



SOC 2 REPORT

FOR

DATA CENTER AND CLOUD OPERATIONS

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS
RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

NOVEMBER 1, 2022, TO OCTOBER 31, 2023

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

This report is intended solely for use by the management of Flexential Corp., user entities of Flexential Corp.'s services, and other parties who have sufficient knowledge and understanding of Flexential Corp.'s services covered by this report (each referred to herein as a "specified user").

If the report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2	MANAGEMENT'S ASSERTION	5
SECTION 3	DESCRIPTION OF THE SYSTEM	7
SECTION 4	TESTING MATRICES	28
SECTION 5	OTHER INFORMATION PROVIDED BY FLEXENTIAL	85

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Flexential Corp.:

Scope

We have examined Flexential Corp.'s ("Flexential" or the "service organization") accompanying description of its Data Center and Cloud Operations system, in Section 3, throughout the period November 1, 2022, to October 31, 2023, (the "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 November 1, 2022, to October 31, 2023, to provide reasonable assurance that Flexential's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Flexential uses Equinix as a subservice organization for data center colocation services to house hardware and infrastructure to deliver cloud operations services in Europe. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Flexential, to achieve Flexential's service commitments and system requirements based on the applicable trust services criteria. The description presents Flexential's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Flexential's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section 5, "Other Information Provided by Flexential" is presented by Flexential management to provide additional information and is not a part of the description. Information about Flexential's management's responses to exceptions noted has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Flexential's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

Flexential 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 Flexential's service commitments and system requirements were achieved. Flexential has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Flexential 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 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 (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. 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 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.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement, including the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report 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 risk 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 Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects:

- a. the description presents Flexential's Data Center and Cloud Operations system that was designed and implemented throughout the period November 1, 2022, to October 31, 2023, in accordance with the description criteria;

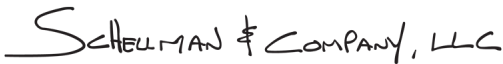
- b. the controls stated in the description were suitably designed throughout the period [November 1, 2022, to October 31, 2023, to provide reasonable assurance that Flexential's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and the user entities applied the complementary controls assumed in the design of Flexential's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that Flexential's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and user entity controls assumed in the design of Flexential's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Flexential; user entities of Flexential's Data Center and Cloud Operations system during some or all of the period of November 1, 2022, to October 31, 2023, business partners of Flexential subject to risks arising from interactions with the Data Center and Cloud Operations system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators 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 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; and
- 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 these specified parties.

 SCHEELMAN & COMPANY, LLC

Columbus, Ohio
December 8, 2023

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Flexential's Data Center and Cloud Operations system, in Section 3, throughout the period November 1, 2022, to October 31, 2023, (the "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"). The description is intended to provide report users with information about the Data Center and Cloud Operations system that may be useful when assessing the risks arising from interactions with Flexential's system, particularly information about system controls that Flexential 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, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Flexential uses Equinix as a subservice organization for data center colocation services to house hardware and infrastructure to deliver cloud operations services in Europe. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Flexential, to achieve Flexential's service commitments and system requirements based on the applicable trust services criteria. The description presents Flexential's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Flexential's controls. The description does not disclose the actual controls at the subservice organization.

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

- a. the description presents Flexential's Data Center and Cloud Operations system that was designed and implemented throughout the period November 1, 2022, to October 31, 2023, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that Flexential'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 the user entities applied the complementary controls assumed in the design of Flexential's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period November 1, 2022, to October 31, 2023, to provide reasonable assurance that Flexential's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and user entity controls assumed in the design of Flexential's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Flexential was founded in 2017 through the combination of ViaWest Inc. (originally founded in 1999 and headquartered in Denver, Colorado) and Peak 10 (originally founded in 2000 and headquartered in Charlotte, North Carolina). Flexential currently employs approximately 870 employees across the United States. Flexential maintains two headquarters locations in Charlotte, North Carolina, and Denver, Colorado. The executive management team consists of industry leaders with experience in information technology (IT) services and data center operations.

Description of Services Provided

Flexential's colocation services is provided in 19 geographic markets, across locations within the United States. With 39 physical data center locations and growing, Flexential operates raised floor gross square footage of well over 1 million square feet. Technical assistance and operational staff provide monitoring and customer support 24x7x365. Colocation services include white floor space with dedicated and secure cabinets and cages, redundant power, and critical infrastructure (uninterruptible power supply (UPS), cooling, fire prevention), physical security, and network connectivity / redundant telecommunication and bandwidth services. The company combines its nationwide data center footprint with its portfolio of cloud and managed services, to provide flexible hybrid IT services to customers throughout North America.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Flexential designs its processes and procedures related to Data Center and Cloud Operations system to meet its objectives for providing Data Center and Cloud Operations services. Those objectives are based on the service commitments that Flexential makes to user entities, the laws and regulations that govern the provision of the Data Center and Cloud Operations system, and the operational, and compliance requirements that Flexential has established for the services. The Data Center and Cloud Operations of Flexential are subject to the state privacy security laws and regulations in the jurisdictions in which Flexential operates.

Flexential's commitments regarding security, availability, and confidentiality are documented and communicated to internal and external users via policies and procedures and customer Service Level Agreements (SLAs). In addition, policies and procedures are communicated and acknowledged by the internal user community via company Human Resource Information System (HRIS) and embedded within Flexential's Compliance Management Program and control activities.

Security, availability, and confidentiality commitments to user entities are documented and communicated in SLAs as well as in the description of the service offering provided online. The principal security, availability and confidentiality commitments are standardized and includes the following:

- the use of physical and logical access controls to safeguard the storage of client data within the system boundaries and restrict access to sensitive resources;
- the maintenance of the information security program including Flexential's infrastructure, technical controls, processes, policies, and certifications;
- a comprehensive and flexible disaster recovery solution;
- 24x7x365 surveillance monitoring at data centers;
- the development, testing, and maintenance of business continuity plans for critical functions; and
- the retention and destruction of confidential data in accordance with Flexential's policies.

Flexential has also established system requirements that support the achievement of the principal service commitments. These requirements include the following:

- the use of encryption technologies to protect system user data both at rest and in transit;
- role-based access control with the principal of least privilege;
- the use of firewalls to protect its network from the internet;
- system monitoring to detect inappropriate behavior on the network;
- change management procedures to support the requisite authorization, documentation, testing, and approval of changes;
- availability monitoring applications are in place to monitor the capacity and performance levels of systems supporting the services and alert operations personnel when predefined thresholds are exceeded; and
- environmental monitoring systems are equipped to monitor the environmental systems and conditions within the data centers.

Such requirements are communicated in Flexential's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Data Center and Cloud Operations.

The aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

The scope of this report includes the Data Center and Cloud Operations system performed for the following facilities:

Data Center	Address
1. Charlotte - North	10105 David Taylor Drive, Charlotte, NC, 28262
2. Charlotte - South	8910 Lenox Pointe Drive, Suites A, G, Charlotte, NC 28273
3. Raleigh	5150 McCrimmon Parkway, Morrisville, NC 27560
4. Phoenix - Deer Valley	1850 W. Deer Valley Road, Phoenix, AZ 85027
5. Denver - Aurora	11900 E Cornell Avenue, Suite A, Aurora, CO 80014
6. Denver - Downtown	1500 Champa Street, Suite 100, Denver, CO 80202
7. Denver - Centennial	12500 E Arapahoe Road, Suite C, Centennial, CO 80112
8. Denver - Englewood	8636 South Peoria Street, Englewood, CO 80112

Data Center	Address
9. Jacksonville	4905 Belfort Road, Suite 145, Jacksonville, FL 32256
10. Fort Lauderdale	5301 NW 33rd Avenue, Fort Lauderdale, FL 33309
11. Tampa - North	8350 Parkedge Drive, Tampa, FL, 33637
12. Tampa – West	9417 Corporate Lake Drive, Tampa, FL 33634
13. Atlanta - Alpharetta	12655 Edison Drive, Alpharetta, GA, 30005
14. Atlanta - Norcross	2775 Northwoods Parkway, Norcross, GA 30071
15. Louisville - East	2101 Nelson Miller Parkway, Louisville, KY 40223
16. Louisville - Downtown	752 Barret Avenue, Louisville, KY 40204
17. Minneapolis - Chaska	3500 Lyman Boulevard, Chaska, MN 55318
18. Las Vegas - Downtown	302 Carson Avenue, Suite 100, Las Vegas, NV 89101
19. Las Vegas - Downtown	304 Carson Avenue, Suite 370, Las Vegas, NV 89101
20. Las Vegas - North	3330 E Lone Mountain Road, North Las Vegas, NV 89081
21. Cincinnati	5307 Muhlhauser Road, West Chester Township, OH 45011
22. Portland – Hillsboro 1	3935 NW Aloclek Place, Building C, Hillsboro, OR 97124
23. Portland – Hillsboro 2	5737 NE Huffman Street, Hillsboro OR 97124
24. Portland – Hillsboro 3	5419 NE Starr Boulevard, Hillsboro, OR 97124
25. Portland – Hillsboro 4	4915 NE Starr Blvd, Hillsboro, OR 97124
26. Allentown*	744 Roble Road, Allentown, PA 18109
27. Collegeville	101 Troutman Road, Collegeville, PA 19426
28. Nashville – Cool Springs	425 Duke Drive, Suite 400, Franklin, TN 37067
29. Nashville – Franklin	4600 Carothers Parkway, Franklin, TN 37067
30. Nashville – Brentwood	7100 Commerce Way, Brentwood, TN 37027
31. Dallas – Downtown	1950 N Stemmons Freeway, Dallas, TX 75207
32. Dallas – Plano	3500 E Plano Parkway, Plano, TX 75074
33. Dallas - Richardson	3010 Waterview Parkway, Richardson, TX 75080
34. Salt Lake City – South Valley	7202 S Campus View Drive, West Jordan, UT 84084
35. Salt Lake City – Lindon*	333 S 520 W, Lindon, UT 84042
36. Salt Lake City – Millcreek	3949 S 200 E, Murray, UT 84107
37. Salt Lake City – Downtown	572 Delong Street, Suite 100, Salt Lake City, UT 84104
38. Salt Lake City – Fair Park*	118 S 1000 W, Salt Lake City, UT 84104
39. Richmond	8851 Park Central Drive, Richmond, VA 23227

** Note: The denoted data center sites are staffed Monday – Friday, 8AM - 5PM, and is monitored remotely 24x7x365. Staff are on-call 24/7 for remote hands requirements.*

Infrastructure

The in-scope infrastructure consists of multiple applications, operating system and platforms, as shown in the table below:

Primary Infrastructure		
Components	Type	Purpose
Badge card access system	Entrapass, Genetec, C-Cure, Velocity	The badge card access system is utilized in conjunction with the biometric recognition access system to control access to the greater data center facilities and the raised floor within the datacenter facilities.
Biometric recognition access system	BioStar, BioConnect	The biometric recognition access system is utilized in conjunction with the badge card access system to verify identity with two factor authentication prior to granting access to the datacenter facilities and the raised floor within the data center facilities.
Closed Circuit Television (CCTV)/Video	ExacqVision, Genetec	The CCTV system utilized in conjunction with the badge card access system to provide video coverage of entry/exit points and secure areas within the data center facility.
Firewalls	Fortigate FortiOS	Corporate firewalls are utilized to restrict traffic into the management network, and service delivery firewalls are utilized to filter and route traffic for customer-specific environments.
Intrusion Prevention & Detection System	Fortigate	Enterprise intrusion prevention system/intrusion detection system (IPS)/(IDS) tooling to prevent and detect potential external threats to Flexential systems and network that is integrated within Flexential's SIEM (Security Incident Event Management) tooling and capabilities.
Backup system	CommVault	Automated backup system software and network of servers that provide backup and recovery.
Routers and switches	Arista, Ciena, Cisco, FortiNet, Juniper, Smartoptics	Routers, switches, and optical transport are utilized to route network traffic.
Virtual hypervisor	VMware vCenter	VMware vCenter server that provides authentication and restricts access to customer virtual environments.
VMware hosts	VMware (ESXi)	VMware ESX hosts for running customer virtual machines.
Web portals	Embotics vCommander, Flexential Customer Portal (CommVault portal, Zerto portal, Cloud Fabric, vCloud, MyCloud)	Customer portal system, through which customers manage their virtual machines.

People

Flexential utilizes the following functional areas of operations to support the Data Center and Cloud Operations system:

- Executive management – responsible for organizing and overseeing activities, accomplishing goals, and overseeing objectives in an efficient and effective manner.
- Managed services – responsible for managing and protecting users' information and systems from unauthorized access and use while maintaining integrity and availability.
- Engineering – responsible for specifying, deploying, and maintaining infrastructure systems, security, and support for user entities.
- Professional services – responsible for providing user entities with assistance before and after the initial sale by providing information, guidance, delivering goods, and continued support.
- Marketing – responsible for marketing and sales functions.
- Operations – responsible for maintaining and operating data center infrastructure and user entities' information technology environments in an efficient manner through the use of staff, resources, facilities, and business solutions.
- Physical Security – responsible for the design, development, implementation, and management of Flexential's physical security policies, programs and controls.
- Information Security – responsible for the design, development, implementation, and management of Flexential's information and cybersecurity policies, programs and controls.

Procedures

Access, Authentication, and Authorization

Formal IT policies and procedures exist that describe the logical access standard. Employees are expected to adhere to Flexential's policies and procedures that define how services should be delivered. These are located on the company's intranet and can be accessed by authorized personnel.

Access to network devices is controlled by the implementation of access control lists (ACLs) that limit where connections can be made from. Users authenticate to the network devices using Terminal Access Controller Access-Control System (TACACS+), which leverages Active Directory (AD) group membership to define permission levels in network devices, which are restricted by different group tier assignments. The user must also be defined to a specific group within TACACS+ in order to administer network devices. Authentication to TACACS+ is controlled by AD. Access for a group tier is requested based on the necessity of the job function and must be approved by the employee's manager before access is granted. FortiClient is used for multi-factor authentication (MFA) to network devices. Users have unique usernames and FortiTokens which change at a fixed interval of 30 seconds.

