# Trust Services Criteria, Related Controls and Tests of Controls Relevant to the security, availability and confidentiality Categories

| **CONTROL ENVIRONMENT** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **CC1.1** | The entity demonstrates a commitment to integrity and ethical values. | | |
|  | Management has established defined roles and responsibilities to oversee the implementation of the information security policy. | Inspected security policies to determine that TEST COMPANY had established defined roles and responsibilities to oversee the implementation of the information security policy. | No exceptions noted. |
| Employees must acknowledge the TEST COMPANY Business Conduct Guidelines () upon hire, which describe their responsibilities and expected behavior regarding data and information system usage. | Inspected the TEST COMPANY to determine that it documented employee responsibilities and expected behavior regarding data and information system usage. | No exceptions noted. |
| Inspected acknowledgements for a sample of new hires to determine that new hires were required to acknowledge that they had read and agreed to the upon hire. | Exceptions noted. 6 out of 25 new hires sampled did not acknowledge the TEST COMPANY within 30 days of hire and 1 out of 25 new hires sampled did not acknowledge the during the review period. |
| Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has been granted access. | Inspected the confidentiality agreement to determine that it prohibited the disclosure of information and other data to which the employee had been granted access. | No exceptions noted. |
|  | Inspected signed confidentiality agreements for a sample of new hires to determine that new hires were provided and accepted the agreement. | No exceptions noted. |
| All users must read and sign a SmartCloud for Government (SCG) Rules of Behavior (RoB) prior to accessing systems and annually thereafter. The RoB outlines TEST COMPANY's commitments to integrity and ethical values. | Inspected the RoB to determine that the RoB document demonstrated a commitment to integrity and ethical values. | No exceptions noted. |
| Inspected acknowledgements for a sample of new hires to determine that new hires were required to acknowledge that they had read and agreed to the SCG RoB prior to accessing systems. | No exceptions noted. |
| Inspected acknowledgements for a sample of employees to determine that employees were required to acknowledge that they had read and signed the SCG RoB annually. | No exceptions noted. |
| New personnel offered employment are subject to background checks. | Inspected background check completion evidence for a sample of new hires to determine that new hires were subject to background checks. | No exceptions noted. |
| **CC1.2** | The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | | |
|  | The FedRAMP Joint Authorization Board (JAB) is designated as the Authorizing Official (AO) for the system and is independent from management. The FedRAMP JAB oversees the development and performance of internal controls through the FedRAMP continuous monitoring process. | Inspected the Provisional Authorization to Operate (P-ATO) to determine that the FedRAMP JAB was designated as the AO for the system, was independent from management, and oversaw the development and performance of internal controls through the FedRAMP continuous monitoring process. | No exceptions noted. |
| The system’s P-ATO is updated at least every three years or whenever there is a significant change to the systems, as decided by the TEST COMPANY AO. | Inspected the most recent P-ATO to determine that it was updated within the past three (3) years or whenever there was a significant change to the systems, as decided by the TEST COMPANY AO. | No exceptions noted. |
| TEST COMPANY has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected the organization chart to determine that it defined the organizational structure and reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |
| **CC1.3** | Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | |
|  | TEST COMPANY has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected the organization chart to determine that it defined the organizational structure and reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |
| Management has established defined roles and responsibilities to oversee the implementation of the information security policy. | Inspected security policies to determine that TEST COMPANY had established defined roles and responsibilities to oversee the implementation of the information security policy. | No exceptions noted. |
| **CC1.4** | The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | |
|  | Managers are required to complete performance appraisals for direct reports at least annually. | Inspected performance appraisals for a sample of employees to determine that managers were required to complete performance appraisals for direct reports at least annually. | No exceptions noted. |
| TEST COMPANY requires all Secure Cloud for Government (SCG) personnel to undergo security awareness training, including development in system security concepts and issues, upon hire and annually thereafter. | Inspected training documentation to determine that security training included development in system security concepts and issues. | No exceptions noted. |
| Inspected training completion evidence for a sample of new hires to determine that security training was completed upon hire for each new hire sampled. | No exceptions noted. |
|  | Inspected training completion evidence for a sample of employees to determine that security training was completed annually for each employee sampled. | Exceptions noted. 4 out of 25 current employees sampled did not complete the annual training within the review period. |
| New personnel offered employment are subject to background checks. | Inspected background check completion evidence for a sample of new hires to determine that new hires were subject to background checks. | No exceptions noted. |
| Job descriptions are documented for employees supporting the service. | Inspected job descriptions for a sample of employees to determine that job descriptions were documented for employees supporting the service. | No exceptions noted. |
| **CC1.5** | The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | |
|  | TEST COMPANY has an organization chart that defines the organizational structure, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected the organization chart to determine that it defined the organizational structure and reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |
| Management has established defined roles and responsibilities to oversee the implementation of the information security policy. | Inspected security policies to determine that TEST COMPANY had established defined roles and responsibilities to oversee the implementation of the information security policy. | No exceptions noted. |
| Managers are required to complete performance appraisals for direct reports at least annually. | Inspected performance appraisals for a sample of employees to determine that managers were required to complete performance appraisals for direct reports at least annually. | No exceptions noted. |

| **COMMUNICATION AND INFORMATION** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **CC2.1** | The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | |
|  | The Information Security Policy (ISP) documents information security rules and requirements for the SCG environment and related systems and is reviewed at least every three years or more frequently if significant changes occur. | Inspected the ISP to determine that it documented information security rules and requirements for the SCG environment and related systems and was reviewed at least every three years or more frequently if significant changes occurred. | No exceptions noted. |
| A System Security Plan (SSP) is documented for the SCG environment that provides an overview of the security requirements for the system, describes the security controls in place, and is reviewed and updated at least annually or when significant changes occur. | Inspected the SSP to determine that it was documented for the SCG environment and provided an overview of the security requirements for the system, described the security controls in place, and was reviewed and updated at least annually or when significant changes occurred. | No exceptions noted. |
