020), ServiceNow, Inc. (with more frequency if requested), Mircro Focus (starting August 17, 2020 with more frequency if requested) and Okta, Inc. (starting September 22, 2020). Meetings with BMC Software, Inc. (starting on October 19, 2020) and Docusign, Inc. are scheduled every two weeks, while meeting with RiskSense, Inc. is scheduled quarterly (starting January 2021). A monthly meeting is held with Microsoft, LLC. The Department communicates with Zayo Group, LLC management regarding existing services as stated in the contracts.	Reviewed meeting documentation to determine if the Department conducted meetings with the service providers at various intervals.	No deviations noted.
		CC9.2.B	The Department annually monitors the DCMS managed CCF and Communications Building to ensure appropriate physical and environmental controls are in place.	Reviewed checklists and analysis to determine if the Department annually monitored the CCF and Communications Building.	No deviations noted.
		CC9.2.C	The GRC group collects and reviews subservice providers' System and Organization Controls (SOC) reports from BMC Software, Inc., Docusign, Inc., Microsoft, LLC, Micro Focus Software, Inc., NICUSA, Inc., Google, LLC, Okta, Inc., RiskSense, Inc., Salesforce, Inc., ServiceNow, Inc., Splunk, Inc., and Zayo Group, LLC for alignment with the State of Illinois enterprise information system security policies.	Reviewed SOC reports to determine if the GRC group reviewed for alignment with the State of Illinois enterprise information system security policies.	3 of 13 subservice providers' SOC reports were not provided.

		CC9.2.D	The subservice providers’ contracts require them to contact the Department in the event of a security incident or information breach which impacts the State's data.	Reviewed subservice providers' contracts to determine if the contracts require the subservice providers to contact the Department in the event of a security incident or information breach.	2 of 12 subservice providers' contracts did not contain the requirement for the subservice provider to contact the Department in the event of a security incident or information breach.

Criterial Related to the Availability Category

Criteria Number	Trust Services Criteria	Control Number	Controls Specified by the Department	Tests of Controls Performed by the Office of the Auditor General	Results of Tests
	Criteria Related to Availability Category				
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	A1.1.A	Data Storage performance and capacity are monitored using vendor specific toolsets.	Reviewed toolsets' configurations to determine if data storage performance and capacity were monitored.	No deviations noted.
		A1.1.B	Automated alerts are sent via email to Data Storage technicians and management when capacity is reached or exceeds 80%.	Reviewed storage system configurations to determine if automated alerts were configured.	No deviations noted.
		A1.1.C	Midrange data backups are monitored by [redacted] and [redacted]	Reviewed the [redacted] [redacted] configurations to determine if midrange system data backups were monitored.	No deviations noted.
		A1.1.D	[redacted] is used to monitor and report on midrange backups.	Reviewed [redacted] to determine if it monitored and reported on midrange backups.	No deviations noted.
		A1.1.E	Performance and capacity monitoring are documented via internal memorandum distributed via email to Enterprise Infrastructure management monthly.	Selected a sample of internal memoranda to determine if they were distributed monthly to Enterprise Infrastructure management.	No deviations noted.
		A1.1.F	Midrange availability is monitored by the Operations Command Center via the [redacted] [redacted]	Observed [redacted] to determine if availability and performance were monitored.	No deviations noted.
		A1.1.G	SQL database servers use the [redacted] tool set for additional monitoring. The [redacted]ystem alerts have been set up to generate emails to SQL support staff.	Reviewed the [redacted] configuration to determine if monitoring and email alerts to SQL support staff were configured.	No deviations noted.
		A1.1.H	The Active Directory Domain Controllers use [redacted] for additional monitoring. [redacted] alerts have been set up to email alerts to AD support staff.	Reviewed [redacted] configurations to determine if monitoring and email alerts to AD support staff were configured.	No deviations noted.
		A1.1.I	The Department has implemented mainframe backup procedures to assist staff in the event of failures.	Reviewed policies to determine if they outlined procedures in the event of failed backups.	No deviations noted.