Administrative access to network devices is commensurate with job function and is limited to the engineering and operational support teams. In order to access the network devices, Flexential has created ACLs on each device to allow only certain internet protocol (IP) addresses to connect to the device.

Flexential has implemented logical security controls to restrict access to customer networks and data. When customers call or login online to request support services, Flexential Service Support (FSS) or Technical Assistance Center (TAC) personnel use a series of secret questions and answers to authenticate the user. The automated service management system is configured to store these customer-specific questions.

Access Requests and Access Revocation

Employees have access to Flexential systems, applications, and network devices, with access-level restrictions based on specific job functions that the user performs for Flexential. New access to the network is initiated by the hiring manager. HR provides the hiring manager with the new employee setup form to fill out and submit to the

technology services department and an onboarding ticket is generated. Access rights are assigned based on the function/role identified on the new employee setup form.

Requests for user access modifications is initiated by the employee's manager by submitting the employee role change form to the technology services department and a ticket is generated. Access rights are modified based on the function/role identified on the employee role change form.

The employee's manager initiates the employee termination process by alerting the HR department using the HRIS. HR then approves the termination which creates a parent ticket in the service management system. Child tickets are generated from the parent ticket that are assigned to relevant departments to revoke access from the corporate domain and Flexential facilities, networks, network devices, and systems. Upon account deactivation, single sign-on (SSO) and group-based access is terminated. The HR department and/or the employee's manager conducts an exit interview with the terminated employee and collects Flexential assets.

To help ensure that access to systems, applications, and network devices remains authorized, over time key personnel perform logical access reviews on users who have access to the corporate domain and network devices. This review consists of inspecting the entire user base to verify that no terminated employees have access to the systems and to verify that users' current access rights are still required based on job changes or roles they are currently fulfilling within the organization. Any exceptions identified by management are sent to the system administrators of the respective systems for resolution, and the changed access lists are revalidated for completion of the review by management.

New customer environments within the Flexential data center facilities are required to meet standards set by management. Those standards are based on mutually agreed upon criteria and contractual obligations. Provisioning policies and procedures are documented to guide the provisioning process in new customer implementation and maintenance activities that include, but are not limited to, the following:

- Developing a customer profile within Salesforce and order records within the service management system.
- Creating project tasks and milestones and assigning sub-tasks.
- Project management monitoring and completion task responsibilities.
- Managing changes to customer implementation order.

Procedures for customer implementation tasks and resolution of issues are facilitated by the provisioning personnel. Standard build procedures are maintained to guide the customer implementation process. The build procedures include tasks for installation and maintenance of the following:

- Active Directory
- Server installation
- Domain setup
- Windows installation
- Certificates
- Virtual Private Networks (VPNs)
- Service applications

Provisioning personnel are in place to oversee new customer implementation tasks and facilitate the resolution of any implementation issues.

Customer environment requirements are documented within standard agreements and forms. Master service agreements are in place with customers that define the terms of services provided. The master services agreements include the nature, timing and extent of services provided, escalation procedures, roles and responsibilities, service warranties, and SLAs. Prior to implementation, customers are also required to review and sign the master services agreement which includes the pricing and description of subscribed services as well as the service level agreement. Standard implementation information forms are utilized by provisioning personnel to define customer and technical requirements for newly requested services.

In addition to the standard agreements and forms, a service order management module within the service management system is utilized to document and maintain customer implementation initiation and activity progress. The customer implementation project manager creates a request in the service management system to provision

the new customer environment and assigns and monitors the completion of each sub-task (or request item) via the service management system dashboard to ensure that customer requirements have been fulfilled.

Physical Security

Physical security of the data centers is the responsibility of data center and facility support personnel, along with coordination with the security team and senior management. Physical access to Flexential locations is monitored by operational personnel 24x7x365.

Flexential data center facilities employ physical security controls to help ensure that only authorized personnel access the data centers. Documented physical security policies and procedures are in place to guide personnel in physical security administration as well as vendor administration procedures. Each data center facility is equipped with two separate two-factor authentication systems to control access. A Flexential badge is required to enter the buildings while a badge and personal identification number (PIN) code, or a badge and biometric fingerprint scan, are required to enter the data center rooms. After successful authentication into the data center raised floor area, there are additional physical security controls that are required to access the customer's equipment using another lock and key, badge, PIN, or biometric reader. Each customer is allocated their own space through the use of secured racks, cages, or suites. There are no exterior facing windows in the walls of the areas where client production servers are located.

Badge access is monitored through various systems, and administrator privileges are restricted to user accounts accessible by authorized operational personnel. Badge access privileges of terminated employees are revoked as a component of the employee termination process. Management performs an access review of terminated employees on a quarterly basis.

Visitors are required to sign in at the front desk prior to entering Flexential facilities and must be accompanied and supervised by a Flexential employee or an authorized client escort. Visitors are also required to wear a visitor badge while in Flexential facilities at all times. Visitor badges do not allow unescorted access to the facility or data centers. TAC personnel are staffed at the data center facilities to log visitor access and monitor the digital surveillance systems at the data centers on a 24 hour basis.. Vendors must sign and acknowledge a vendor accountability form in order to begin performing maintenance within the data centers.

Flexential data center facility physical access activity is monitored through various monitoring systems. Each Flexential data center facility has security cameras installed to monitor and record physical access events.

Data is recorded based on activity/motion with the minimum data retention period for certain areas of 90 days. Data center facility doors also have monitoring systems in place to alert facilities personnel regarding doors that remain open too long, doors that are forced open, or doors that are opened that should remain closed. Camera activity is fed to the TAC and monitored by facility personnel. Data center personnel at each data center perform facility rounds daily to physically inspect each data center's building exterior, docks, storage facilities, security cameras, and security systems. This helps to ensure that physical security systems are operating as designed.

Change Management

Policies and procedures are in place to guide personnel in documenting, scheduling, and performing infrastructure changes and maintenance activities. Changes related to facility and environmental systems and IT infrastructure that are known to, or have the potential to, affect customer services are placed in a scheduled change window. Routine activities are excluded from Flexential's change management process; the list of defined routine activities are pre-approved by the Change Advisory Board (CAB). Any change to Flexential systems or infrastructure, including additions, deletions, or modifications, are required to follow the change management guidelines.

Operations and support personnel utilize the service management system to centrally track infrastructure change requests and maintenance activities. Information security is a key factor in assessing risk. Flexential has configured the risk assessment matrix within the service management system to measure complexity and impact to conduct the risk evaluation process. The tool will require change records to undergo risk assessment before submission. Reviewers and approvers of proposed changes will consider the impact to Flexential's information security when assessing the potential risk of a change.

Infrastructure and maintenance activities are determined by the rated risk and listed type of the following change:

- Standard – low risk changes that are pre-approved. Standard change definitions are reviewed annually by the CAB and will be updated accordingly during the review.
- Low risk and normal – low risk normal changes do not require a second level of review or approval.
- Low risk and emergency – emergency changes require a second level CAB approval by the change manager. The change manager may provide an ad hoc review or conduct a review in the weekly CAB session.
- Medium risk (normal /emergency) – medium risk changes (other than standard) always require a second level CAB approval by the change manager. The change manager may provide an ad-hoc review or conduct a review in the weekly CAB session.
- High risk (normal /emergency) – high risk changes (other than standard) always require a second level CAB approval. Where time allows the change manager will seek to conduct a review in the weekly CAB session, but work may need to be completed before this approval can be documented. The change manager may provide an ad-hoc review.
- Flexential-initiated (any risk rating) – Flexential-initiated change types do not require second level review. Instead, these change types require confirmation that the change event schedule has been approved by the impacted customer.

A CAB meets weekly to review and approve changes, and each change ticket is evaluated on a case-by-case basis for the desired scheduling timeframe. A standard change record only requires management review/approval if it encounters a conflict and needs a conflict-override. Changes will be implemented in accordance with the Methods of Procedure and Standard Operating Procedures (MOP/SOP) and will be documented in such a way as to provide affected parties with the information required to evaluate the impact/results of the change and to successfully carry out the assigned functions following the change. The development and test environments are physically and logically separated from the production environment. Flexential creates test data that replaces confidential information with test information during the change management process to ensure customer data is not used for testing changes. The ability to implement changes into the production environment is restricted to user accounts accessible by authorized personnel.

Data Backup and Disaster Recovery

As part of the Flexential managed service solutions, an automated backup system is available for subscribing customers. A default backup configuration is utilized to perform system backups (full weekly and daily incremental backups). The backup system status notifications are available for subscribing customers through the web portal. A backup restoration is performed as a component of the business operations. Flexential has policies and procedures in place related to disaster recovery and the management of emergency situations. This plan is tested on an annual basis. An emergency is defined as: any unplanned event that causes or has the potential to cause deaths or significant injuries to employees, customers, or the public; or that can significantly disrupt operations, cause physical or environmental damage, or threaten Flexential's financial standing or public image. The term "disaster" is deliberately not used within Flexential's policies and procedures document to avoid confusion with large-scale natural events or the overwhelming image it portrays.

The incident command system (ICS) methodology is outlined for Flexential's employees for responding to emergency situations. Flexential uses the ICS approach to facilitate internal emergency management and to coordinate with outside authorities.

The ICS provides a structured approach to declaring an emergency, managing an emergency, managing central communications, and transitioning an emergency over to outside authorities. Under this approach, a single individual, the incident commander (IC) is the primary decision-making authority to mitigate and resolve an emergency situation. An emergency operations center (EOC) serves as the communications center to coordinate internal communications and manage information. The crisis management team (CMT) serves to provide a management team to direct specific activities in specific areas of expertise.

As it relates to technological emergencies, Flexential has outlined these to include any interruption or loss of utility service, power source, environmental control, information system or equipment needed to maintain Flexential's operations. Loss of power would have significant consequences for Flexential's operations; for that reason, facilities

are designed with redundant power systems, including facility uninterruptible power supplies and generator systems. These systems are designed to provide continuous power in the event of a loss of utility power. In the event of a loss of utility power, the local critical incident manager (CIM) will be designated as the IC. The incident commander will take steps to ensure continued power to critical systems using available redundant systems.

Flexential's network infrastructure is critical to the operation of key systems as well as customer's systems. In the event of an interruption in network connectivity, the network manager shall be designated as the IC. The incident commander will coordinate efforts with carriers and customers to return normal communications as quickly as possible.

Environmental Security

Flexential has implemented and documented policies and procedures to ensure the environmental security of each data center. When a new data center is commissioned, management obtains a report from a third-party specialist to ascertain that each new data center has been properly commissioned. These reports include reviews of project specifications and submittals, inspections of equipment installations, observations of original equipment manufacturer (OEM) startups, and reviews of electrical and mechanical infrastructures.

Data centers are equipped with fire and smoke detectors which trigger visible and audible alarms in the event of a fire. Pre-action dry-pipe water sprinklers or agent-based fire suppression systems are present at each location along with hand-held fire extinguishers to allow for prompt suppression of fires. Management contracts with third-party specialists to inspect the fire detection and suppression systems on an annual basis and the inspection reports are retained as evidence of completion. Facilities personnel inspect the hand-held fire extinguishers on a monthly basis, while a third-party inspects the fire extinguishers on an annual basis. Documentation of each inspection is retained.

The data centers are equipped with multiple air conditioning units to regulate temperature and humidity. Management contracts with third-party specialists to inspect the air conditioning units on an annual basis and the inspection reports are retained as evidence of completion. The data centers are equipped with water detection devices to detect and mitigate water damage in the event of a flood or water leak. These water detection units are placed near the air conditioning units, either in drip pans or under the raised floor.

Each data center is equipped with fueled electric power generators and redundant UPS systems to provide continuous power in the event of an outage. The generators and UPS systems are each inspected for maintenance and load tests by a third-party on a semi-annual basis. Management obtains reports for completed maintenance activities and inspections.

Environmental monitoring systems are utilized to monitor the environmental systems and conditions within the data centers including fire alarm status and suppression systems, temperature, humidity and air quality, power levels and availability. The environmental monitoring application is configured to notify operations personnel via on-screen or e-mail alert notifications if certain predefined thresholds are exceeded on monitored systems. Lastly, TAC personnel perform multiple daily patrols to monitor and record readings from certain environmental equipment.

Incident Response

Incident response and support procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting managed and network services and include the following:

- Severity level definitions
- Escalation procedures
- Response time requirements for service alerts

An automated service management / ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting the services provided. The ticketing system is configured to include the incident date, time, summary, contact name, status, impact level, urgency, and associated SLA. A post incident report is performed for incidents to determine the root cause, system impact and resolution. Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.

System Monitoring

Facilities are monitored 24x7 by facilities engineers. Staff members are in place either on-site or on call after business hours to monitor and resolve problems affecting services provided.

Documented standard build procedures are utilized for the installation and maintenance of production systems. These build procedures help ensure a consistent configuration for production systems. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to send automated e-mail notifications to IT personnel when predefined thresholds are exceeded.

An enterprise monitoring portal is available for subscribing customers. The monitoring application is configured to alert operations personnel via onscreen and e-mail alert notifications when certain predefined thresholds are exceeded on monitored systems. Performance metric and service level reports including availability, alert history, and trend analysis are available. The enterprise monitoring application is utilized to monitor the following:

- Availability of the network, host services and ports
- Bandwidth utilization and performance
- Device resource utilization

To further ensure the security of systems, a central anti-virus software is utilized on production systems and is configured to perform scans of monitored systems on real-time basis. The central anti-virus is also configured to perform weekly scans for any new files installed on monitored systems and all files received, downloaded, copied, or modified.

Penetration testing is conducted to measure the security posture of target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Flexential. The third-party vendor's approach begins with a vulnerability analysis of the target system. This is performed to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed on a quarterly basis in accordance with Flexential policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Flexential. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Data

User entities are responsible for the procedures, by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within this environment; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

Requests for services are initiated and authorized by user entities by directly contacting the customer support department. Customer requests are recorded and tracked within an internal ticketing system through resolution. The ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting contracted services. Customer requests are managed according to established SLAs.