| A Security Assessment Report (SAR) is performed by a third-party assessment organization (3PAO) annually. Plan of Actions and Milestones (POA&Ms) are developed and changes are implemented to remediate all vulnerabilities. | Inspected the most recent SAR to determine that a SAR was performed by a 3PAO within the past year. | No exceptions noted. |
| Inspected POA&M review documentation for the SAR to determine POA&Ms were developed and changes were implemented to remediate all vulnerabilities. | No exceptions noted. |
| **CC2.2** | The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | | |
|  | The ISP and the SSP are made available and communicated to authorized personnel on an internal protected network share. | Observed TEST COMPANY's internal protected network share to determine that the ISP and SSP were made available and communicated to authorized personnel on an internal protected network share. | No exceptions noted. |
| Job descriptions are documented for employees supporting the service. | Inspected job descriptions for a sample of employees to determine that job descriptions were documented for employees supporting the service. | No exceptions noted. |
| TEST COMPANY has developed and distributed the security incident policies and procedures that are communicated to authorized users. | Inspected the security incident response policies and procedures to determine that they were developed. | No exceptions noted. |
| Observed ServiceNow to determine that security incident policies and procedures were communicated to authorized users. | No exceptions noted. |
| TEST COMPANY requires all Secure Cloud for Government (SCG) personnel to undergo security awareness training, including development in system security concepts and issues, upon hire and annually thereafter. | Inspected training documentation to determine that security training included development in system security concepts and issues. | No exceptions noted. |
| Inspected training completion evidence for a sample of new hires to determine that security training was completed upon hire for each new hire sampled. | No exceptions noted. |
|  | Inspected training completion evidence for a sample of employees to determine that security training was completed annually for each employee sampled. | Exceptions noted. 4 out of 25 current employees sampled did not complete the annual training within the review period. |
| TEST COMPANY has documented network diagrams that are available to authorized users upon request. | Inspected network diagrams to determine that they were documented and available to authorized users upon request. | No exceptions noted. |
| **CC2.3** | The entity communicates with external parties regarding matters affecting the functioning of internal control. | | |
|  | TEST COMPANY has prepared a description of the system and its boundaries and provides this description to internal and external authorized users. | Inspected the most recent copy of the TEST COMPANY SCG's system description to determine that the system description was documented and available to authorized internal and external users. | No exceptions noted. |
| TEST COMPANY completes an interconnection security agreement (ISA) prior to establishing any persistent connection to the environment.   The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. There were no new persistent connections established with the environment during the review period. | Inquired of management and inspected the SSP to determine that the circumstances that warrant the operation of the control did not occur during the period. | Not tested. There were no new persistent connections established with the environment during the review period. |
| Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. | Inspected contracts for a sample of vendors to determine that formal information sharing agreements were in place and included confidentiality commitments for each vendor sampled. | No exceptions noted. |
| TEST COMPANY provides a service desk that allows users to report system information on failures, incidents, concerns, and other complaints to the appropriate personnel. | Observed the service desk to determine that TEST COMPANY provided a service desk that allowed users to report system information on failures, incidents, concerns, and other complaints to the appropriate personnel. | No exceptions noted. |

| **RISK ASSESSMENT** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **CC3.1** | The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | |
|  | The system is classified in accordance with Federal Information Processing Standard (FIPS) 199 and TEST COMPANY selects and implements the required FedRAMP security controls applicable to its environment. | Inspected the SSP to determine that the system was classified in accordance with FIPS-199 and that TEST COMPANY selected and implemented the required FedRAMP security controls applicable to its environment. | No exception noted. |
| A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the risk management program to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions 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. | | |
|  | Risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the most recent risk assessment to determine that a risk assessment was performed within the past year and, as part of this process, threats and changes to service commitments were identified, the risks were formally assessed, and the risk assessments included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |
| A Security Assessment Report (SAR) is performed by a third-party assessment organization (3PAO) annually. Plan of Actions and Milestones (POA&Ms) are developed and changes are implemented to remediate all vulnerabilities. | Inspected the most recent SAR to determine that a SAR was performed by a 3PAO within the past year. | No exceptions noted. |
| Inspected POA&M review documentation for the SAR to determine POA&Ms were developed and changes were implemented to remediate all vulnerabilities. | No exceptions noted. |
| Internal vulnerability scans for the SCG environment are performed at least monthly. A remediation plan is developed and changes are implemented to remediate all high and moderate vulnerabilities at a minimum. | Inspected internal vulnerability scans for a sample of months and remediation plans to determine that internal vulnerability scans were performed monthly and remediation plans were developed to remediate all high and moderate vulnerabilities at a minimum. | No exceptions noted. |
| Penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate all high and moderate vulnerabilities at a minimum. | Inspected the most recent penetration test report and remediation plan to determine that penetration testing occurred within the last year and a remediation plan was developed to remediate all high and moderate vulnerabilities at a minimum. | No exceptions noted. |
| A list of subservice organizations and critical vendors is maintained and those parties are required to maintain their own security practices and procedures. Conformance is assessed annually by reviewing third-party attestation reports or performing a vendor risk assessment. | Inspected third-party attestation reports or vendor risk assessment documentation for a sample of vendors to determine that a third-party attestation report or risk assessment was performed within the past year for each vendor sampled. | No exceptions noted. |
| **CC3.3** | The entity considers the potential for fraud in assessing risks to the achievement of objectives. | | |
|  | Risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the most recent risk assessment to determine that a risk assessment was performed within the past year and, as part of this process, threats and changes to service commitments were identified, the risks were formally assessed, and the risk assessments included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |
| A Security Assessment Report (SAR) is performed by a third-party assessment organization (3PAO) annually. Plan of Actions and Milestones (POA&Ms) are developed and changes are implemented to remediate all vulnerabilities. | Inspected the most recent SAR to determine that a SAR was performed by a 3PAO within the past year. | No exceptions noted. |
| Inspected POA&M review documentation for the SAR to determine POA&Ms were developed and changes were implemented to remediate all vulnerabilities. | No exceptions noted. |
| **CC3.4** | The entity identifies and assesses changes that could significantly impact the system of internal control. | | |
|  | The Information Security Policy (ISP) documents information security rules and requirements for the SCG environment and related systems and is reviewed at least every three years or more frequently if significant changes occur. | Inspected the ISP to determine that it documented information security rules and requirements for the SCG environment and related systems and was reviewed at least every three years or more frequently if significant changes occurred. | No exceptions noted. |
| The SCG has a POA&M program in place to document TEST COMPANY's planned remedial actions to correct weaknesses or deficiencies. | Inspected the SCG POA&M program to determine that it documented TEST COMPANY's planned remedial actions to correct weaknesses or deficiencies. | No exceptions noted. |
| Internal vulnerability scans for the SCG environment are performed at least monthly. A remediation plan is developed and changes are implemented to remediate all high and moderate vulnerabilities at a minimum. | Inspected internal vulnerability scans for a sample of months and remediation plans to determine that internal vulnerability scans were performed monthly and remediation plans were developed to remediate all high and moderate vulnerabilities at a minimum. | No exceptions noted. |
| Penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate all high and moderate vulnerabilities at a minimum. | Inspected the most recent penetration test report and remediation plan to determine that penetration testing occurred within the last year and a remediation plan was developed to remediate all high and moderate vulnerabilities at a minimum. | No exceptions noted. |
| The SCG receives alerts, advisories, and directives in the Security Intelligence and Operations Center (SIOC) mailbox from industry standard sources (e.g., United States Computer Emergency Readiness Team [US-CERT], SANS Institute, National Institute of Standards and Technology [NIST], Microsoft, Cisco) that are relevant to system security. | Inspected example alerts, advisories, and directives to determine that the SIOC mailbox received alerts from industry standard sources (e.g., US-CERT, SANS Institute, NIST, Microsoft, and Cisco) that were relevant to system security. | No exceptions noted. |

| **MONITORING ACTIVITIES** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **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. | | |
|  | A Security Assessment Report (SAR) is performed by a third-party assessment organization (3PAO) annually. Plan of Actions and Milestones (POA&Ms) are developed and changes are implemented to remediate all vulnerabilities. | Inspected the most recent SAR to determine that a SAR was performed by a 3PAO within the past year. | No exceptions noted. |
| Inspected POA&M review documentation for the SAR to determine POA&Ms were developed and changes were implemented to remediate all vulnerabilities. | No exceptions noted. |
| Internal vulnerability scans for the SCG environment are performed at least monthly. A remediation plan is developed and changes are implemented to remediate all high and moderate vulnerabilities at a minimum. | Inspected internal vulnerability scans for a sample of months and remediation plans to determine that internal vulnerability scans were performed monthly and remediation plans were developed to remediate all high and moderate vulnerabilities at a minimum. | No exceptions noted. |
| Penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate all high and moderate vulnerabilities at a minimum. | Inspected the most recent penetration test report and remediation plan to determine that penetration testing occurred within the last year and a remediation plan was developed to remediate all high and moderate vulnerabilities at a minimum. | No exceptions noted. |
| An information technology (IT) infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific, predefined thresholds are met. | Inspected IT infrastructure monitoring tool configurations and an example notification to determine that IT infrastructure monitoring tools were utilized to monitor IT infrastructure availability and performance and generated alerts when specific, predefined thresholds were met. | No exceptions noted. |
| Environmental monitoring devices are in place and configured to automatically generate an alert to management of environmental incidents. | Inspected the environmental monitoring tool configuration and alert dashboard to determine that the monitoring tools were configured to generate alerts for environmental incidents. | No exceptions noted. |
| A list of subservice organizations and critical vendors is maintained and those parties are required to maintain their own security practices and procedures. Conformance is assessed annually by reviewing third-party attestation reports or performing a vendor risk assessment. | Inspected third-party attestation reports or vendor risk assessment documentation for a sample of vendors to determine that a third-party attestation report or risk assessment was performed within the past year for each vendor sampled. | No exceptions 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. | | |
|  | Reports are provided to the FedRAMP JAB monthly and include a summary of the month’s results, scanner files, and an updated POA&M sheet. | Inspected reports for a sample of months to determine that reports were provided to the FedRAMP JAB monthly and included a summary of the month’s results, scanner files, and an updated POA&M sheet. | No exceptions noted. |
| All POA&Ms are reviewed at least quarterly by the Senior Information Security Officer (SISO) with the System Owner (SO), Lead Information Officer (LIO), and AO via a standing meeting. | Inspected POA&M review documentation for sample of quarters to determine that all POA&Ms were reviewed at least quarterly by the SISO with the SO, LIO, and AO via a standing meeting. | No exceptions noted. |
| A list of subservice organizations and critical vendors is maintained and those parties are required to maintain their own security practices and procedures. Conformance is assessed annually by reviewing third-party attestation reports or performing a vendor risk assessment. | Inspected third-party attestation reports or vendor risk assessment documentation for a sample of vendors to determine that a third-party attestation report or risk assessment was performed within the past year for each vendor sampled. | No exceptions noted. |

| **CONTROL ACTIVITIES** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **CC5.1** | The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | | |
|  | The system is classified in accordance with Federal Information Processing Standard (FIPS) 199 and TEST COMPANY selects and implements the required FedRAMP security controls applicable to its environment. | Inspected the SSP to determine that the system was classified in accordance with FIPS-199 and that TEST COMPANY selected and implemented the required FedRAMP security controls applicable to its environment. | No exception noted. |
| **CC5.2** | The entity also selects and develops general control activities over technology to support the achievement of objectives. | | |
|  | The system is classified in accordance with Federal Information Processing Standard (FIPS) 199 and TEST COMPANY selects and implements the required FedRAMP security controls applicable to its environment. | Inspected the SSP to determine that the system was classified in accordance with FIPS-199 and that TEST COMPANY selected and implemented the required FedRAMP security controls applicable to its environment. | No exception noted. |