A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A1.2.A	Device configurations are saved on a network management server, which verifies device configuration revisions daily, and new configurations are backed up when detected.	Reviewed configurations' backup schedule to determine if the configurations were saved on a network management server.	From April 15, 2021 to April 23, 2021 device configuration revisions were not backed up.
		A1.2.B	Configurations saved on the network management server are backed up daily to the CCF and the Alternate Data Center (ADC) through the midrange backup system.	Reviewed the backup schedule to determine if the network management server was backed up daily to the CCF and the ADC.	No deviations noted.
		A1.2.C	Data on mainframe systems are backed up daily and weekly utilizing [redacted]	Observed the [redacted] to determine if mainframe backups were performed daily and weekly.	No deviations noted.
		A1.2.D	The Department utilizes [redacted] to schedule and verify the completion of the backups.	Selected a sample of backup schedules to determine if mainframe backups were scheduled and the completion was verified.	No deviations noted.
		A1.2.E	In the event of a mainframe daily backup job failure, the Department's Operations Center staff records the incident in the Shift Report.	Reviewed a sample of daily and weekly backup reports, Remedy tickets, and Daily Shift reports to determine if mainframe backup jobs had failed.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating the effectiveness of this control.
		A1.2.F	The Department's Storage staff review the output of the weekly backup jobs for success or failure. The failure is researched and corrected, and then the failed portion of the backup job is resubmitted for completion.	Reviewed a sample of daily and weekly backup reports, Remedy tickets, and Daily Shift reports to determine if mainframe backup jobs had failed.	The Department did not encounter failed backups during the period covered by the report. Therefore, the Service Auditor was unable to test the operating effectiveness of this control.
		A1.2.G	Mainframe data replication occurs every [redacted] between the CCF and the ADC [redacted] The monitoring software sends the Enterprise Storage and Backup group an alert if the data is out of sync for more than 24 hours.	Reviewed the [redacted] configurations to determine if replication occurred every [redacted] and an alert was sent if the data was out of sync for more than 24 hours.	No deviations noted.
		A1.2.H	The [redacted] Replicated Status log keeps a log of replication between the two [redacted] and tracks library replication outcomes for [redacted] replication activity.	Reviewed the [redacted] replication log to determine if the current replication activity was recorded and tracked the replication outcomes.	No deviations noted.
		A1.2.I	[redacted] are used to back up the midrange environment.	Reviewed [redacted] to determine if they were used to backup the midrange environment.	No deviations noted.