Information Category	Description	Examples
Unclassified Public	Information is not confidential and can be made public without any implications for Flexential. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	<ul style="list-style-type: none"> Product brochures widely distributed Information widely available in the public domain, including publicly available Flexential web site areas Downloads of Flexential documents and whitepapers provided for public consumption Reports required by regulatory authorities Information approved for public release
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Flexential's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	<ul style="list-style-type: none"> Passwords and information on corporate security procedures Know-how used to process client information Standard operating procedures and policies used in all parts of Flexential's businesses Flexential-developed software code, whether used internally or sold to clients
Customer Confidential Data	Information received from customers in any form or processing in production by Flexential. The original copy of such information must not be changed in any way without written permission from the customer. The highest possible levels of integrity, confidentiality, and restricted availability are vital. Personal identifiable information (PII) and personal health information (PHI) entrusted to Flexential is considered 'confidential.' PII and PHI data owned by customers residing within Flexential compliant systems must be encrypted and maintained per contractual obligation. PII and PHI data owned by Flexential must be encrypted and maintained by Flexential per the information security policy. Access is restricted based on the individual's role and current responsibilities. Access will not be granted unless a legitimate business-oriented need for such information exists. Third parties supporting Flexential are required to maintain the same level of standards to ensure PII is protected.	<ul style="list-style-type: none"> Customer media Electronic transmissions from customers Product information generated for the client by Flexential production activities as specified by the customer
Customer Hardware Assets	Hardware assets leased by the customers that reside within customer space. Assets should be considered sensitive/restricted as data that would not classify as PII or PHI may reside on assets but would still be considered sensitive/restricted. Hardware assets purchased by customers and installed in a Flexential facility, such as key management systems may also be classified as sensitive/restricted.	<ul style="list-style-type: none"> Customer leased servers, network switches, or firewalls Customer purchased technologies such as key management systems, which are installed in Flexential facility

Information Category	Description	Examples
Flexential Confidential Data	Information collected and used by Flexential in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	<ul style="list-style-type: none"> Salaries and other personal data Accounting data and internal financial reports Confidential customer business data and confidential contracts Non-disclosure agreements with clients/vendors Flexential business plans
Vendor/Partner Confidential	Information that can be disclosed to a vendor or partner who has signed non-disclosure agreement (NDA) agreement, e.g., standard master service agreement (MSA), however, the vendor/partner cannot share the information outside of their organization.	<ul style="list-style-type: none"> Contracts Vendor/partner facing documents Non-sensitive Client-specific information Proprietary information
Third-Party Personally Identifiable Information	<p>Third-party PII is data collected by Flexential's clients that can be used alone or with other sources available to identify a specific individual.</p> <p>This information is generally protected by one or more statutory or regulatory requirements such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), EU directive 95/46/EC, General Data Protection Rule (GDPR), as well as other state and federal consumer privacy protection laws.</p> <p>Access to this information is highly restricted and is generally unnecessary in the course of normal operations. The highest possible levels of integrity, confidentiality, and restricted availability are vital to conform to contractual, legal, and regulatory requirements.</p> <p>Flexential encrypts any third-party PII under its control during transmission and storage.</p>	<p>Personally identifiable information includes:</p> <ul style="list-style-type: none"> Full name (if not common) National identification number IP address (in some cases) Vehicle registration plate number Driver's license number Face, fingerprints, or handwriting Credit card numbers Digital identity Birthday Birthplace Genetic Information
EU Personal Data	Any information relating to an identified or identifiable natural person (i.e., information that can identify a person AND non-identifying information that can be linked to an identifiable person) in the European Union. The person does not have to be a formal resident of the EU, but their personal data must relate to their presence in the EU (e.g., the collection of personal information from a US resident while traveling on business in the EU constitutes "EU personal data").	<p>A data subject in the EU's:</p> <ul style="list-style-type: none"> Name Financial account information Government identification number Location data Online identifier (e.g., internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags) Factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person

Significant Changes During the Period

Flexential discontinued the usage of SilverSky, Inc. (BAE Systems) as a subservice provider for security monitoring (including IPS/IDS) in September 2022. Security monitoring tooling, operational processes, configurations and controls are included within the scope of Flexential's control environment, performed by Flexential's information security team, and within the scope of this report.

Additionally, in February 2023, Flexential commissioned the Hillsboro 4 data center which was added within the scope of this report. The Salt Lake City – Cottonwood Data center facility was de-commissioned in November 2022.

Subservice Organization

Equinix provides colocation services for the hardware and infrastructure utilized by Flexential to deliver cloud operations in Europe and were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Equinix, alone or in combination with controls at Flexential, and the types of controls expected to be implemented at Equinix to achieve Flexential's principal service commitments and system requirements based on the applicable trust services criteria.

Control Activities Expected to be Implemented by Subservice Organization	Applicable Trust Services Criteria
Equinix is expected to implement control activities for physical access control systems to restrict access to and within the corporate facility and data center housing the facilities, backup media, and other system components such as firewalls, routers, and servers to properly authorized individuals.	CC6.4
Equinix is expected to implement control activities for establishing and adhering to policies and procedures to ensure changes made to physical access privileges for customers is in accordance with standard operating procedure.	
Equinix is expected to implement control activities for reviewing visitors, customers, vendors, and contractors government issued ID prior to allowing access to the facilities.	
Equinix is expected to implement control activities for completing a termination form and remove physical access to the facilities as a component of the employee termination process.	
Equinix is expected to implement control activities for ensuring the following equipment is in place for each facility: <ul style="list-style-type: none">• Fire detection and suppression• Power management	A1.2
Equinix is expected to implement control activities for performing scheduled maintenance procedures to ensure that: <ul style="list-style-type: none">• Fire detection and suppression equipment is working properly• Test and confirm the operation of power maintenance systems• HVAC equipment, cooling equipment, and leak detection sensors are working properly	
Equinix is expected to implement control activities for maintaining and monitoring temperature and humidity throughout the facilities through the use of air conditioning and ventilation equipment.	
Equinix is expected to implement control activities for monitoring the facilities 24x7 and that staff members are in place either on site or on call 24x7 who are alerted by the building management system (BMS) for system exceptions.	

Control Activities Expected to be Implemented by Subservice Organization	Applicable Trust Services Criteria
Equinix is expected to implement control activities for implementing emergency procedures to help guide personnel in protecting against disruptions caused by an unexpected event.	A1.2

CONTROL ENVIRONMENT

The control environment at Flexential is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by executive management and operations management.

Integrity and Ethical Values

Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Flexential's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include the communication and review of Flexential's values and behavioral standards to personnel through policy statements, codes of conduct, training, and periodic meetings. Control activities that Flexential has implemented in this area include the following:

- A documented business code of conduct to communicate company values and behavioral standards to personnel.
- Employees complete an acknowledgment as a component of the onboarding process, and annually thereafter, indicating that they have been given access to and understand their responsibility for adhering to the standards and requirements outlined within the ethics guide, business code of conduct and employee handbook policies.
- Background checks are performed for employees and contingent workers as a component of the hiring process to verify employee candidate's credentials, and qualifications including previous employment and criminal history.
- Performance and conduct evaluations are performed for personnel on an annual basis.
- Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.
- Employees are directed on how to report unethical behavior in a confidential manner.

Executive Management Oversight

Executive management is responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives. Flexential control awareness is influenced by its executive management team. Attributes that define Flexential include the independence from management, their previous experiences as senior executive specializing in solutions, technology, and marketing and development. The chief executive officer (CEO) and the executive team communicate on an as needed basis in the event significant issues are required to be raised to the executive management team. Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment. If a significant issue is reported, an internal investigation may be initiated and monitored by the executive management team, which may include engagement of third-party investigator, auditor, or counsel by the executive management team. If key decisions are made by the executive team, they are communicated to the company by the CEO.

Organizational Structure and Assignment of Authority and Responsibility

The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. This includes assignment of authority and responsibility for operating activities and establishment of reporting relationships and authorization protocols. Policies describing business practices, knowledge, and experience required of key personnel and resources are communicated to employees for carrying out their duties. Control activities that Flexential has implemented in this area include the following:

- A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.
- Roles and responsibilities are defined in written job descriptions and address specific requirements relevant to the system and are communicated to personnel through the entity's SharePoint site.

Commitment to Competence

Employee competence is a key element of a control environment and Flexential is committed to recruiting and retaining individuals with skills that align with company objectives. Hiring decisions are based on various factors, including education and prior relative experience, to ensure candidate skills align with role responsibilities. Background checks are obtained prior to the finalization of an offer. Flexential also invests in ongoing training and development for its employees to empower individuals and extend their skills across various areas.

Accountability

Flexential's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to identifying and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel. Control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held on an annual basis to discuss major initiatives and issues that affect the business as a whole.
- Management has identified and documented objectives to track and accomplish long and short-term goals, which are specific, measurable, attainable, relevant, and time-bound (SMART).

Flexential HR department communicates to employees expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions. Flexential is committed to competent and trustworthy people and the advancement of qualified personnel to higher levels of responsibilities. Flexential training policies contains detailed prospective roles and responsibilities that are communicated to employees and available via the corporate intranet.

RISK ASSESSMENT

Objective Setting

Flexential has considered the significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities. Management is responsible for identifying the risks that threaten achievement of the control objectives stated in the management's description of the service organizations systems. Risk assessment activities include the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, and others with access to the entity's information system.

Risk Identification and Analysis

Operations management meets periodically or more frequently, if necessary, to review the status of each area of the company's operations and to assess risks that could affect service delivery to its customers. Also, management holds an Information Security Business Leadership Committee (ISBLC) quarterly to discuss any issues that occurred and what improvements can be made in operations to help prevent the issue from occurring again. The meeting consists of mid to senior leadership representatives from across Flexential's business units. Information accumulated and discussed during monthly operations and weekly meetings is also fed into other meetings with senior and executive management. Flexential created this review to enable Flexential to better identify risks, discuss remediation plans for identified risks, and develop action plans to remediate identified risks to help improve Flexential's security, availability, and confidentiality obligations to its customers. Risks identified during the assessments are documented and tracked to resolution.

Flexential has documented policies and procedures in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. Risks are prioritized by risk score and reviewed by management. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring and to identify the control activities necessary to mitigate the risk.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. Additionally, the annual risk assessment considers the potential for fraud.

Risk Mitigation

Risk mitigation activities include the ability to identify, select and develop activities that sufficiently meet the identified risks, and the organization has documented policies and procedures to guide personnel during this process. Risk identification and mitigation activities performed during the annual risk assessment process also consider the risks that could arise from potential business disruptions caused by an unexpected event. The annual risk assessment is reviewed during the executive management meetings and status of risk treatments and review of proposed new risks are discussed.

Vendors and business partners are also considered during the annual risk assessment and mitigation activities. To assist with this process, vendor management policies are in place that addresses specific requirements for a vendor and business partner; the due diligence process prior to accepting new vendors or business partners; a monitoring process to review vendor and business partner compliance on an ongoing basis, and how to handle exceptions.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, and confidentiality categories.

Selection and Development of Control Activities

The establishment of control activities is inclusive of general control activities over technology. The management personnel of Flexential evaluate the relationships between business processes and the use of technology to perform those processes to determine the dependencies on technology. The security management processes for the technology, along with other factors, are analyzed to define and establish the necessary control activities to achieve control objectives that include technology.

The establishment of the control activities is enforced by defined policies and procedures that specifically state management's directives for Flexential personnel. The policies serve as the rules that personnel must follow when implementing certain control activities. The procedures are the series of steps the personnel should follow when performing business or technology processes and the control activities that are components of those processes. After the policies, procedures and control activities are all established, each are implemented, monitored, reviewed, and improved when necessary.

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Flexential's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Data Center and Cloud Operations system.

INFORMATION AND COMMUNICATION SYSTEMS

Information is necessary for Flexential to carry out internal control responsibilities to support the achievement of its objectives related to the Data Center and Cloud Operations system. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control. Data is only retained for as long as required to carry out the system function or services.

The following provides a summary of internal and external sources of information used in the Data Center and Cloud Operations system:

- Help desk tickets used to record, track, and resolve support issues.
- Change tickets used to document and track change requests and change management activities including development, testing, and approvals
- HR employment and termination information.
- Data flow diagrams.
- Application, network, and system event logging and alerts received from centralized log monitoring systems.
- External security, legal, and compliance advisory groups and forums.

Internal Communications

Communication is an integral component of Flexential's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Flexential, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, quarterly All-Hands meetings provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the All-Hands meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures, along with roles and responsibilities are communicated to the appropriate Flexential personnel via the intranet site. Employees are also provided guidance on how to report unethical behavior in a confidential manner.

External Communications

Flexential has also implemented various methods of communications to help provide assurance that customers understand the roles and responsibilities for using Flexential's services and communicating significant events. These methods include visibility with incidents where the customer and Flexential have transparency to identify and correct issues from representatives from customers, and the use of e-mail messages and the customer contact line to communicate time-sensitive information and system description information, including operations and system-boundaries. A system description is also documented that includes the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems. The system description is communicated to authorized users. Additionally, the entity's security, availability, and confidentiality commitments and requirements are documented in customer contracts.

MONITORING

Management and supervisory personnel monitor the quality of internal controls as part of their activities. Flexential has implemented a series of management reports and metrics that measure the results of various processes involved in providing services to its customers. Some of the key metrics that the operations management team monitors are as follows:

- Capacity:
 - Power
 - Space
 - Cooling
 - Generator
 - Network
 - Servers
- Quality of service:
 - Network uptime
 - Backbone availability
 - Facility uptime
- Operations center:
 - Support call answer speeds
 - Support call volumes
 - Support ticket response times
 - Support ticket resolution times

The Flexential security, operations, and compliance teams are responsible for implementing procedures and guidelines to identify the risks inherent in Flexential's operations. The foundation of the risk management process is management's knowledge of its operations and its close working relationship with its customers. For any risks identified, management is responsible for implementing security control measures. Monitoring of risks is coordinated through various security and operational committees.