| A System Security Plan (SSP) is documented for the SCG environment that provides an overview of the security requirements for the system, describes the security controls in place, and is reviewed and updated at least annually or when significant changes occur. | Inspected the SSP to determine that it was documented for the SCG environment and provided an overview of the security requirements for the system, described the security controls in place, and was reviewed and updated at least annually or when significant changes occurred. | No exceptions noted. |
| **CC5.3** | The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | | |
|  | The Information Security Policy (ISP) documents information security rules and requirements for the SCG environment and related systems and is reviewed at least every three years or more frequently if significant changes occur. | Inspected the ISP to determine that it documented information security rules and requirements for the SCG environment and related systems and was reviewed at least every three years or more frequently if significant changes occurred. | No exceptions noted. |
| A System Security Plan (SSP) is documented for the SCG environment that provides an overview of the security requirements for the system, describes the security controls in place, and is reviewed and updated at least annually or when significant changes occur. | Inspected the SSP to determine that it was documented for the SCG environment and provided an overview of the security requirements for the system, described the security controls in place, and was reviewed and updated at least annually or when significant changes occurred. | No exceptions noted. |
| A list of subservice organizations and critical vendors is maintained and those parties are required to maintain their own security practices and procedures. Conformance is assessed annually by reviewing third-party attestation reports or performing a vendor risk assessment. | Inspected third-party attestation reports or vendor risk assessment documentation for a sample of vendors to determine that a third-party attestation report or risk assessment was performed within the past year for each vendor sampled. | No exceptions noted. |

| **LOGICAL AND PHYSICAL ACCESS CONTROLS** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **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. | | |
|  | Privileged access to the following in-scope system components is restricted to authorized users with a business need: - Network -Operating system (OS) - Database - Hypervisor - Firewall | Inspected in-scope system component access listings and inquired of management to determine that the following components privileged access was restricted to authorized users with a business need: - Network  - OS - Database - Hypervisor - Firewall | No exceptions noted. |
| The following in-scope system components require unique usernames and passwords prior to authenticating users: - Network - OS - Database - Hypervisor - Firewall | Inspected login attempts to determine that the following system components required unique usernames and passwords prior to authenticating users:  - Network - OS - Database - Hypervisor - Firewall | No exceptions noted. |
| TEST COMPANY restricts access to production systems to authorized employees with multi-factor authentication (MFA) over an encrypted virtual private network (VPN) connection. | Observed a remote login session to determine that MFA over an encrypted VPN connection was required to access the production network. | No exceptions noted |
| Passwords for in-scope system components are configured according to TEST COMPANY's policy. TEST COMPANY policy requires the following (unless there is a system limitation): - 14-character minimum - Complexity enabled - 60-day password change - Lockout after 3 invalid attempts | Inspected password configurations for in-scope system components to determine that passwords were configured according to the following TEST COMPANY policy (unless there was a system limitation): - 14-character minimum - Complexity enabled - 60-day password change - Lockout after 3 invalid attempts | No exceptions noted |
| TEST COMPANY prevents further access to the SCG system by initiating a session lock after 15 minutes of inactivity. | Inspected system configurations to determine that TEST COMPANY prevented further access to the SCG system by initiating a session lock after 15 minutes of inactivity. | No exceptions noted. |
| A security information event management (SIEM) system is utilized to identify trends that may have a potential impact on TEST COMPANY's ability to achieve its system security objectives. | Inspected SIEM system configurations to determine that a SIEM was utilized to identify trends that may have had a potential impact on TEST COMPANY's ability to achieve its system security objectives. | No exceptions noted. |
| Intrusion prevention systems are used to provide continuous monitoring of the SCG network and prevention of potential security breaches. | Inspected intrusion prevention system configurations to determine that continuous monitoring of the SCG network and prevention of potential security breaches was in place. | No exceptions noted. |
| TEST COMPANY identifies, inventories, classifies, and manages information assets. | Inspected the system inventory to determine that TEST COMPANY identified, inventoried, classified, and managed information assets. | No exceptions 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. | | |
|  | Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned. | Inspected access request forms for a sample of users that received access to the in-scope system components to determine that an access request form was documented and approved by management prior to access being provisioned for each user sampled. | No exceptions noted. |
| A termination checklist is completed, logical access is revoked, and badges are disabled and collected by management within 24 hours as part of the termination process. | Inspected a listing of terminated employees and compared the listing to the active user listing to determine that terminated employees did not retain access to the in-scope system and platforms after their separation. | No exceptions noted. |
| Inspected termination tickets for a sample of employees terminated during the review period to determine that logical access was revoked and badges were disabled and collected by management within 24 hours as part of the termination process for each terminated employee sampled. | Exceptions noted. 2 of the 8 terminated employees sampled did not have their logical and physical access revoked within 24 hours of their termination date. |
| Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner. | Inspected access review documentation for a sample of quarters to determine that an access review was performed for in-scope system components quarterly and that tickets were created to remove inappropriate access. | Exception noted. Access review documentation for 1 out of 2 of the quarters sampled could not be provided. |
| **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. | | |
|  | Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned. | Inspected access request forms for a sample of users that received access to the in-scope system components to determine that an access request form was documented and approved by management prior to access being provisioned for each user sampled. | No exceptions noted. |
| A termination checklist is completed, logical access is revoked, and badges are disabled and collected by management within 24 hours as part of the termination process. | Inspected a listing of terminated employees and compared the listing to the active user listing to determine that terminated employees did not retain access to the in-scope system and platforms after their separation. | No exceptions noted. |
| Inspected termination tickets for a sample of employees terminated during the review period to determine that logical access was revoked and badges were disabled and collected by management within 24 hours as part of the termination process for each terminated employee sampled. | Exceptions noted. 2 of the 8 terminated employees sampled did not have their logical and physical access revoked within 24 hours of their termination date. |
| Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner. | Inspected access review documentation for a sample of quarters to determine that an access review was performed for in-scope system components quarterly and that tickets were created to remove inappropriate access. | Exception noted. Access review documentation for 1 out of 2 of the quarters sampled could not be provided. |
| A Separation of Duties (SOD) Matrix has been developed and separates the duties of individuals as necessary. | Inspected the SOD Matrix to determine that it was developed and outlined the separate duties of individuals as necessary. | No exceptions noted. |
| **CC6.4** | The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives. | | |
|  | The entrance to the data center is equipped with a mantrap that utilizes multiple doors to control user access into the data center. | Observed the data center entrance to determine that the data center was equipped with a mantrap that utilized multiple doors to control user access into the data center. | No exceptions noted. |
| Access control systems and closed-circuit television (CCTV) cameras are in place throughout the data center. | Observed access control methods to determine that access control systems and CCTV cameras were in place throughout the data center. | No exceptions noted. |
| Access to the in-scope data centers is controlled via multi-factor authentication (MFA), which includes a fingerprint scan and proximity radio frequency (RF) badge swipe prior to allowing entry. | Observed the in-scope data centers access procedures to determine that access to the in-scope data centers was controlled via MFA, which included a fingerprint scan and proximity RF badge swipe prior to allowing entry. | No exceptions noted. |
| Physical access requests are submitted by an employee's functional manager via a ServiceNow ticket and must be approved by the Cloud Shared Services (CSS) secure area owner. | Inspected ServiceNow tickets for a sample of users that received access to the data center to determine that a physical access request was submitted by the employee's functional manager via a ServiceNow ticket and approved by the CSS secure area owner for each user sampled. | No exceptions noted. |
| A termination checklist is completed, logical access is revoked, and badges are disabled and collected by management within 24 hours as part of the termination process. | Inspected a listing of terminated employees and compared the listing to the active user listing to determine that terminated employees did not retain access to the in-scope system and platforms after their separation. | No exceptions noted. |
| Inspected termination tickets for a sample of employees terminated during the review period to determine that logical access was revoked and badges were disabled and collected by management within 24 hours as part of the termination process for each terminated employee sampled. | Exceptions noted. 2 of the 8 terminated employees sampled did not have their logical and physical access revoked within 24 hours of their termination date. |
| Visitors are required to sign in with security, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas. | Observed the temporary physical access authorization process at each in-scope data center to determine that visitors were required to identify themselves, sign in as visitors, obtain a visitor badge, and be escorted while accessing the data center or secure areas. | No exceptions noted. |
| Physical visitor logs are reviewed at least monthly. This review is captured through a ServiceNow ticket. | Inspected ServiceNow tickets for a sample of months to determine that physical visitor logs were reviewed at least monthly. | No exceptions noted. |
| Physical access reviews are performed quarterly by the Information Assurance (IA) Compliance Officer and documented in a ServiceNow ticket. | Inspected ServiceNow tickets for a sample of quarters to determine that physical access reviews were performed quarterly by the IA Compliance Officer. | Exceptions noted. For 2 out of 2 quarters sampled, evidence of physical access reviews could not be provided. |
| Removable media is secured in locked cabinets behind a badge-accessed workspace. | Observed removable media storage procedures to determine that removable media was secured in locked cabinets behind a badge-accessed workspace. | No exceptions noted. |
| Backup tapes that are removed from the information system environment are stored in padlocked cases. | Observed padlocked cases to determine that backup tapes that were removed from the information system environment were stored in padlocked cases. | No exceptions noted. |
| **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. | | |
|  | All electronic equipment subject to removal or destruction must be tracked with a ServiceNow ticket and approved by the Change Advisory Board (CAB). Cleansing of drives and tapes shall be completed prior to removal from facilities information management system (FIMS) control. | Inspected certificates of destruction for a sample of media destroyed during the review period to determine that electronic media containing confidential information was purged or destroyed in accordance with best practices, and certificates of destruction were issued for each device destroyed. | No exceptions noted. |
| Removable media in digital format (tapes and hard drives) is only approved for sanitization through the employment of degaussing. | Inspected data disposal procedures to determine that removable media in digital format (tapes and hard drives) was only approved for sanitization through the employment of degaussing. | No exceptions noted. |
| Inspected sanitation evidence for a sample of sanitized media to determine that removable media in digital format (tapes and hard drives) was only approved for sanitization through the employment of degaussing. | No exceptions noted. |
| **CC6.6** | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | |
|  | Firewalls are used and configured to prevent unauthorized access. | Inspected the firewall configuration to determine that firewalls were in place and configured to prevent unauthorized access. | No exceptions noted. |
| TEST COMPANY has documented network and system hardening standards. | Inspected hardening standards to determine that they were documented. | No exceptions noted. |
| Infrastructure supporting the service is patched monthly to help ensure servers supporting the service are hardened against security threats. | Inspected ServiceNow tickets for a sample of months to determine that the infrastructure supporting the service was patched monthly to help ensure that servers supporting the service were hardened against security threats. | No exceptions noted. |
| TEST COMPANY restricts access to production systems to authorized employees with multi-factor authentication (MFA) over an encrypted virtual private network (VPN) connection. | Observed a remote login session to determine that MFA over an encrypted VPN connection was required to access the production network. | No exceptions 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. | | |
|  | TEST COMPANY restricts access to production systems to authorized employees with multi-factor authentication (MFA) over an encrypted virtual private network (VPN) connection. | Observed a remote login session to determine that MFA over an encrypted VPN connection was required to access the production network. | No exceptions noted |
| Backup tapes sent off-site are encrypted prior to being extracted from the tape drive. | Inspected backup tape encryption configurations to determine that backup tapes sent off-site were encrypted prior to being extracted from the tape drive. | No exceptions 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. | | |
|  | A security information event management (SIEM) system is utilized to identify trends that may have a potential impact on TEST COMPANY's ability to achieve its system security objectives. | Inspected SIEM system configurations to determine that a SIEM was utilized to identify trends that may have had a potential impact on TEST COMPANY's ability to achieve its system security objectives. | No exceptions noted. |