A1.2.J	Midrange server backups are performed daily or weekly and are either incremental or full.	Reviewed the [redacted] design to determine if midrange servers were backed up daily or weekly and were either incremental or full.	No deviations noted.
A1.2.K	[redacted] automatically generate daily reports indicating the backup status of scheduled jobs from the prior day. These daily reports are emailed to the Enterprise Storage and Backup group who then investigates the cause of failures and works to resolve the problem.	Observed [redacted] [redacted] to determine if they were configured to send daily reports of the backup status for all scheduled jobs.	No deviations noted.
		Interviewed Enterprise Storage and Backup staff to determine the actions taken to resolve the failures.	No deviations noted.
A1.2.L	Backed up server data is written to a Data Domain storage system and then replicated to another Data Domain storage system at the ADC. The Data Domain storage systems generate a daily status report which is emailed to the Enterprise Storage and Backup group.	Reviewed the replication of the Data Domain storage system to determine if it was replicated to the ADC.	No deviations noted.
		Reviewed the Data Domain configuration to determine if daily reports of the replication status for all scheduled jobs were emailed to the Enterprise Storage and Backup group.	No deviations noted.
A1.2.M	The Data Domain storage systems also send email alerts to the Enterprise Storage and Backup group when issues arise that may need additional attention.	Reviewed the Data Domain configuration to determine if alerts were sent to the Enterprise Storage and Backup group.	No deviations noted.
A1.2.N	The Data Domain systems automatically alert vendor support in the event of hardware or system failures.	Reviewed the Data Domain storage system configuration to determine if alerts were sent to the vendor support.	No deviations noted.
A1.2.O	The database backups are written to the Data Domain storage systems via Common Internet File System or Network File System and then replicated to the ADC.	Reviewed the replication of the Data Domain storage system to determine if it was replicated to the ADC.	No deviations noted.
A1.2.P	A [redacted] goes through the production SQL servers and creates a report with the latest backup date and it is sent to the SQL team daily. The SQL team reviews it and follows up for any failures.	Reviewed the SQL configuration to determine the status of backups was documented daily.	No deviations noted.
A1.2.Q	The SQL team also gets alerts from the SQL servers when backup jobs fail.	Reviewed the SQL servers' configurations to determine if alerts were enabled.	No deviations noted.
A1.2.R	The SQL team receives alerts from the [redacted] monitoring software if a database has missed a backup.	Reviewed the [redacted] monitoring software configuration to determine if automatic alerts were enabled.	No deviations noted.
A1.2.S	The Enterprise Storage and Backup group has policies on the [redacted] that take daily snapshots of all shares which are then retained up to 60 days.	Reviewed the [redacted] policies to determine if daily snapshots of all shares were taken and retained for up to 60 days.	No deviations noted.

		A1.2.T	The [redacted] generates a daily report showing successful and failed synchronization attempts with the ADC.	Reviewed the [redacted] storage device configuration to determine if daily reports documenting successful and failed synchronization attempts were generated.	No deviations noted.
		A1.2.U	The [redacted] has a call home feature that notifies vendor support. For critical issues, the [redacted] call home feature additionally notifies the Enterprise Storage and Backup group.	Reviewed the [redacted] configuration to determine if the call home feature was activated and notifications were sent to the Enterprise Storage and Backup group.	No deviations noted.
		A1.2.V	The Department has implemented redundancy in the Data Center LANs and at agency locations where technically, fiscally, and operationally feasible.	Review configurations to determine if they had been configured for redundancy.	No deviations noted.
		A1.2.W	The software MOVEit is used to transmit midrange data between servers and applications and provides email alerts for any failures to Department and agency support staff.	Reviewed the MOVEit software configurations to determine if MOVEit was used to transmit data between servers and applications and if email alerts were sent for failures to Department and agency support staff.	No deviations noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A1.3.A	Disaster recovery tests are performed annually via one of the following methods of either tabletop simulations, walk-throughs of plans, proof of concept testing, or functional exercises.	Reviewed recovery testing documentation to determine if testing was conducted annually.	No deviations noted.

SECTION V

OTHER INFORMATION PROVIDED BY THE DEPARTMENT OF INNOVATION AND TECHNOLOGY THAT IS NOT COVERED BY THE SERVICE AUDITOR'S REPORT

Trust Principal Control	Department's Response
CC1.1.G, CC1.4.C, CC1.5.C, CC2.2.J	The Department will continue sending training reminders to the employees.
CC1.5.A	The Department will continue distributing monthly evaluation tickler reports. It is the supervisor's responsibility and obligation to complete the performance evaluation as required and submit to HR for processing.
CC2.2.F	The Department will create and disseminate a policy and procedure review schedule to ensure documentation for all policies and procedures assessment dates is maintained.
CC2.3D, CC9.2.D	The Department will continue to request and will endeavor to require through vendor contracts and related written documentation that subservice providers contact the Department in the event of a security incident or information breach.
CC3.1.B, CC5.1.B	The Department will continue providing risk assessments to client agencies.
CC6.2.A	The Department will research opportunities to generate reports in the requested format for future audit testing.
CC6.2.B	The Department will review and clarify the employee offboarding process.
CC6.2.B	The Department will remind staff of service request requirements.
CC6.2.C	The Department will research opportunities to generate reports in the requested format for future audit testing. Additionally, the Department will remind staff of service request requirements.
CC6.3.C	The Department will review the list of individuals with administrative rights and modify access as necessary.
CC6.3.D	The Department continues completing the RACF reconciliation.
CC6.4.E	The Department will remind staff of the internal process guide to ensure all fields are completed.
CC6.4.H	The Department will research opportunities to generate reports in the requested format for future audit testing.
CC6.4.O	The Department will follow up with the Department of Central Management Services (DCMS) to ensure that the DCMS follows the Department's badging process.
CC6.5.A	The Department will continue working on cleaning up the offboarding tickets.