Ongoing Monitoring

Monitoring applications are utilized to monitor and analyze in-scope systems and are configured to alert IT personnel when defined thresholds have been reached. Flexential's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Flexential's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, significant changes in operations or methods of processing financial information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and the importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often.

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. These assessments are considered by management, along with any other internal control evaluations. The findings of these efforts are utilized to ensure follow-up actions are taken and subsequent evaluations are modified, as necessary.

Security monitoring applications, internal vulnerability scans, and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches. A third party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.

Monitoring of Subservice Organization

Flexential management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet the relevant control objectives through written contracts, such as service level agreements. In addition, Flexential has defined the following activities to oversee controls performed by vendors that could impact the Data Center and Cloud Operations system:

- Reviewing and reconciling output reports.
- Holding periodic discussions with the subservice organization.
- Reviewing attestation reports over services provided by vendors and subservice organizations.
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Evaluating and Communicating Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the service management system for internal tracking. ISBLC meetings are held on a quarterly basis for management to review reported deficiencies and corrective actions.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Flexential's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Data Center and Cloud Operations system provided by Flexential. The scope of the testing was restricted to the Data Center and Cloud Operations system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period November 1, 2022, through October 31, 2023.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- the nature of the control and the frequency with which it operates;
- the control risk mitigated by the control;
- the effectiveness of entity-level controls, especially controls that monitor other controls;
- the degree to which the control relies on the effectiveness of other controls; and
- whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organization, in order to complement the control activities and achieve the service commitments and system requirements are presented in the “Subservice Organization” sections within Section 3.

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	Inspected the employee handbook and the employee ethics manual to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	No exceptions noted.
CC1.1.2	An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the electronic receipt of acknowledgement for a sample of new employees hired during the period to determine that personnel were required to acknowledge the employee handbook and code of conduct upon hire for each sample selected during the period.	The test of the control activity disclosed that acknowledgment of the employee handbook and code of conduct did not occur within 60 days upon hire for two of 25 sampled new employees hired during the period.
CC1.1.4	Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the completed employee handbook acknowledgement for a sample of current employees to determine that personnel acknowledged the employee handbook and code of conduct on an annual basis for each employee sampled during the period.	No exceptions noted.
CC1.1.5	Upon hire, personnel are required to complete a background check.	Inquired of the HR manager regarding background checks to determine that background checks were completed upon hire	No exceptions noted.
		Inspected the completed background check for a sample of new employees hired during the period to determine that background checks were completed upon hire for each employee sampled during the period.	No exceptions noted.
CC1.1.6	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed on an annual basis for each employee sampled during the period.	No exceptions noted.
CC1.1.7	Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the employee disciplinary action procedures and employee handbook to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.
CC1.1.8	Employees are directed on how to report unethical behavior in a confidential manner.	Inspected the employee handbook to determine that employees were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	Executive management roles and responsibilities are documented.	Inspected the job description for a sample of executive management roles to determine that executive management roles and responsibilities were documented.	No exceptions noted.
CC1.2.2	Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.
CC1.2.3	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the most recent ISBLC meeting calendar invite, agenda, and meeting minutes during the period to determine that executive management met during the period with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
CC1.3.2	Roles and responsibilities are defined in written job descriptions and address specific requirements relevant to the system and are communicated to personnel through the entity's SharePoint site.	Inquired of the compliance manager regarding job descriptions to determine that written job descriptions were communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Inspected the job description for a sample of current employees to determine that roles and responsibilities were defined in written job descriptions and addressed specific requirements relevant to the system for each sample selected.	No exceptions noted.
CC1.3.3	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the most recent ISBLC meeting calendar invite, agenda, and meeting minutes during the period to determine that executive management met during the period with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the new employee hiring procedures to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
CC1.4.2	Policies and procedures are in place that outline the performance evaluation process requirements for personnel.	Inspected the employee handbook to determine that policies and procedures were in place that outlined the performance evaluation process requirements for personnel.	No exceptions noted.
CC1.4.3	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed on an annual basis for each employee sampled during the period.	No exceptions noted.
CC1.4.4	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	Inquired of the compliance manager regarding job descriptions to determine that written job descriptions were communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Inspected the job description for a sample of current employees to determine that roles and responsibilities were defined in written job descriptions and addressed specific requirements relevant to the system for each sample selected.	No exceptions noted.
CC1.4.5	Executive management has created a training program for its employees.	Inspected the training program documentation to determine that executive management created a training program for its employees.	No exceptions noted.
CC1.4.6	As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations as it relates to the job role and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations as it relates to the job role and responsibilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.7	Employees are required to attend security awareness training upon hire and annually thereafter.	Inspected the security awareness training completion report for a sample of new employees hired during the period to determine that employees were required to complete security awareness training upon hire for each sample selected during the period.	The test of the control activity disclosed that security awareness training was not completed within 60 days upon hire for three of 25 sampled new employees hired during the period.
		Inspected the security awareness training completion report for a sample of current employees to determine that employees were required to complete security awareness training on an annual basis for each sample selected during the period.	No exceptions noted.
CC1.4.8	Upon hire, personnel are required to complete a background check.	Inquired of the HR manager regarding background checks to determine that background checks were completed upon hire.	No exceptions noted.
		Inspected the completed background check for a sample of new employees hired during the period to determine that background checks were completed upon hire for each employee sampled during the period.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
CC1.5.2	Roles and responsibilities are defined in written job descriptions and address specific requirements relevant to the system and are communicated to personnel through the entity's SharePoint site.	Inquired of the compliance manager regarding job descriptions to determine that written job descriptions were communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Inspected the job description for a sample of current employees to determine that roles and responsibilities were defined in written job descriptions and addressed specific requirements relevant to the system for each sample selected.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.3	Upon hire, personnel are required to acknowledge the employee handbook and code of conduct which requires adherence to the personnel's job role and responsibilities.	Inspected the electronic receipt of acknowledgement for a sample of new employees hired during the period to determine that personnel were required to acknowledge the employee handbook and code of conduct upon hire for each sample selected during the period.	Refer to the test results applied in CC1.1.3.
CC1.5.4	Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the completed employee handbook acknowledgement for a sample of current employees to determine that personnel acknowledged the employee handbook and code of conduct on an annual basis for each employee sampled during the period.	No exceptions noted.
CC1.5.5	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed on an annual basis for each employee sampled during the period.	No exceptions noted.
CC1.5.6	Executive management has documented objectives that are SMART.	Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were SMART.	No exceptions noted.
CC1.5.7	Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the employee disciplinary action procedures and employee handbook to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's SharePoint site.	Inspected the information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's SharePoint site.	No exceptions noted.
CC2.1.2	Data is only retained for as long as required to perform the required system functionality, service, or use.	Inspected the data retention policies and procedures to determine that data was retained for only as long as required to perform the required system functionality, service, or use.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.3	Management reviews reports on a quarterly basis summarizing incident, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the ISBLC meeting agenda and minutes for a sample of quarters during the period to determine that management reviewed reports on a quarterly basis during the period summarizing incident, root cause of incidents, and corrective action plans, and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
CC2.1.4	Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected data flow diagrams to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
CC2.1.5	Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the security monitoring system configurations and an example review performed during the period to determine that security monitoring applications and manual reviews were utilized during the period to monitor and analyze the in-scope systems for possible or actual security breaches.	No exceptions noted.
CC2.1.6	The monitoring application is configured to generate reports for ongoing monitoring of performance metrics and service levels including, but not limited to, the following: <ul style="list-style-type: none"> • Availability • Alert history • Trend analysis reports 	Inspected the enterprise monitoring application configurations and an example summary report to determine that the monitoring application was configured to generate reports for ongoing monitoring of performance metrics and service levels including the following: <ul style="list-style-type: none"> • Availability • Alert history • Trend analysis reports 	No exceptions noted.
CC2.1.7	IT personnel perform internal vulnerability scans on a quarterly basis to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the internal vulnerability scan results for a sample of quarters during the period to determine that IT personnel performed internal vulnerability scans on a quarterly basis to monitor and analyze the in-scope systems for possible or actual security breaches for each quarter sampled during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.8	A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results performed during the period to determine that a third-party performed a penetration testing during the period to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's SharePoint site.	Inspected the information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's SharePoint site.	No exceptions noted.
CC2.2.2	Documented escalation procedures for reporting failures, incidents, concerns, and other complaints are made available to internal and external users.	Inspected the incident management policies and procedures, the corporate intranet, and Flexential support site to determine that documented escalation procedures for reporting failures, incidents, concerns, and other complaints were made available to internal and external users.	No exceptions noted.
CC2.2.3	Roles and responsibilities are defined in written job descriptions and address specific requirements relevant to the system and are communicated to personnel through the entity's SharePoint site.	Inquired of the compliance manager regarding job descriptions to determine that written job descriptions were communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Inspected the job description for a sample of current employees to determine that roles and responsibilities were defined in written job descriptions and addressed specific requirements relevant to the system for each sample selected.	No exceptions noted.
CC2.2.4	The entity's policies and procedures, code of conduct, employee handbook, and including changes made to the entity's objectives are communicated and accessible to employees through SharePoint.	Inspected the entity's SharePoint site to determine that the entity's policies and procedures, code of conduct, employee handbook, and including changes made to the entity's objectives were communicated and accessible to employees through SharePoint.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.5	Employees are required to attend security awareness training upon hire and annually thereafter.	Inspected the security awareness training completion report for a sample of new employees hired during the period to determine that employees were required to complete security awareness training upon hire for each sample selected during the period.	Refer to the test results applied in CC1.4.7.
		Inspected the security awareness training completion report for a sample of current employees to determine that employees were required to complete security awareness training on an annual basis for each sample selected during the period.	No exceptions noted.
CC2.2.6	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the most recent ISBLC meeting calendar invite, agenda, and meeting minutes during the period to determine that executive management met during the period with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
CC2.2.7	Employees are directed on how to report unethical behavior in a confidential manner.	Inspected the employee handbook to determine that employees were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Standard policies and contracts are made available to communicate the system commitments and requirements of external users prior to allowing access to the system.	Inspected the external facing policies and an example contract to determine that standard policies and contracts were made available to communicate the system commitments and requirements of external users prior to allowing access to the system.	No exceptions noted.
CC2.3.2	Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the service agreement for a sample of customers onboarded during the period to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements for each sample selected during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.3	Documented escalation procedures for reporting failures, incidents, concerns, and other complaints are made available to internal and external users.	Inspected the incident management policies and procedures, the corporate intranet, and Flexential support site to determine that documented escalation procedures for reporting failures, incidents, concerns, and other complaints were made available to internal and external users.	No exceptions noted.
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the documented key performance indicators for operational and internal controls effectiveness, employee handbook, and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
CC3.1.2	Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the information security management policies and procedures to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
		Inspected the most recently completed risk assessment performed during the period to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved during the period.	No exceptions noted.
CC3.1.3	Executive management reviews policies, procedures, and other control documents for alignment to the entity's objectives on an annual basis.	Inspected the most recent ISBLC meeting calendar invite, agenda, and meeting minutes during the period to determine that executive management reviewed policies, procedures, and other control documents for alignment to the entity's objectives during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.4	Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
CC3.1.5	Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
CC3.1.6	Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee performance evaluation policies and procedures and the documented key performance indicators for operational and internal controls effectiveness to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
CC3.1.7	Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
CC3.1.8	The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations, and standards.	Inspected the entity's completed attestation reports to determine that the entity underwent compliance audits at least annually to show compliance to relevant laws, regulations, and standards.	No exceptions noted.
CC3.2 COSO Principle 7: 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.			
CC3.2.1	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the information security management policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.2	Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	Inspected the information security management policies and procedures to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	No exceptions noted.
CC3.2.3	A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the most recently completed risk assessment performed during the period to determine that a formal risk assessment was performed during the period to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
CC3.2.4	<p>The entity's risk assessment process includes:</p> <ul style="list-style-type: none"> Identifying the relevant information assets that are important to business operations Prioritizing the criticality of those relevant information assets Identifying and assessing the impact of the threats to those information assets Identifying and assessing the impact of the vulnerabilities associated with the identified threats Assessing the likelihood of identified threats and vulnerabilities Determining the risks associated with the information assets Addressing the associated risks identified for each identified vulnerability 	<p>Inspected the risk assessment, the information security policy, and the risk management policies and procedures to determine that the entity's risk assessment process included:</p> <ul style="list-style-type: none"> Identifying the relevant information assets that are important to business operations Prioritizing the criticality of those relevant information assets Identifying and assessing the impact of the threats to those information assets Identifying and assessing the impact of the vulnerabilities associated with the identified threats Assessing the likelihood of identified threats and vulnerabilities Determining the risks associated with the information assets Addressing the associated risks identified for each identified vulnerability 	No exceptions noted.
CC3.2.5	Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the information security management policies and procedures to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recently completed risk assessment performed during the period to determine that identified risks were rated using a risk evaluation process and ratings were approved by management during the period.	No exceptions noted.
CC3.2.6	Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the information security management policies and procedures and the most recently completed risk assessment performed during the period to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process during the period.	No exceptions noted.
CC3.2.7	For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the risk management policies and procedures and the most recently completed risk assessment performed during the period to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities during the period.	No exceptions noted.
CC3.2.8	The annual comprehensive risk assessment results are reviewed and approved by management.	Inspected the most recently completed risk assessment, the ISBLC meeting agenda performed during the period, and the risk management policy to determine that the annual comprehensive risk assessment results were reviewed and approved by management during the period.	No exceptions noted.
CC3.2.9	As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third parties.	Inspected the risk management policies and procedures, the vendor security policy, and the most recently completed risk assessment performed during the period to determine that management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third parties during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the most recently completed risk assessment performed during the period to determine that on an annual basis, management identified and assessed the types of fraud that could impact their business and operations during the period.	No exceptions noted.
CC3.3.2	As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the most recently completed risk assessment performed during the period to determine that as part of management's assessment of fraud risks during the period, management considered how personnel could engage in or justify fraudulent activities.	No exceptions noted.
CC3.3.3	As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.	Inspected the most recently completed risk assessment performed during the period to determine that as part of management's assessment of fraud risks during the period, management considered threats and vulnerabilities that arise from the use of IT.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Inspected the most recently completed risk assessment performed during the period to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment during the period.	No exceptions noted.
CC3.4.2	Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recently completed risk assessment performed during the period to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment during the period.	No exceptions noted.
CC3.4.3	Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the information security and management policies and procedures to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Inspected the most recently completed risk assessment performed during the period to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment during the period.	No exceptions noted.
CC3.4.4	Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the vendor security policy and the most recently completed risk assessment performed during the period to determine that changes in vendor and third-party relationships were considered and evaluated as part of the annual comprehensive risk assessment during the period.	No exceptions noted.
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the security monitoring system configurations and an example review performed during the period to determine that security monitoring applications and manual reviews were utilized during the period to monitor and analyze the in-scope systems for possible or actual security breaches.	No exceptions noted.
CC4.1.2	The security monitoring applications are configured to alert IT personnel when certain defined thresholds have been reached.	Inspected the monitoring system configurations and an example alert generated during the period to determine that the security monitoring applications were configured to alert IT personnel when certain defined thresholds had been reached during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.3	<p>The monitoring application is configured to generate reports for ongoing monitoring of performance metrics and service levels including, but not limited to, the following:</p> <ul style="list-style-type: none"> • Availability • Alert history • Trend analysis reports 	<p>Inspected the enterprise monitoring application configurations and an example summary report to determine that the monitoring application was configured to generate reports for ongoing monitoring of performance metrics and service levels including the following:</p> <ul style="list-style-type: none"> • Availability • Alert history • Trend analysis reports 	No exceptions noted.
CC4.1.4	IT personnel perform internal vulnerability scans on a quarterly basis to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the internal vulnerability scan results for a sample of quarters during the period to determine that IT personnel performed internal vulnerability scans on a quarterly basis to monitor and analyze the in-scope systems for possible or actual security breaches for each quarter sampled during the period.	No exceptions noted.
CC4.1.5	A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results performed during the period to determine that a third-party performed a penetration testing during the period to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
CC4.1.6	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the most recent ISBLC meeting calendar invite, agenda, and meeting minutes during the period to determine that executive management met during the period with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
CC4.1.7	Service support personnel are scheduled to be available 24 hours per day for monitoring and resolution of problems affecting services provided.	Inquired of the data center operations manager regarding service support personnel staffing to determine that service support personnel were scheduled to be available 24 hours per day for monitoring and resolution of problems affecting services provided.	No exceptions noted.
		Inspected the support personnel staffing schedule for a sample of dates during the period to determine that service support personnel were scheduled to be available 24 hours per day for monitoring and resolution of problems affecting services provided.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.8	Internal control assessments are performed by individuals with sufficient knowledge of what is being evaluated.	Inspected the organizational chart and the internal audit assessment documentation to determine that evaluations were performed by individuals with sufficient knowledge of what is being evaluated.	No exceptions noted.
CC4.2 COSO Principle 17: 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.			
CC4.2.1	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the most recent ISBLC meeting calendar invite, agenda, and meeting minutes during the period to determine that executive management met during the period with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
CC4.2.2	Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed.	Inquired of the compliance manager regarding compliance assessments to determine that management tracked vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed.	No exceptions noted.
		Inspected the most recent executive committee meeting and the risk assessment performed during the period to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed.	No exceptions noted.
CC4.2.3	Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the security monitoring system configurations and an example review performed during the period to determine that security monitoring applications and manual reviews were utilized during the period to monitor and analyze the in-scope systems for possible or actual security breaches.	No exceptions noted.
CC4.2.4	The security monitoring applications are configured to alert IT personnel when certain defined thresholds have been reached.	Inspected the monitoring system configurations and an example alert generated during the period to determine that the security monitoring applications were configured to alert IT personnel when certain defined thresholds had been reached during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.5	Documented escalation procedures for reporting failures, incidents, concerns, and other complaints are made available to internal and external users.	Inspected the incident management policies and procedures, the corporate intranet, and Flexential support site to determine that documented escalation procedures for reporting failures, incidents, concerns, and other complaints were made available to internal and external users.	No exceptions noted.
CC4.2.6	Incidents are documented and tracked in a standardized ticketing system and are updated to reflect the planned incident and problem, resolution, and is communicated to affected users.	Inspected security incident tickets for a sample of security incident tickets closed during the period to determine that incidents were documented and tracked in a standardized ticketing system during the period and were updated to reflect the planned incident and problem, resolution, and was communicated to affected users for each sample selected.	No exceptions noted.
Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	Inspected the risk assessment policies and procedures and the most recently completed risk assessment performed during the period to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps during the period.	No exceptions noted.
CC5.1.2	Performance of the internal controls implemented within the environment are assigned to process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and internal controls roles and responsibilities matrix to determine that performance of the internal controls implemented within the environment were assigned to process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
CC5.1.3	Management has documented the relevant controls in place for each key business or operational process.	Inspected the internal controls roles and responsibilities matrix and the internal audit report to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.4	Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls roles and responsibilities matrix and the internal audit report to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
CC5.1.5	Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results performed during the period to determine that the business continuity and disaster recovery plans were tested during the period.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the internal controls roles and responsibilities matrix and the internal audit report to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.
CC5.2.2	Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the internal controls roles and responsibilities matrix and the internal audit report to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
CC5.2.3	Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the internal controls roles and responsibilities matrix and the internal audit report to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
CC5.2.4	As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the most recently completed risk assessment performed during the period to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.5	<p>The internal controls implemented around the entity's technology infrastructure include, but are not limited to:</p> <ul style="list-style-type: none"> Restricting access rights to authorized users Limiting services to what is required for business operations Authentication of access Protecting the entity's assets from external threats 	<p>Inspected the internal controls roles and responsibilities matrix and the internal audit report to determine that the internal controls implemented around the entity's technology infrastructure included:</p> <ul style="list-style-type: none"> Restricting access rights to authorized users Limiting services to what is required for business operations Authentication of access Protecting the entity's assets from external threats 	No exceptions noted.
CC5.2.6	Management has established controls around the acquisition, development, and maintenance of the entity's technology infrastructure.	Inspected the internal controls roles and responsibilities matrix and the internal audit report to determine that management established controls around the acquisition, development, and maintenance of the entity's technology infrastructure.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's SharePoint site.	No exceptions noted.
CC5.3.2	Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the internal controls roles and responsibilities matrix to determine that process owners were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
CC5.3.3	Roles and responsibilities are defined in written job descriptions and address specific requirements relevant to the system and are communicated to personnel through the entity's SharePoint site.	Inquired of the compliance manager regarding job descriptions to determine that written job descriptions were communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Inspected the job description for a sample of current employees to determine that roles and responsibilities were defined in written job descriptions and addressed specific requirements relevant to the system for each sample selected.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.4	Performance of the internal controls implemented within the environment are assigned to process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and internal controls roles and responsibilities matrix to determine that performance of the internal controls implemented within the environment were assigned to process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
CC5.3.5	Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	Inspected the information security and risk management policies and procedures to determine that process owners and management operated the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	No exceptions noted.
CC5.3.6	Effectiveness of the internal controls implemented within the environment are evaluated annually.	Inspected the internal audit results report performed during the period to determine that effectiveness of the internal controls implemented within the environment were evaluated during the period.	No exceptions noted.