| Intrusion prevention systems are used to provide continuous monitoring of the SCG network and prevention of potential security breaches. | Inspected intrusion prevention system configurations to determine that continuous monitoring of the SCG network and prevention of potential security breaches was in place. | No exceptions noted. |
| Firewalls are used and configured to prevent unauthorized access. | Inspected the firewall configuration to determine that firewalls were in place and configured to prevent unauthorized access. | No exceptions noted. |
| TEST COMPANY has documented network and system hardening standards. | Inspected hardening standards to determine that they were documented. | No exceptions noted. |
| Infrastructure supporting the service is patched monthly to help ensure servers supporting the service are hardened against security threats. | Inspected ServiceNow tickets for a sample of months to determine that the infrastructure supporting the service was patched monthly to help ensure that servers supporting the service were hardened against security threats. | No exceptions noted. |
| TEST COMPANY has deployed anti-malware technology for environments commonly susceptible to malicious attack and has configured it to be updated routinely, logged, and installed on all relevant production servers. | Inspected screenshots of anti-malware software configurations to determine that it was configured to be updated routinely, logged, and installed on all relevant production servers. | No exceptions noted |

| **SYSTEM OPERATIONS** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **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. | | |
|  | Internal vulnerability scans for the SCG environment are performed at least monthly. A remediation plan is developed and changes are implemented to remediate all high and moderate vulnerabilities at a minimum. | Inspected internal vulnerability scans for a sample of months and remediation plans to determine that internal vulnerability scans were performed monthly and remediation plans were developed to remediate all high and moderate vulnerabilities at a minimum. | No exceptions noted. |
| Penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate all high and moderate vulnerabilities at a minimum. | Inspected the most recent penetration test report and remediation plan to determine that penetration testing occurred within the last year and a remediation plan was developed to remediate all high and moderate vulnerabilities at a minimum. | No exceptions noted. |
| A configuration management system is in place to ensure that system configurations are deployed consistently throughout the environment. | Inspected the configuration management system to determine that a system was in place and configurations were deployed consistently throughout the environment. | No exceptions noted. |
| TEST COMPANY has deployed anti-malware technology for environments commonly susceptible to malicious attack and has configured it to be updated routinely, logged, and installed on all relevant production servers. | Inspected screenshots of anti-malware software configurations to determine that it was configured to be updated routinely, logged, and installed on all relevant production servers. | No exceptions noted |
| The SCG receives alerts, advisories, and directives in the Security Intelligence and Operations Center (SIOC) mailbox from industry standard sources (e.g., United States Computer Emergency Readiness Team [US-CERT], SANS Institute, National Institute of Standards and Technology [NIST], Microsoft, Cisco) that are relevant to system security. | Inspected example alerts, advisories, and directives to determine that the SIOC mailbox received alerts from industry standard sources (e.g., US-CERT, SANS Institute, NIST, Microsoft, and Cisco) that were relevant to system security. | No exceptions noted. |
| Infrastructure supporting the service is patched monthly to help ensure servers supporting the service are hardened against security threats. | Inspected ServiceNow tickets for a sample of months to determine that the infrastructure supporting the service was patched monthly to help ensure that servers supporting the service were hardened against security threats. | No exceptions 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. | | |
|  | An information technology (IT) infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific, predefined thresholds are met. | Inspected IT infrastructure monitoring tool configurations and an example notification to determine that IT infrastructure monitoring tools were utilized to monitor IT infrastructure availability and performance and generated alerts when specific, predefined thresholds were met. | No exceptions noted. |
| Environmental monitoring devices are in place and configured to automatically generate an alert to management of environmental incidents. | Inspected the environmental monitoring tool configuration and alert dashboard to determine that the monitoring tools were configured to generate alerts for environmental incidents. | No exceptions noted. |
| A security information event management (SIEM) system is utilized to identify trends that may have a potential impact on TEST COMPANY's ability to achieve its system security objectives. | Inspected SIEM system configurations to determine that a SIEM was utilized to identify trends that may have had a potential impact on TEST COMPANY's ability to achieve its system security objectives. | No exceptions noted. |
| Intrusion prevention systems are used to provide continuous monitoring of the SCG network and prevention of potential security breaches. | Inspected intrusion prevention system configurations to determine that continuous monitoring of the SCG network and prevention of potential security breaches was in place. | No exceptions noted. |
| TEST COMPANY has deployed anti-malware technology for environments commonly susceptible to malicious attack and has configured it to be updated routinely, logged, and installed on all relevant production servers. | Inspected screenshots of anti-malware software configurations to determine that it was configured to be updated routinely, logged, and installed on all relevant production servers. | No exceptions 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. | | |
|  | TEST COMPANY has developed and distributed the security incident policies and procedures that are communicated to authorized users. | Inspected the security incident response policies and procedures to determine that they were developed. | No exceptions noted. |
| Observed ServiceNow to determine that security incident policies and procedures were communicated to authorized users. | No exceptions noted. |
| A security information event management (SIEM) system is utilized to identify trends that may have a potential impact on TEST COMPANY's ability to achieve its system security objectives. | Inspected SIEM system configurations to determine that a SIEM was utilized to identify trends that may have had a potential impact on TEST COMPANY's ability to achieve its system security objectives. | No exceptions noted. |
| All events related to security, availability, and confidentiality are logged, tracked, and communicated to affected parties by management until resolved. | Inspected a sample of IT security, availability, and confidentiality event tickets to determine that security events were logged, tracked, and communicated to affected parties by management until resolved. | No exceptions 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. | | |
|  | TEST COMPANY has developed and distributed the security incident policies and procedures that are communicated to authorized users. | Inspected the security incident response policies and procedures to determine that they were developed. | No exceptions noted. |
| Observed ServiceNow to determine that security incident policies and procedures were communicated to authorized users. | No exceptions noted. |