CC6.8.1, CC6.8.J, CC6.8.K	It is common that some endpoints will be out of compliance at any given time due to being offline, out of network connectivity, and other reasons. The Endpoint Protection team utilizes a process to investigate and correct endpoints that are out of compliance. The team will continue to investigate and address any out-of-date files or updates as well as additional tools.
CC7.1.A	The Department will ensure that its distribution list is updated and continue distributing weekly vulnerability scans to Group CIOs and agency CIOs.
CC7.4.C, CC7.3.E	The Department has configured and will send notifications to the CISO and Deputy CISO automatically from the incident case management system to document their awareness.
CC8.1.A	The Department will retire the Remedy on Demand User Guide when the Department starts using the new service management tool in FY22.
CC8.1.C	The Department will update the internal document and remind staff of the internal process guide.
CC8.1.D, CC8.1.E	The Department will continue to follow the enterprise change management process guide and retire the Remedy on Demand change management process guide in FY22 that caused the exception.
CC8.1.H, CC8.1.I	The Department will remind staff of the internal process guide and documentation of testing.
CC9.2C	The Department will continue to require subservice providers to submit SOC reports, bridge letters, or an equivalent document.
A1.2.A	The Department will continue to back up devices before implementing a tool migration in order to minimize risk and allow for recovery of the backup as needed.

ACRONYM GLOSSARY

Act – Department of Innovation and Technology Act
AD – Active Directory
ADC – Alternate Data Center
ADFS – Active Directory Federal Services
AIX – Advanced Interactive eXecutive
APIs – Application Program Interfaces
ATSR – Agency Technology Service Requestor
CAC – Change Advisory Committee
CCF – Central Computer Facility
CICS – Customer Information Control System
CIOs – Chief Information Officers
CISO – Chief Information Security Officer
CJIS – Criminal Justice Information Services
CMOS – Complementary Metal Oxide Semiconductor
CMS – Central Management Services
DB2 – Database 2
DCMS – Department of Central Management Services
Department – Department of Innovation and Technology
DIM – Department's Identity Management
[redacted]
DoIT – Department of Innovation and Technology
Employee Portal - intranet
[redacted]
EUC – End User Computing
FTPS – File Transfer Protocol Secure
GRC – Governance, Risk and Compliance
GUI – Graphical User Interface
HR – Human Resources
ICN – Illinois Century Network
ID – Identification
ILCS – Illinois Compiled Statutes
IMS – Information Management System
IT – Information Technology
JCL – Job Control Language
LAN – Local Area Network
MIM – Microsoft Identity Management
MORT – Major Outage Response Team
MS-ISAC – Multi-State Information Sharing and Analysis Center
NIST – National Institute of Standards and Technology
ORAQ – Organization Risk Assessment Questionnaire
OS – Operating System
PAR – Personnel Action Request
PSC – Personal Service Contractor
ROD – Remedy on Demand

RMP – Risk Management Program
SOC – System and Organization Controls
SOC – Security Operation Center
SSO – Single SignOn
SQL – Structured Query Language
Velocity – Velocity Access Control System
VPN – Virtual Private Network
WAN – Wide Area Network
z/OS – Zero Downtime Operating System
z/VM – Zero Downtime Virtual Machine