Logical and Physical Access Controls

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.

CC6.1.1	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components were maintained to classify and manage the information assets.	No exceptions noted.
CC6.1.2	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
CC6.1.3	The in-scope systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	<p>Inspected the network domain password configurations to determine that network users were authenticated via a user account and password before being granted access to the network and that the network was configured to enforce the following password requirements:</p> <ul style="list-style-type: none"> • Minimum password length • Password age (minimum and maximum) • Password history • Password complexity requirements 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.4	Network account lockout settings are in place that include: <ul style="list-style-type: none"> Account lockout duration Account lockout threshold Account lockout counter reset 	Inspected the network account lockout configurations to determine that network account lockout settings were in place that included: <ul style="list-style-type: none"> Account lockout duration Account lockout threshold Account lockout counter reset 	No exceptions noted.
CC6.1.5	Predefined security groups are utilized to assign role-based access privileges to the in-scope systems.	Inquired of the security manager regarding predefined security groups to determine that predefined security groups were utilized to assign role-based access privileges to the in-scope systems.	No exceptions noted.
		Inspected the network admins and predefined access groups to determine that predefined security groups were utilized to assign role-based access privileges to the in-scope systems.	No exceptions noted.
CC6.1.6	Administrative privileges on the managed services network are restricted to user accounts accessible by authorized personnel.	Inquired of the compliance manager regarding administrative privileges to the managed services network to determine that administrative privileges on the managed services network were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the listing of user accounts with network administrative access to determine that administrative privileges on the managed services network were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.7	User access requests are documented on a standard access request form and require the approval of a manager.	Inspected the standard user access request form for a sample of new users onboarded during the period to determine that user access requests were documented on a standard access request form and required the approval of a manager for each sample selected during the period.	No exceptions noted.
CC6.1.8	A termination checklist is completed, and access is revoked for employees as a component of the employee termination process.	Inquired of the compliance manager regarding user account deactivation to the managed services network to determine that a termination checklist was completed, and access was revoked for employees as a component of the employee termination.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the completed termination checklist for a sample of terminated employees during the period to determine that a termination checklist was completed, and access was revoked for employees as a component of the employee termination for each sample selected during the period.	No exceptions noted.
CC6.1.9	User access reviews are performed on a quarterly basis to help ensure that access to data is restricted.	Inspected the completed user access review for a sample of quarters during the period to determine that user access reviews were performed on a quarterly basis to help ensure that access to data was restricted for each quarter sampled during the period.	No exceptions noted.
CC6.1.10	Encrypted VPNs are utilized for remote access to help ensure the security and integrity of data passing over the public network.	Inspected the VPN encryption configurations to determine that encrypted VPNs were utilized for remote access to help ensure the security and integrity of data passing over the public network.	No exceptions noted.
CC6.1.11	Web servers utilize TLS encryption for web communication sessions.	Inspected the web portal encryption settings to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC6.1.12	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Inspected the firewall configurations to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall rule.	No exceptions noted.
CC6.1.13	The firewall system requires administrators to authenticate from a pre-defined subnet using an authorized user account and password, and MFA token to perform firewall administration tasks.	Inquired of the compliance manager regarding firewall system authentication to determine that the firewall system required administrators to authenticate from a pre-defined subnet using an authorized user account, password, and MFA token prior to performing firewall administration tasks.	No exceptions noted.
		Inspected the firewall system to determine that the firewall system required administrators to authenticate from a pre-defined subnet using an authorized user account, password, and MFA token prior to performing firewall administration tasks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.14	Administrative privileges on the firewall system are restricted to user accounts accessible by authorized personnel.	Inquired of the compliance manager regarding administrative access to the firewall system to determine that administrative privileges on the firewall system were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the listing of user accounts with firewall system administrative privileges with the assistance of the compliance manager to determine that administrative privileges on the firewall system were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.15	Systems are configured to log access attempts and events and send the logs to a centralized log server. Support personnel are notified when predefined access attempt thresholds are exceeded.	Inspected the audit logging configurations, an example log, and an alert notification generated during the period to determine that systems were configured to log access attempts and events and send the logs to a centralized log server and that support personnel were notified when predefined access attempt thresholds were exceeded.	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.			
CC6.2.1	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
CC6.2.2	User access requests are documented on a standard access request form and require the approval of a manager.	Inspected the standard user access request form for a sample of new users onboarded during the period to determine that user access requests were documented on a standard access request form and required the approval of a manager for each sample selected during the period.	No exceptions noted.
CC6.2.3	A termination checklist is completed, and access is revoked for employees as a component of the employee termination process.	Inquired of the compliance manager regarding user account deactivation to the managed services network to determine that a termination checklist was completed, and access was revoked for employees as a component of the employee termination.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the completed termination checklist for a sample of terminated employees during the period to determine that a termination checklist was completed, and access was revoked for employees as a component of the employee termination for each sample selected during the period.	No exceptions noted.
CC6.2.4	Predefined security groups are utilized to assign role-based access privileges to the in-scope systems.	Inquired of the compliance manager regarding predefined security groups to determine that predefined security groups were utilized to assign role-based access privileges to the in-scope systems.	No exceptions noted.
		Inspected the network admins and predefined access groups to determine that predefined security groups were utilized to assign role-based access privileges to the in-scope systems.	No exceptions noted.
CC6.2.5	User access reviews are performed on a quarterly basis to help ensure that access to data is restricted.	Inspected the completed user access review for a sample of quarters during the period to determine that user access reviews were performed on a quarterly basis to help ensure that access to data was restricted for each quarter sampled during the period.	No exceptions noted.
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.			
CC6.3.1	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place for system authentication, access, and security monitoring.	No exceptions noted.
CC6.3.2	User access requests are documented on a standard access request form and require the approval of a manager.	Inspected the standard user access request form for a sample of new users onboarded during the period to determine that user access requests were documented on a standard access request form and required the approval of a manager for each sample selected during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.3	A termination checklist is completed, and access is revoked for employees as a component of the employee termination process.	Inquired of the compliance manager regarding user account deactivation to the managed services network to determine that a termination checklist was completed, and access was revoked for employees as a component of the employee termination.	No exceptions noted.
		Inspected the completed termination checklist for a sample of terminated employees during the period to determine that a termination checklist was completed, and access was revoked for employees as a component of the employee termination for each sample selected during the period.	No exceptions noted.
CC6.3.4	Predefined security groups are utilized to assign role-based access privileges to the in-scope systems.	Inquired of the compliance manager regarding predefined security groups to determine that predefined security groups were utilized to assign role-based access privileges to the in-scope systems.	No exceptions noted.
		Inspected the network admins and predefined access groups to determine that predefined security groups were utilized to assign role-based access privileges to the in-scope systems.	No exceptions noted.
CC6.3.5	User access reviews are performed on a quarterly basis to help ensure that access to data is restricted.	Inspected the completed user access review for a sample of quarters during the period to determine that user access reviews were performed on a quarterly basis to help ensure that access to data was restricted for each quarter sampled during the period.	No exceptions 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.			
CC6.4.1	Documented physical security policies and procedures are in place to guide personnel in physical security administration.	Inspected the physical security policy and procedures to determine that documented physical security policies and procedures were in place to guide personnel in physical security administration.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.2	<p>Two separate two-factor authentication systems are utilized to control access to the data centers. The systems require the following before granting access:</p> <ul style="list-style-type: none"> Flexential badge to enter the building Badge and PIN code, or a badge and biometric fingerprint scan to enter the data centers 	<p>Inquired of the infrastructure manager regarding access to the data centers to determine that two separate two-factor authentication systems were utilized to control access to the data centers and that the systems required the following before granting access:</p> <ul style="list-style-type: none"> Flexential badge to enter the building Badge and PIN code, or a badge and biometric fingerprint scan to enter the data centers 	No exceptions noted.
		<p>Observed the use of two separate two-factor authentication systems for the in-scope data centers to determine that two separate two-factor authentication systems were utilized to control access to the data centers and that the systems required the following before granting access:</p> <ul style="list-style-type: none"> Flexential badge to enter the building Badge and PIN code, or a badge and biometric fingerprint scan to enter the data centers 	No exceptions noted.
CC6.4.3	Visitors are required to sign-in with onsite security personnel prior to entering the data centers.	Observed the visitor registration procedures for the in-scope data centers to determine that visitors were required to sign-in with onsite security personnel prior to entering the data centers.	No exceptions noted.
		Inspected the visitor registration log for the in-scope data centers to determine that visitors were required to sign-in with onsite security personnel.	No exceptions noted.
CC6.4.4	Data center visitors are required to be accompanied and supervised by an authorized Flexential employee or client escort.	Observed the data center visitor procedures for the in-scope data centers to determine that data center visitors were required to be accompanied and supervised by an authorized Flexential employee or client escort.	No exceptions noted.
		Inspected the physical security policy and procedures to determine that data center visitors were required to be accompanied and supervised by an authorized Flexential employee or client escort.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.5	Visitors are required to wear a visitor badge while visiting the data centers.	Inquired of the infrastructure manager regarding visitor badges at the data center to determine that visitors were required to wear a visitor badge while visiting the data centers.	No exceptions noted.
		Observed the data center visitor registration procedures for the in-scope data centers to determine that visitors were required to wear a visitor badge while visiting the data centers.	No exceptions noted.
		Inspected the physical security policy and procedures to determine that visitors were required to wear a visitor badge while visiting the data centers.	No exceptions noted.
CC6.4.6	Client equipment is maintained in lockable cages or racks within the data centers.	Inquired of the infrastructure manager regarding client equipment to determine that client equipment was maintained in lockable cages or racks within the data centers.	No exceptions noted.
		Observed the lockable cages and racks for the in-scope data centers to determine that client equipment was maintained in lockable cages or racks within the data centers.	No exceptions noted.
CC6.4.7	There are no exterior facing windows in the walls of the areas where client production servers are located.	Observed the in-scope data centers to determine that there were no exterior facing windows in the walls of the areas where client production servers were located.	No exceptions noted.
CC6.4.8	<p>Documented security procedures are in place to govern vendor access to the data centers, and include, but are not limited to, the following:</p> <ul style="list-style-type: none"> • Health and safety • Vendor Verification and Access • Vendor Accountability • Maintenance activity logging 	<p>Inspected the vendor security policy and procedures to determine that documented security procedures were in place to govern vendor access to the data centers, and included:</p> <ul style="list-style-type: none"> • Health and safety • Vendor Verification and Access • Vendor Accountability • Maintenance activity logging 	No exceptions noted.
CC6.4.9	Vendors are required to sign a vendor accountability form to perform maintenance in the data centers.	Inquired of the infrastructure manager regarding vendor access procedures to determine that vendors were required to sign a vendor accountability form to perform maintenance in the data centers.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vendor security policy and procedures to determine that vendors were required to sign a vendor accountability form to perform maintenance in the data centers.	No exceptions noted.
		Inspected the vendor accountability form template and the vendor log to determine that vendors were required to sign a vendor accountability form to perform maintenance in the data centers.	No exceptions noted.
CC6.4.10	Management reviews badge access of terminated employees on a quarterly basis.	Inspected the completed badge access review for a sample of quarters during the period to determine that management reviewed badge access of terminated employees for each quarter sampled during the period.	No exceptions noted.
CC6.4.11	Badge access privileges of terminated employees are revoked as a component of the employee termination process.	Inquired of the infrastructure manager regarding badge access procedures to determine that badge access privileges of terminated employees were revoked as a component of the employee termination process.	No exceptions noted.
		Inspected the badge access listing and the completed termination checklist for a sample of terminated employees during period to determine that badge access privileges of terminated employees were revoked as a component of the employee termination process for each sample selected during the period.	No exceptions noted.
	Equinix is expected to implement control activities for physical access control systems to restrict access to and within the corporate facility and data center housing the facilities, backup media, and other system components such as firewalls, routers, and servers to properly authorize individuals.		
	Equinix is expected to implement control activities for establishing and adhering to policies and procedures to ensure changes made to physical access privileges for customers is in accordance with standard operating procedure.		
	Equinix is expected to implement control activities for reviewing visitors, customers, vendors, and contractors government issued ID prior to allowing access to the facilities.		
	Equinix is expected to implement control activities for completing a termination form and remove physical access to the facilities as a component of the employee termination process.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC6.5.1	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	<p>Inspected the information security policy, data retention policy, and data destruction policies and procedures to determine that documented data destruction policies and procedures were in place that included:</p> <ul style="list-style-type: none"> Identifying confidential information requiring destruction when the end of the retention period is reached Erasing or destroying confidential information that has been identified for destruction 	No exceptions noted.
CC6.5.2	The entity purges stored data once it has met its defined retention period.	Inspected the data retention and media reuse and disposal policies and procedures to determine that the entity purged stored data once it had met its defined retention period.	No exceptions noted.
CC6.5.3	An inventory log is maintained of assets with confidential data and is destroyed or purged in accordance with retention policies and procedures.	Inquired of the compliance manager regarding data disposal to determine that an inventory log was maintained of assets with confidential data and was destroyed or purged in accordance with retention policies and procedures.	No exceptions noted.
		Inspected the information security policy, the inventory log, and a sample of assets disposed within the period to determine that an inventory log was maintained of assets with confidential data and was destroyed or purged in accordance with retention policies and procedures for each sample selected.	No exceptions noted.
CC6.5.4	Data that is no longer required for business purposes is rendered unreadable.	Inquired of the compliance manager regarding certificate of destruction to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
		Inspected the listing of requests to destroy hard drives and other IT related assets and the certificates of destruction during the period to determine that data that was no longer required for business purposes was rendered unreadable during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Encrypted VPNs are utilized for remote access to help ensure the security and integrity of data passing over the public network.	Inspected the VPN encryption configurations to determine that encrypted VPNs were utilized for remote access to help ensure the security and integrity of data passing over the public network.	No exceptions noted.
CC6.6.2	Web servers utilize TLS encryption for web communication sessions.	Inspected the web portal encryption settings to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC6.6.3	A stateful inspection, high-availability firewall system is in place at the network perimeter to filter unauthorized inbound traffic.	Inspected the network diagrams and the firewall configurations to determine that a stateful inspection, high-availability firewall system was in place at the network perimeter to filter unauthorized inbound traffic.	No exceptions noted.
CC6.6.4	The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Inspected the firewall configurations to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall rule.	No exceptions noted.
CC6.6.5	Firewall and router rules are reviewed on a semi-annual basis to ensure that only necessary connections are configured within the rulesets.	Inquired of the compliance manager regarding the firewall and router rules to determine that firewall and router rules were reviewed on a semi-annual basis to ensure that only necessary connections were configured within the rulesets.	No exceptions noted.
		Inspected the firewall and router ruleset policy and the most recently completed firewall review performed during the period to determine that firewall and router rules were reviewed on a semi-annual basis during the period to ensure that only necessary connections were configured within the rulesets.	No exceptions noted.
CC6.6.6	An IPS is utilized to analyze and report network events.	Inspected the IPS configurations and an example alert generated during the period to determine that an IPS was utilized to analyze and report network events.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC6.7.1	Policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the information security policy and data protection procedures to determine that policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