| TEST COMPANY provides a service desk that allows users to report system information on failures, incidents, concerns, and other complaints to the appropriate personnel. | Observed the service desk to determine that TEST COMPANY provided a service desk that allowed users to report system information on failures, incidents, concerns, and other complaints to the appropriate personnel. | No exceptions noted. |
| All incidents related to security, availability, and confidentiality are logged, tracked, and communicated to affected parties by management until resolved.  The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the review period. | Inquired of management and inspected security, availability, and confidentiality incident review documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. | Not tested. No incidents related to security occurred during the period. |
| Security incident response training and testing is completed at least annually. | Inspected the most recent incident response training and testing to determine that it was performed within the past year. | No exceptions noted. |
| **CC7.5** | The entity identifies, develops, and implements activities to recover from identified security incidents. | | |
|  | TEST COMPANY has developed and distributed the security incident policies and procedures that are communicated to authorized users. | Inspected the security incident response policies and procedures to determine that they were developed. | No exceptions noted. |
| Observed ServiceNow to determine that security incident policies and procedures were communicated to authorized users. | No exceptions noted. |
| All incidents related to security, availability, and confidentiality are logged, tracked, and communicated to affected parties by management until resolved.  The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the review period. | Inquired of management and inspected security, availability, and confidentiality incident review documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. | Not tested. No incidents related to security occurred during the period. |
| A documented Contingency Plan (CP) is in place and made available to key personnel. | Inspected the CP to determine that it was documented and made available to key personnel. | No exceptions noted. |

| **CHANGE MANAGEMENT** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **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. | | |
|  | A configuration management system is in place to ensure that system configurations are deployed consistently throughout the environment. | Inspected the configuration management system to determine that a system was in place and configurations were deployed consistently throughout the environment. | No exceptions noted. |
| Formally documented change management procedures are in place to govern the modification and maintenance of production systems and address security, availability, and confidentiality requirements. | Inspected the change management procedures to determine that procedures were in place to govern the modification and maintenance of production systems and addressed security, availability, and confidentiality requirements. | No exceptions noted. |
| The TEST COMPANY change management process requires that changes made to the production system are: - Authorized - Formally documented  - Categorized based on change risk - Included in a backout plan (if applicable) - Tested prior to migration to production (if applicable) - Approved by the CAB for comprehensive changes prior to implementation - Approved by the Technical Manager for routine changes prior to implementation | Inspected change request tickets for a sample of production system changes that occurred during the review period to determine that production change requests were: - Authorized - Formally documented  - Categorized based on change risk - Included in a backout plan - Tested prior to migration to production - Approved by the CAB for comprehensive changes prior to implementation - Approved by the Technical Manager for routine changes prior to implementation | No exceptions noted. |
| The TEST COMPANY emergency change management process requires that emergency changes made to the production system are: -Authorized -Formally documented  -Categorized based on change risk -Included in a backout plan (if applicable) -Tested prior to migration to production (if applicable) -Approved by the CAB (initial approval may be verbal; however, it must be documented after the emergency change is implemented) | Inspected change request tickets for a sample of emergency changes to the production system that occurred during the review period to determine that emergency change requests were: -Authorized -Formally documented  -Categorized based on change risk -Included in a backout plan -Tested prior to migration to production -Approved by the CAB (initial approval may be verbal; however, it must be documented after the emergency change is implemented) | No exceptions noted. |

| **RISK MITIGATION** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **CC9.1** | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | |
|  | A documented Contingency Plan (CP) is in place and made available to key personnel. | Inspected the CP to determine that it was documented and made available to key personnel. | No exceptions noted. |
| TEST COMPANY has developed and distributed the security incident policies and procedures that are communicated to authorized users. | Inspected the security incident response policies and procedures to determine that they were developed. | No exceptions noted. |
| Observed ServiceNow to determine that security incident policies and procedures were communicated to authorized users. | No exceptions noted. |
| Backup procedures are documented to address the risk that interruption of service is minimized. The procedure requires daily and weekly backups of data and all operating software. | Inspected backup procedures to determine that backup procedures were documented to address the risk that interruption of service was minimized and that the procedure required daily and weekly backups of data and all operating software. | No exceptions noted. |
| TEST COMPANY uses a multi-location strategy for its facilities to permit the resumption of operations at other TEST COMPANY facilities in the event of the loss of a facility. | Inspected evidence of redundant data centers to determine that TEST COMPANY used a multi-location strategy for its facilities to permit the resumption of operations at other TEST COMPANY facilities in the event of the loss of a facility. | No exceptions noted. |
| A documented risk management program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | Inspected the risk management program to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. | No exceptions noted. |
| Risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. | Inspected the most recent risk assessment to determine that a risk assessment was performed within the past year and, as part of this process, threats and changes to service commitments were identified, the risks were formally assessed, and the risk assessments included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |
| All POA&Ms are reviewed at least quarterly by the Senior Information Security Officer (SISO) with the System Owner (SO), Lead Information Officer (LIO), and AO via a standing meeting. | Inspected POA&M review documentation for sample of quarters to determine that all POA&Ms were reviewed at least quarterly by the SISO with the SO, LIO, and AO via a standing meeting. | No exceptions noted. |
| **CC9.2** | The entity assesses and manages risks associated with vendors and business partners. | | |
|  | Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. | Inspected contracts for a sample of vendors to determine that formal information sharing agreements were in place and included confidentiality commitments for each vendor sampled. | No exceptions noted. |
| A list of subservice organizations and critical vendors is maintained and those parties are required to maintain their own security practices and procedures. Conformance is assessed annually by reviewing third-party attestation reports or performing a vendor risk assessment. | Inspected third-party attestation reports or vendor risk assessment documentation for a sample of vendors to determine that a third-party attestation report or risk assessment was performed within the past year for each vendor sampled. | No exceptions noted. |

additional criteria for Availability

| **AVAILABILITY** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **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. | | |
|  | An information technology (IT) infrastructure monitoring tool is utilized to monitor IT infrastructure availability and performance and generates alerts when specific, predefined thresholds are met. | Inspected IT infrastructure monitoring tool configurations and an example notification to determine that IT infrastructure monitoring tools were utilized to monitor IT infrastructure availability and performance and generated alerts when specific, predefined thresholds were met. | No exceptions noted. |
| Environmental monitoring devices are in place and configured to automatically generate an alert to management of environmental incidents. | Inspected the environmental monitoring tool configuration and alert dashboard to determine that the monitoring tools were configured to generate alerts for environmental incidents. | No exceptions noted. |
| **A1.2** | The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives. | | |
|  | Environmental monitoring devices are in place and configured to automatically generate an alert to management of environmental incidents. | Inspected the environmental monitoring tool configuration and alert dashboard to determine that the monitoring tools were configured to generate alerts for environmental incidents. | No exceptions noted. |
| TEST COMPANY has implemented environmental security measures in the data center that include a Very Early Smoke Detection Apparatus (VESDA); Heating, Ventilation, and Air Conditioning (HVAC) systems; a fire suppression system; water detectors installed within the raised floor areas; uninterruptible power supplies; and emergency power supplies. | Observed the data center and inspected controlled areas to determine that TEST COMPANY had implemented environmental security measures in the data center that included a VESDA, HVAC systems, a fire suppression system, water detectors installed within the raised floor areas, uninterruptible power supplies, and emergency power supplies. | No exceptions noted. |
| Maintenance inspections of fire suppression devices and smoke detectors at TEST COMPANY's data centers are performed at least annually. | Inspected facility maintenance records of fire suppression devices and smoke detectors at each of the in-scope data centers to determine that maintenance occurred within the past year. | Exception noted. Maintenance inspections were not performed during the review period due to the COVID-19 pandemic. |
| Maintenance inspections of backup generators, HVAC units, and uninterruptible power supply (UPS) units are performed at least annually. | Inspected facility maintenance records of backup generators, HVAC units, and UPS units at each of the in-scope data centers to determine that maintenance occurred within the past year. | Exception noted. Maintenance inspections were not performed during the review period due to the COVID-19 pandemic. |
| Backup procedures are documented to address the risk that interruption of service is minimized. The procedure requires daily and weekly backups of data and all operating software. | Inspected backup procedures to determine that backup procedures were documented to address the risk that interruption of service was minimized and that the procedure required daily and weekly backups of data and all operating software. | No exceptions noted. |
| Daily incremental backups are configured for data and all OSs. | Observed the backup configuration to determine that daily incremental backups were configured for data and all OSs. | No exceptions noted. |
| Backup tapes are moved to an offsite location weekly. | Inspected backup tape rotation evidence for a sample of weeks to determine that backup tapes were moved to an offsite location weekly. | No exceptions noted. |
| TEST COMPANY uses a multi-location strategy for its facilities to permit the resumption of operations at other TEST COMPANY facilities in the event of the loss of a facility. | Inspected evidence of redundant data centers to determine that TEST COMPANY used a multi-location strategy for its facilities to permit the resumption of operations at other TEST COMPANY facilities in the event of the loss of a facility. | No exceptions noted. |
| **A1.3** | The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | |
|  | A CP test is performed at least annually. After each test or exercise, a post mortem is completed and lessons learned are incorporated into the CP. | Inspected the most recent CP test to determine that a CP test was performed within the past year, a post mortem was completed, and lessons learned were incorporated into the CP. | No exceptions noted. |
| TEST COMPANY tests the restoration of data at least monthly to verify media reliability and information integrity. | Inspected the data restoration test evidence for a sample of months to determine that a data restoration test to verify media reliability and information integrity was performed at least monthly. | No exceptions noted. |

additional criteria for confidentiality

| **CONFIDENTIALITY** | | | |
| --- | --- | --- | --- |
|  | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor’s Tests** | **Results of Tests** |
| **C1.1** | The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality. | | |
|  | A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel. | Inspected the data classification policy to determine that policies existed around ensuring that confidential data was properly secured and restricted to authorized personnel. | No exceptions noted. |
| Employees are required to sign a confidentiality agreement as a routine part of their employment. This agreement prohibits any disclosures of information and other data to which the employee has been granted access. | Inspected the confidentiality agreement to determine that it prohibited the disclosure of information and other data to which the employee had been granted access. | No exceptions noted. |
| Inspected signed confidentiality agreements for a sample of new hires to determine that new hires were provided and accepted the agreement. | No exceptions noted. |
| Formal information sharing agreements are in place with related parties and vendors. These agreements include confidentiality commitments applicable to that entity. | Inspected contracts for a sample of vendors to determine that formal information sharing agreements were in place and included confidentiality commitments for each vendor sampled. | No exceptions noted. |
| **C1.2** | The entity disposes of confidential information to meet the entity’s objectives related to confidentiality. | | |
|  | All electronic equipment subject to removal or destruction must be tracked with a ServiceNow ticket and approved by the Change Advisory Board (CAB). Cleansing of drives and tapes shall be completed prior to removal from facilities information management system (FIMS) control. | Inspected certificates of destruction for a sample of media destroyed during the review period to determine that electronic media containing confidential information was purged or destroyed in accordance with best practices, and certificates of destruction were issued for each device destroyed. | No exceptions noted. |
| Removable media in digital format (tapes and hard drives) is only approved for sanitization through the employment of degaussing. | Inspected data disposal procedures to determine that removable media in digital format (tapes and hard drives) was only approved for sanitization through the employment of degaussing. | No exceptions noted. |
| Inspected sanitation evidence for a sample of sanitized media to determine that removable media in digital format (tapes and hard drives) was only approved for sanitization through the employment of degaussing. | No exceptions noted. |