CC6.7.2	Encrypted VPNs are utilized for remote access to help ensure the security and integrity of data passing over the public network.	Inspected the VPN encryption configurations to determine that encrypted VPNs were utilized for remote access to help ensure the security and integrity of data passing over the public network.	No exceptions noted.
CC6.7.3	Web servers utilize TLS encryption for web communication sessions.	Inspected the web portal encryption settings to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC6.7.4	An automated backup system is utilized to perform scheduled system backups.	Inspected the automated backup system configurations and an example backup log generated during the period to determine that an automated backup system was utilized to perform scheduled system backups.	No exceptions noted.
CC6.7.5	Data that entered into the system, processed by the system, and output from the system is protected from unauthorized access.	Inspected the encryption configurations to determine that data entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.
CC6.7.6	Documented security procedures are in place to govern vendor access to the data centers, and include, but are not limited to, the following: <ul style="list-style-type: none"> • Health and safety • Vendor Verification and Access • Vendor Accountability • Maintenance activity logging 	Inspected the vendor security policy and procedures to determine that documented security procedures were in place to govern vendor access to the data centers, and included: <ul style="list-style-type: none"> • Health and safety • Vendor Verification and Access • Vendor Accountability • Maintenance activity logging 	No exceptions noted.
CC6.7.7	Vendors are required to sign a vendor accountability form to perform maintenance in the data centers.	Inquired of the infrastructure manager regarding vendor access procedures to determine that vendors were required to sign a vendor accountability form to perform maintenance in the data centers.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the vendor security policy and procedures to determine that vendors were required to sign a vendor accountability form to perform maintenance in the data centers.	No exceptions noted.
		Inspected the vendor accountability form template and the vendor log to determine that vendors were required to sign a vendor accountability form to perform maintenance in the data centers.	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.			
CC6.8.1	Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment.	Inspected the information security policy, the vulnerability management program, and the hardening provisioning checklists to determine that information assets, software, hardware, tools, and applications introduced into the environment were scanned for vulnerabilities and malware prior to implementation into the environment.	No exceptions noted.
CC6.8.2	A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: <ul style="list-style-type: none">Scan for updates to antivirus definitions and update registered devices on a daily basisScan registered devices on a weekly basis	Inquired of the compliance manager regarding antivirus configurations to determine that a central antivirus server was configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: <ul style="list-style-type: none">Scan for updates to antivirus definitions and update registered devices on a daily basisScan registered devices on a weekly basis	No exceptions noted.
		Inspected the enterprise antivirus software configurations to determine that a central antivirus server was configured with antivirus software to protect registered production Windows servers and workstations with the following configurations: <ul style="list-style-type: none">Scan for updates to antivirus definitions and update registered devices on a daily basisScan registered devices on a weekly basis	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.8.3	Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the security monitoring system configurations and an example review performed during the period to determine that security monitoring applications and manual reviews were utilized during the period to monitor and analyze the in-scope systems for possible or actual security breaches.	No exceptions noted.
CC6.8.4	IT personnel perform internal vulnerability scans on a quarterly basis to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the internal vulnerability scan results for a sample of quarters during the period to determine that IT personnel performed internal vulnerability scans on a quarterly basis to monitor and analyze the in-scope systems for possible or actual security breaches for each quarter sampled during the period.	No exceptions noted.
CC6.8.5	Systems are configured to log access attempts and events and send the logs to a centralized log server. Support personnel are notified when predefined access attempt thresholds are exceeded.	Inspected the audit logging configurations, an example log, and an alert notification generated during the period to determine that systems were configured to log access attempts and events and send the logs to a centralized log server and that support personnel were notified when predefined access attempt thresholds were exceeded.	No exceptions noted.
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.			
CC7.1.1	<p>Documented standard build procedures are in place for installation and maintenance of customer systems and include, but are not limited to, the following procedures:</p> <ul style="list-style-type: none"> • Active Directory configuration • Server installation • Domain setup • Windows installation • Certificates • Virtual private networks (VPNs) • Service applications 	<p>Inspected the standard build procedures, checklists, and the information security policy to determine that documented standard build procedures were in place for installation and maintenance of customer systems and included the following procedures:</p> <ul style="list-style-type: none"> • Active Directory configuration • Server installation • Domain setup • Windows installation • Certificates • VPNs • Service applications 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.2	Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected information security policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
CC7.1.3	Systems are configured to log access attempts and events and send the logs to a centralized log server. Support personnel are notified when predefined access attempt thresholds are exceeded.	Inspected the audit logging configurations, an example log, and an alert notification generated during the period to determine that systems were configured to log access attempts and events and send the logs to a centralized log server and that support personnel were notified when predefined access attempt thresholds were exceeded.	No exceptions noted.
CC7.1.4	Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the security monitoring system configurations and an example review to determine that security monitoring applications and manual reviews were utilized to monitor and analyze the in-scope systems for possible or actual security breaches.	No exceptions noted.
CC7.1.5	The security monitoring applications are configured to alert IT personnel when certain defined thresholds have been reached.	Inspected the monitoring system configurations and an example alert to determine that the security monitoring applications were configured to alert IT personnel when certain defined thresholds had been reached.	No exceptions noted.
CC7.1.6	An IPS is utilized to analyze and report network events.	Inspected the IPS configurations and an example alert to determine that an IPS was utilized to analyze and report network events.	No exceptions noted.
CC7.1.7	IT personnel perform internal vulnerability scans on a quarterly basis to monitor and analyze the in-scope systems for possible or actual security breaches.	Inspected the internal vulnerability scan results for a sample of quarters within the period and with the assistance of director of information security to determine that IT personnel performed internal vulnerability scans on a quarterly basis to monitor and analyze the in-scope systems for possible or actual security breaches for each quarter sampled.	No exceptions noted.
CC7.1.8	A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results performed during the period to determine that a third-party performed a penetration testing annually during the period to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.9	Management reviews reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the ISBLC meeting agenda and minutes for a sample of quarters during the period to determine that management reviewed reports on a quarterly basis during the period and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes for each quarter sampled.	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.			
CC7.2.1	Documented incident management procedures including the process for informing the entity about breaches of the system security and for submitting complaints is communicated to employees and authorized users.	Inspected the incident management policies and procedures to determine that the incident management procedures included the process for informing the entity about breaches of system security and for submitting complaints was communicated to employees and authorized users.	No exceptions noted.
CC7.2.2	Incidents are documented and tracked in a standardized ticketing system and are updated to reflect the incident and problem, and the resolution is communicated to affected users.	Inspected security incident tickets for a sample of security incident tickets closed within the period to determine that incidents were documented and tracked in a standardized ticketing system during the period and were updated to reflect the planned incident and problem, resolution, and was communicated to affected users for each sample selected.	No exceptions noted.
CC7.2.3	Systems are configured to log access attempts and events and send the logs to a centralized log server. Support personnel are notified when predefined access attempt thresholds are exceeded.	Inspected the audit logging configurations, an example log, and an alert notification generated during the period to determine that systems were configured to log access attempts and events and send the logs to a centralized log server and that support personnel were notified when predefined access attempt thresholds were exceeded.	No exceptions noted.
CC7.2.4	The security monitoring applications are configured to alert IT personnel when certain defined thresholds have been reached.	Inspected the monitoring system configurations and an example alert to determine that the security monitoring applications were configured to alert IT personnel when certain defined thresholds had been reached.	No exceptions noted.
CC7.2.5	An IPS is utilized to analyze and report network events.	Inspected the IPS configurations and an example alert to determine that an IPS was utilized to analyze and report network events.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.6	<p>A central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations with the following configurations:</p> <ul style="list-style-type: none"> Scan for updates to antivirus definitions and update registered customers on a daily basis Scan registered customers on a weekly basis 	<p>Inquired of the compliance manager regarding antivirus configurations to determine that a central antivirus server is configured with antivirus software to protect registered production Windows servers and workstations with the following configurations:</p> <ul style="list-style-type: none"> Scan for updates to antivirus definitions and update registered customers on a daily basis Scan registered customers on a weekly basis 	No exceptions noted.
		<p>Inspected the enterprise antivirus software configurations to determine that a central antivirus server was configured with antivirus software to protect registered production Windows servers and workstations with the following configurations:</p> <ul style="list-style-type: none"> Scan for updates to antivirus definitions and update registered customers on a daily basis Scan registered customers on a weekly basis 	No exceptions noted.
CC7.2.7	<p>A digital surveillance system is in place to record activity in the data centers.</p>	<p>Observed the digital surveillance system for the in-scope data centers to determine that a digital surveillance system was in place to record activity in the data centers.</p>	No exceptions noted.
		<p>Inspected the archived video logs for the in-scope data centers surveillance cameras to determine that a digital surveillance system was in place to record activity in the data centers.</p>	No exceptions noted.
CC7.2.8	<p>TAC personnel are staffed at the data center facilities 24x7 to monitor facility access and log visitors.</p>	<p>Inquired of the infrastructure manager regarding data center staffing to determine that TAC personnel were staffed at the data center facilities 24x7 to monitor facility access and log visitors.</p>	No exceptions noted.
		<p>Inspected the support personnel staffing schedule for the in-scope data centers for a sample of days during the period to determine that TAC personnel were staffed at the data center facilities 24x7 to monitor facility access and log visitors.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.9	Management reviews reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the ISBLC meeting agenda and minutes for a sample of quarters during the period to determine that management reviewed reports on a quarterly basis during the period and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes for each quarter sampled.	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.			
CC7.3.1	Documented incident management procedures including the process for informing the entity about breaches of the system security and for submitting complaints is communicated to employees and authorized users.	Inspected the incident management policies and procedures to determine that the incident management procedures included the process for informing the entity about breaches of system security and for submitting complaints was communicated to employees and authorized users.	No exceptions noted.
CC7.3.2	Incidents are documented and tracked in a standardized ticketing system and are updated to reflect the incident and problem, and the resolution is communicated to affected users.	Inspected security incident tickets for a sample of security incident tickets closed within the period to determine that incidents were documented and tracked in a standardized ticketing system during the period and were updated to reflect the planned incident and problem, resolution, and was communicated to affected users for each sample selected.	No exceptions noted.
CC7.3.3	A post incident report is performed for incidents to determine the root cause, system impact and resolution.	Inspected security incident tickets for a sample of security incident tickets closed within the period to determine that a post incident report was performed for incidents to determine the root cause, system, system impact and resolution for each sample selected.	No exceptions noted.
CC7.3.4	Management reviews reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the ISBLC meeting agenda and minutes for a sample of quarters during the period to determine that management reviewed reports on a quarterly basis during the period and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC7.4.1	Documented incident management procedures including the process for informing the entity about breaches of the system security and for submitting complaints is communicated to employees and authorized users.	Inspected the incident management policies and procedures to determine that the incident management procedures included the process for informing the entity about breaches of system security and for submitting complaints was communicated to employees and authorized users.	No exceptions noted.
CC7.4.2	The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the incident response and escalation procedures to determine that the incident response and escalation procedures were reviewed at least annually during the period for effectiveness.	No exceptions noted.
CC7.4.3	Incidents are documented and tracked in a standardized ticketing system and are updated to reflect the incident and problem, and the resolution is communicated to affected users.	Inspected security incident tickets for a sample of security incident tickets closed within the period to determine that incidents were documented and tracked in a standardized ticketing system during the period and were updated to reflect the planned incident and problem, resolution, and was communicated to affected users for each sample selected.	No exceptions noted.
CC7.4.4	A post incident report is performed for incidents to determine the root cause, system impact and resolution.	Inspected security incident tickets for a sample of security incident tickets closed within the period to determine that a post incident report was performed for incidents to determine the root cause, system, system impact and resolution for each sample selected.	No exceptions noted.
CC7.4.5	Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inspected security incident tickets for a sample of security incident tickets closed within the period to determine that incidents resulting in the unauthorized use or disclosure of personal information were communicated to the affected users for each sample selected.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.6	Management reviews reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the ISBLC meeting agenda and minutes for a sample of quarters during the period to determine that management reviewed reports on a quarterly basis during the period and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes for each quarter sampled.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented incident management procedures including the process for informing the entity about breaches of the system security and for submitting complaints is communicated to employees and authorized users.	Inspected the incident management policies and procedures to determine that the incident management procedures included the process for informing the entity about breaches of system security and for submitting complaints was communicated to employees and authorized users.	No exceptions noted.
CC7.5.2	The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: <ul style="list-style-type: none"> Rebuilding systems Updating software Installing patches Removing unauthorized access Changing configurations 	Inspected the information security policy, the vulnerability management standard, the change management policies and procedures and standard build procedure document and checklists to determine that the entity restored system operations for incidents impacting the environment through activities that included: <ul style="list-style-type: none"> Rebuilding systems Updating software Installing patches Removing unauthorized access Changing configurations 	No exceptions noted.
CC7.5.3	An automated backup system is utilized to perform scheduled system backups.	Inspected the automated backup system configurations and an example backup log to determine that an automated backup system was utilized to perform scheduled system backups.	No exceptions noted.
CC7.5.4	IT personnel perform restoration of backup files as a component of business operations.	Inquired of the compliance manager regarding backup restoration procedures to determine that IT personnel performed restoration of backup files as a component of business operations.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recently completed backup restore during the period to determine that IT personnel performed restoration of backup files as a component of business operations.	No exceptions noted.
CC7.5.5	Management reviews reports on a quarterly basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the ISBLC meeting agenda and minutes for a sample of quarters during the period to determine that management reviewed reports on a quarterly basis during the period and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes for each quarter sampled.	No exceptions noted.
CC7.5.6	Incidents are documented and tracked in a standardized ticketing system and are updated to reflect the incident and problem, and the resolution is communicated to affected users.	Inspected security incident tickets for a sample of security incident tickets closed within the period to determine that incidents were documented and tracked in a standardized ticketing system during the period and were updated to reflect the planned incident and problem, resolution, and was communicated to affected users for each sample selected.	No exceptions noted.
CC7.5.7	A post incident report is performed for incidents to determine the root cause, system impact and resolution.	Inspected security incident tickets for a sample of security incident tickets closed within the period to determine that a post incident report was performed for incidents to determine the root cause, system, system impact and resolution for each sample selected.	No exceptions noted.
CC7.5.8	A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the resumption of essential operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the resumption of essential operations.	No exceptions noted.
CC7.5.9	The disaster recovery plan is tested on an annual basis.	Inspected the completed disaster recovery test results performed during the period to determine that the disaster recovery plans were tested on an annual basis during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC8.1.1	<p>Policies and procedures are in place to guide personnel in documenting, scheduling, and performing infrastructure changes and maintenance activities that address the following:</p> <ul style="list-style-type: none"> • Risk classifications • Priority classifications • Required documentation • Approvals • Customer notifications 	<p>Inspected the change management policies and procedures to determine that policies and procedures were in place to guide personnel in documenting, scheduling, and performing infrastructure changes and maintenance activities that addressed the following:</p> <ul style="list-style-type: none"> • Risk classifications • Priority classifications • Required documentation • Approvals • Customer notifications 	No exceptions noted.
CC8.1.2	<p>Operations and support personnel utilize a change management application to centrally track infrastructure change requests and maintenance activities.</p>	<p>Inspected the service management system, a listing of infrastructure changes, and the request ticket for a sample of infrastructure changes implemented during the period to determine that operations and support personnel utilized a service management system to centrally track infrastructure change requests and maintenance activities for each change sampled during the period.</p>	No exceptions noted.
CC8.1.3	<p>Infrastructure change requests and maintenance activities are documented using standardized forms within the change management application. These forms include, but are not limited to, the following:</p> <ul style="list-style-type: none"> • Individual requesting the change • Description of the change and business reason • Projected risk level • Affected facilities, systems, and components 	<p>Inspected the service management system, a listing of infrastructure changes, and the request ticket for a sample of infrastructure changes implemented during the period to determine that infrastructure change requests and maintenance activities were documented using standardized forms within the service management system for each change sampled during the period. These forms included the following:</p> <ul style="list-style-type: none"> • Individual requesting the change • Description of the change and business reason • Projected risk level • Affected facilities, systems, and components 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.4	Managers and staff perform an impact assessment for infrastructure changes and maintenance activities that is documented within the change management tracking application.	Inspected the service management system, a listing of infrastructure changes, and the request ticket for a sample of infrastructure changes implemented during the period to determine that managers and staff performed an impact assessment for infrastructure changes and maintenance activities that was documented within the service management system for each change sampled during the period.	No exceptions noted.
CC8.1.5	Management approvals are documented within the change management tracking application.	Inspected the service management system, a listing of infrastructure changes, and the request ticket for a sample of infrastructure changes implemented during the period, and the change management policy to determine that management approvals were documented within the service management system for each change sampled during the period.	No exceptions noted.
CC8.1.6	Infrastructure changes and maintenance activities are documented, tested, as applicable, and approved in accordance with the change management policy.	Inspected the change management policy, the service management system, a listing of infrastructure changes, and the request ticket for a sample of infrastructure changes implemented during the period to determine that infrastructure changes and maintenance activities were documented, tested, as applicable, and approved in accordance with the change management policy for each sample selected during the period.	No exceptions noted.
CC8.1.7	Support personnel provide customers with written notifications of maintenance activities in advance of scheduled changes.	Inspected the customer change notification for a sample of infrastructure changes implemented during the period to determine that support personnel provided customers with written notifications of maintenance activities in advance of scheduled changes for each change sampled during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.8	Backout procedures are documented for each infrastructure change implementation to allow for rollback of changes when changes impair system operation.	Inspected the service management system, a listing of infrastructure changes, and the request ticket for a sample of infrastructure changes implemented during the period to determine that backout procedures were documented for each infrastructure change implementation to allow for rollback of changes when changes impair system operation for each change sampled during the period.	No exceptions noted.
CC8.1.9	Development and test environments are physically and logically separated from the production environment.	Inspected the separate environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
CC8.1.10	The entity creates test data that replaces confidential information with test information during the change management process.	Inquired of the compliance manager regarding the use of test data to determine that the entity created test data that replaced confidential information with test information during the change management process.	No exceptions noted.
		Inspected the test data to determine that the entity created test data that replaced confidential information with test information during the change management process.	No exceptions noted.
CC8.1.11	The ability to implement changes into the production environment is restricted to user accounts accessible by authorized personnel.	Inspected the listing of user accounts with the ability to implement changes to the production environment with the assistance of the compliance manager to determine that the ability to implement changes into the production environment was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.12	Change management meetings are held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system.	Inspected the recurring change management meeting calendar invitation and the meeting notes during the period with the assistance of the compliance manager to determine that change management meetings were held during the period to discuss and communicate the ongoing and upcoming projects that affect the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.	Inspected the risk management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities.	No exceptions noted.
CC9.1.2	Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	Inspected the information security management policies and procedures to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	No exceptions noted.
CC9.1.3	A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the most recently completed risk assessment performed during the period to determine that a formal risk assessment was performed during the period to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
CC9.1.4	Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the information security management policies and procedures to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Inspected the most recently completed risk assessment performed during the period to determine that identified risks were rated using a risk evaluation process and ratings were approved by management during the period.	No exceptions noted.
CC9.1.5	Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the information security management policies and procedures and the most recently completed risk assessment performed during the period to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the vendor risk assessment policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.
CC9.2.2	Management develops third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	Inspected the vendor risk assessment policies and procedures to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.
		Inspected the most recently completed risk assessment performed during the period to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process during the period.	No exceptions noted.
CC9.2.3	Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor risk assessment policies and procedures to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Inspected the most recently completed risk assessment performed during the period to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management during the period.	No exceptions noted.
CC9.2.4	Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inquired with the compliance manager regarding the third-party attestation reports to determine that management obtained and reviewed attestation reports of vendors and third parties.	No exceptions noted.
		Inspected the third-party attestation reports for a sample of high risk third parties during the period to determine that management obtained and reviewed attestation reports of vendors and third parties for each sample selected during the period.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
A1.1.1	<p>Documented incident response and support procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting managed and network services and include the following:</p> <ul style="list-style-type: none"> Severity level definitions Escalation procedures Response time requirements for service alerts 	<p>Inspected the incident response and support procedures to determine that documented incident response and support procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting managed and network services and included the following:</p> <ul style="list-style-type: none"> Severity level definitions Escalation procedures Response time requirements for service alerts 	No exceptions noted.
A1.1.2	<p>An enterprise monitoring application is utilized to monitor the following:</p> <ul style="list-style-type: none"> Availability of the network, host services and ports IP packet transmissions and latency Bandwidth utilization and performance CPU and hard disk utilization 	<p>Inquired of the compliance manager regarding the enterprise monitoring application to determine that an enterprise monitoring application was utilized to monitor the following:</p> <ul style="list-style-type: none"> Availability of the network, host services and ports IP packet transmissions and latency Bandwidth utilization and performance CPU and hard disk utilization 	No exceptions noted.
		<p>Inspected the enterprise monitoring application configurations to determine that an enterprise monitoring application was utilized to monitor the following:</p> <ul style="list-style-type: none"> Availability of the network, host services and ports IP packet transmissions and latency Bandwidth utilization and performance CPU and hard disk utilization 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1.3	The monitoring application is configured to generate reports for ongoing monitoring of performance metrics and service levels including, but not limited to, the following: <ul style="list-style-type: none">• Availability• Alert history• Trend analysis reports	Inspected the enterprise monitoring application configurations and an example summary report to determine that the monitoring application was configured to generate reports for ongoing monitoring of performance metrics and service levels including the following: <ul style="list-style-type: none">• Availability• Alert history• Trend analysis reports	No exceptions noted.
A1.1.4	Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed.	Inquired of the compliance manager regarding compliance assessments to determine that management tracked vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed.	No exceptions noted.
		Inspected the most recent executive committee meeting and the risk assessment performed during the period to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed.	No exceptions 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.			
A1.2.1	Documented policies and procedures are in place to govern environmental security practices and responses to certain environmental security events.	Inspected environmental security policies and procedures to determine that documented policies and procedures were in place to govern environmental security practices and responses to certain environmental security events.	No exceptions noted.
A1.2.2	Environmental monitoring systems are utilized to monitor the environmental systems and conditions within the data centers including, but not limited to, the following: <ul style="list-style-type: none">• Fire alarm status and suppression systems• Temperature• Humidity and air quality• Power levels and availability	Inquired of the infrastructure manager regarding the environmental monitoring systems to determine that environmental monitoring systems were utilized to monitor the environmental systems and conditions within the data centers including, but not limited to, the following: <ul style="list-style-type: none">• Fire alarm status and suppression systems• Temperature• Humidity and air quality• Power levels and availability	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Observed the use of the environmental monitoring system for the in-scope data centers to determine that environmental monitoring systems were utilized to monitor the environmental systems and conditions within the data centers including, but not limited to, the following:</p> <ul style="list-style-type: none"> • Fire alarm status and suppression systems • Temperature • Humidity and air quality • Power levels and availability 	No exceptions noted.
A1.2.3	The environmental monitoring application is monitored via on-screen alert notifications if certain predefined thresholds are exceeded on monitored systems.	Inquired of the infrastructure manager regarding monitoring to determine that the environmental monitoring application was monitored via on-screen alert notifications if certain predefined thresholds were exceeded on monitored systems.	No exceptions noted.
		Observed the use of the environmental monitoring system for the in-scope data centers to determine that the environmental monitoring application was monitored via on-screen alert notifications if certain predefined thresholds were exceeded on monitored systems.	No exceptions noted.
A1.2.4	Daily patrols are performed to monitor and record readings from certain environmental equipment.	Inquired of the compliance manager regarding daily patrols to determine that daily patrols were performed to monitor and record readings from certain environmental equipment.	No exceptions noted.
		Observed the daily patrol process for the in-scope data centers to determine that daily patrols were performed to monitor and record readings from certain environmental equipment.	No exceptions noted.
		Inspected environmental security policies and procedures to determine that daily patrols were performed to monitor and record readings from certain environmental equipment.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.5	<p>The data centers are protected by the following fire detection and suppression controls:</p> <ul style="list-style-type: none"> • Audible and visual fire alarms • Pre-action dry-pipe water sprinklers and/or agent-based fire suppression system • Fire and smoke detectors • Hand-held fire extinguishers 	<p>Observed the fire protection equipment for the in-scope data centers to determine that the data centers were protected by the following fire detection and suppression controls:</p> <ul style="list-style-type: none"> • Audible and visual fire alarms • Pre-action dry-pipe water sprinklers and/or agent-based fire suppression system • Fire and smoke detectors • Hand-held fire extinguishers 	No exceptions noted.
A1.2.6	Management obtains inspection reports to ensure that third-party specialists inspect the fire detection and suppression systems on an annual basis.	Inspected the most recently completed fire detection and suppression systems maintenance records for the in-scope data centers during the period to determine that management obtained inspection reports to ensure that third-party specialists inspected the fire detection and suppression systems during the period.	No exceptions noted.
A1.2.7	The data centers are equipped with multiple air conditioning units to regulate temperature and humidity.	Inquired of the infrastructure manager regarding temperature and humidity control in the data centers to determine that the data centers were equipped with multiple air conditioning units to regulate temperature and humidity.	No exceptions noted.
		Observed the air conditioning units for the in-scope data centers to determine that the data centers were equipped with multiple air conditioning units to regulate temperature and humidity.	No exceptions noted.
A1.2.8	Management obtains inspection reports to ensure that third-party specialists inspect the air conditioning units on at least an annual basis.	Inspected the most recently completed air conditioning unit maintenance records for the in-scope data centers during the period to determine that management obtained inspection reports to ensure that third-party specialists inspected the air conditioning units during the period.	No exceptions noted.
A1.2.9	The data centers are equipped with water detection devices to detect and mitigate water damage in the event of a flood or water leak.	Inquired of the infrastructure manager regarding temperature and humidity control in the data centers to determine that the data centers were equipped with water detection devices to detect and mitigate water damage in the event of a flood or water leak.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the water detection devices for of the in-scope data centers to determine that the data centers were equipped with water detection devices to detect and mitigate water damage in the event of a flood or water leak.	No exceptions noted.
A1.2.10	The data centers are connected to multiple redundant UPS systems configured to provide temporary electricity in the event of a power outage.	Inquired of the infrastructure manager regarding the UPS systems to determine that the data centers were connected to multiple redundant UPS systems configured to provide temporary electricity in the event of a power outage.	No exceptions noted.
		Observed the UPS systems for the in-scope data centers to determine that the data centers were connected to multiple redundant UPS systems configured to provide temporary electricity in the event of a power outage.	No exceptions noted.
A1.2.11	Management obtains inspection reports and/or invoices to ensure that third-party specialists inspect the UPS systems on a semi-annual basis.	Inspected the most recently completed UPS system maintenance records performed for the in-scope data centers during the period to determine that management obtained inspection reports and/or invoices to ensure that third-party specialists inspected the UPS systems on a semi-annual basis during the period.	No exceptions noted.
A1.2.12	The data centers are equipped with fueled electric power generators to provide backup power in the event of a power outage.	Inquired of the infrastructure manager regarding the generators to determine that the data centers were equipped with fueled electric power generators to provide backup power in the event of a power outage.	No exceptions noted.
		Observed the generators for the in-scope data centers to determine that the data centers were equipped with fueled electric power generators to provide backup power in the event of a power outage.	No exceptions noted.
A1.2.13	The fueled electric power generators are inspected on a semi-annual basis and the inspection report is retained as evidence of completion.	Inspected the most recently completed generator maintenance records for the in-scope data centers during the period to determine that the fueled electric power generators were inspected on a semi-annual basis during the period and the inspection report was retained as evidence of completion.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.14	Management obtains inspection reports to ensure that generators are load tested on a semi-annual basis.	Inspected the most recently completed generator maintenance records performed for the in-scope data centers during the period to determine that management obtained inspection reports to ensure that generators were load tested on a semi-annual basis during the period.	No exceptions noted.
A1.2.15	An automated backup system is utilized to perform scheduled system backups.	Inspected the automated backup system configurations and an example backup log generated during the period to determine that an automated backup system was utilized to perform scheduled system backups.	No exceptions noted.
A1.2.16	When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inspected backup notification configurations and an example backup alert generated during the period to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	No exceptions noted.
	Equinix is expected to implement control activities for ensuring the following equipment is in place for each facility: <ul style="list-style-type: none">• Fire detection and suppression• Power management		
	Equinix is expected to implement control activities for performing scheduled maintenance procedures to ensure that: <ul style="list-style-type: none">• Fire detection and suppression equipment is working properly• Test and confirm the operation of power maintenance systems• HVAC equipment, cooling equipment, and leak detection sensors are working properly		
	Equinix is expected to implement control activities for maintaining and monitoring temperature and humidity throughout the facilities through the use of air conditioning and ventilation equipment.		
	Equinix is expected to implement control activities for monitoring the facilities 24x7 and that staff members are in place either on site or on call 24x7 who are alerted by the building management system (BMS) for system exceptions.		
	Equinix is expected to implement control activities for implementing emergency procedures to help guide personnel in protecting against disruptions caused by an unexpected event.		
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the resumption of essential operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the resumption of essential operations.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A.1.3.2	Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis during the period.	No exceptions noted.
A1.3.3	The disaster recovery plan is tested on an annual basis.	Inspected the completed disaster recovery test results performed during the period to determine that the disaster recovery plan was tested on an annual basis during the period.	No exceptions noted.
A1.3.4	IT personnel perform restoration of backup files as a component of business operations.	Inquired of the IT manager regarding backup restoration procedures to determine that IT personnel performed restoration of backup files as a component of business operations.	No exceptions noted.
		Inspected the most recently completed backup restore performed during the period with the assistance of the compliance manager to determine that IT personnel performed restoration of backup files as a component of business operations during the period.	No exceptions noted.

ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	<p>Documented confidential policies and procedures are in place that include the following:</p> <ul style="list-style-type: none"> Defining, identifying, and designating information as confidential Storing confidential information Protecting confidential information from erasure or destruction Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed 	<p>Inspected the data protection and information security policies and procedures to determine that documented confidential policies and procedures were in place that included:</p> <ul style="list-style-type: none"> Defining, identifying, and designating information as confidential Storing confidential information Protecting confidential information from erasure or destruction Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1.2	An inventory log is maintained of assets with confidential data.	Inspected the inventory log to determine that an inventory log was maintained of assets with confidential data.	No exceptions noted.
C1.1.3	Access to the badging system is limited to authorized employees.	Inquired of the compliance manager regarding access to the badging system to determine that access to the badging system was limited to authorized employees.	No exceptions noted.
		Inspected the information security policy to determine that access to the badging system was limited to authorized employees.	No exceptions noted.
		Inspected the listing of user accounts with authorized access to the badging system to determine that access to the badging system was limited to authorized employees.	No exceptions noted.
C1.1.4	Confidential information is protected from erasure or destruction during the specified retention period.	Inspected the information security policy, the data disposal, and the data retention policy to determine that confidential information was protected from erasure or destruction during the specified retention period.	No exceptions noted.
C1.1.5	Data that entered into the system, processed by the system, and output from the system is protected from unauthorized access.	Inspected the encryption configurations to determine that data entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	<p>Documented data destruction policies and procedures are in place that include the following:</p> <ul style="list-style-type: none"> Identifying confidential information requiring destruction when the end of the retention period is reached Erasing or destroying confidential information that has been identified for destruction 	<p>Inspected the information security policy, data retention policy, and data destruction policies and procedures to determine that documented data destruction policies and procedures were in place that included:</p> <ul style="list-style-type: none"> Identifying confidential information requiring destruction when the end of the retention period is reached Erasing or destroying confidential information that has been identified for destruction 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2.2	An inventory log is maintained of assets with confidential data and is destroyed or purged in accordance with retention policies and procedures.	Inquired of the compliance manager regarding data disposal to determine that an inventory log was maintained of assets with confidential data and was destroyed or purged in accordance with retention policies and procedures.	No exceptions noted.
		Inspected the information security policy, the inventory log, and a sample of assets disposed during the period to determine that an inventory log was maintained of assets with confidential data and was destroyed or purged in accordance with retention policies and procedures for each sample selected during the period.	No exceptions noted.
C1.2.3	Data that is no longer required for business purposes is rendered unreadable.	Inquired of the compliance manager regarding certificate of destruction to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
		Inspected the listing of requests to destroy hard drives and other IT related assets and the certificates of destruction during the period to determine that data that was no longer required for business purposes was rendered unreadable during the period.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY FLEXENTIAL

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control Environment

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.1.3 CC1.5.3	Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the electronic receipt of acknowledgement for a sample of new employees hired during the period to determine that personnel were required to acknowledge the employee handbook and code of conduct upon hire for each sample selected during the period.	The test of the control activity disclosed that acknowledgment of the employee handbook and code of conduct did not occur within 60 days upon hire for two of 25 sampled new employees hired during the period.
Management's Response:	Flexential confirmed both workers completed the required policy acknowledgements. Additional internal controls have been implemented to ensure policy acknowledgements are completed within 60 days of hire per Flexential policy.		

Control Environment / Communication and Information

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC1.4.7 CC2.2.5	Employees are required to attend security awareness training upon hire and annually thereafter.	Inspected the security awareness training completion report for a sample of new employees hired during the period to determine that employees were required to complete security awareness training upon hire for each sample selected during the period.	The test of the control activity disclosed that security awareness training was not completed within 60 days upon hire for three of 25 sampled new employees hired during the period.
Management's Response:	Flexential confirmed three workers completed the required training. Additional internal controls have been implemented to ensure Flexential training requirements are completed within 60 days of hire per Flexential policy.		