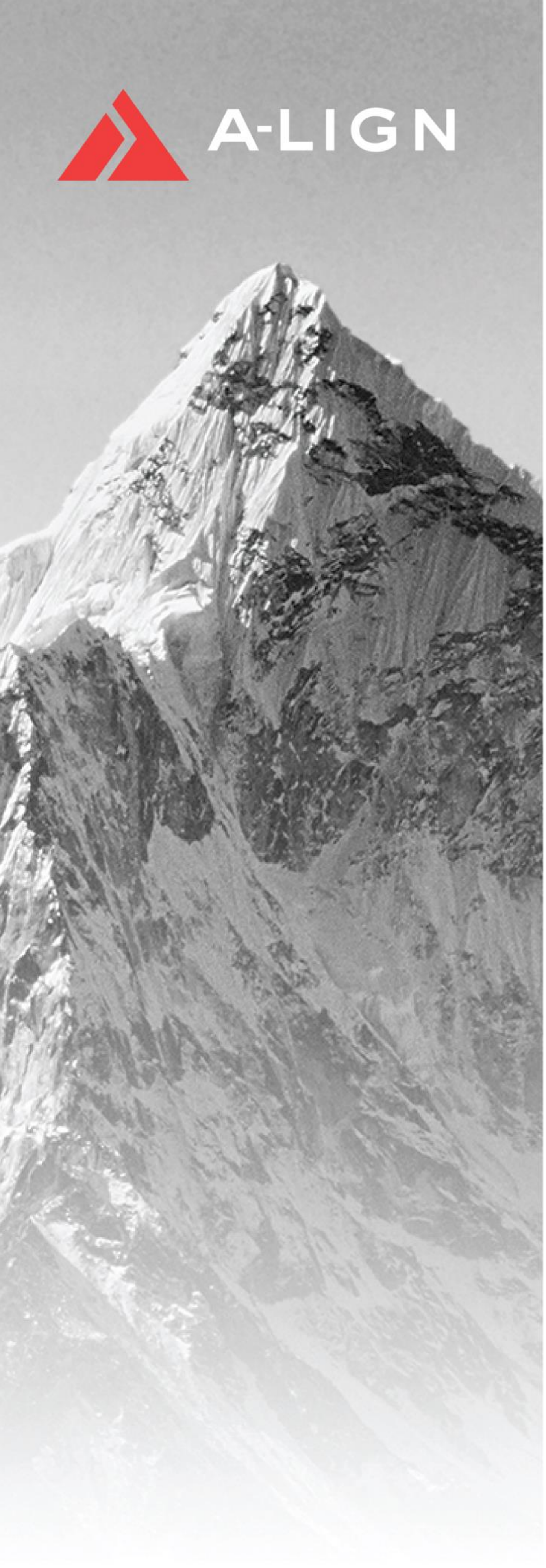

Flexential
Type 2 SOC 3
2020

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

November 1, 2019 To October 31, 2020

Table of Contents

SECTION 1

ASSERTION OF FLEXENTIAL MANAGEMENT

ASSERTION OF FLEXENTIAL MANAGEMENT

November 6, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within Flexential Corp's ('Flexential' or 'the Company') Data Center and Cloud Operations Services System throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that Flexential's service commitments and system requirements relevant to Security, Availability, and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Flexential's Description of Its Data Center and Cloud Operations Services System throughout the period November 1, 2019 to October 31, 2020" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2019 to October 31, 2020, 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, *2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy* (AICPA, *Trust Services Criteria*). Flexential's objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Flexential's Description of Its Data Center and Cloud Operations Services System throughout the period November 1, 2019 to October 31, 2020".

Flexential uses BAE Systems, Inc. to provide managed security monitoring services and Equinix, Inc. and The Westin Building to provide colocation services (collectively, the 'subservice organizations'). 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 organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Flexential's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Flexential's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2019 to October 31, 2020 to provide reasonable assurance that Flexential's service commitments and system requirements were achieved based on the applicable trust services criteria.

David A. Kidd

David A. Kidd
SVP of Governance, Risk & Compliance
Flexential Corp

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Flexential Corp

Scope

We have examined Flexential's accompanying description of Data Center and Cloud Operations Services System titled "Flexential's Description of Its Data Center and Cloud Operations Services System throughout the period November 1, 2019 to October 31, 2020" (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, 2019 to October 31, 2020, 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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Flexential uses BAE Systems, Inc. to provide managed security monitoring services and Equinix, Inc. and The Westin Building to provide colocation services. 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 organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at 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 complementary user entity controls assumed in the design of Flexential's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

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 titled "Assertion of Flexential Management" (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. 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.

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.

Opinion

In our opinion, management's assertion that the controls within Flexential's Data Center and Cloud Operations Services System were suitably designed and operating effectively throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that Flexential's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Flexential’s website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Flexential, user entities of Flexential’s Data Center and Cloud Operations Services during some or all of the period November 1, 2019 to October 31, 2020, business partners of Flexential subject to risks arising from interactions with the Data Center and Cloud Operations Services, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
November 6, 2020

SECTION 3

FLEXENTIAL’S DESCRIPTON OF ITS DATA CENTER AND CLOUD OPERATIONS SERVICES SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2019 TO OCTOBER 31, 2020

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 1,000 employees across the United States. Flexential is headquartered in Charlotte, North Carolina and Denver, Colorado. Flexential's executive management team consists of industry leaders with extensive experience in information technology (IT) services and data center operations.

Description of Services Provided

Flexential's colocation services is provided in 20 geographic markets, across locations within the United States. With 38 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 (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.

The Flexential cloud services are physically hosted at the data centers in Denver, Colorado (Aurora and Englewood); Downtown Salt Lake City, Utah (Delong); Richardson, Texas; Allentown, Pennsylvania; Hillsboro, Oregon (Brookwood); Minneapolis, Minnesota (Chaska); South Charlotte, North Carolina; Atlanta, Georgia (Alpharetta and Norcross); Downtown Louisville, Kentucky; and Nashville, Tennessee (Cool Springs), Seattle, Washington (The Westin Building); and Amsterdam, NL (Equinix) locations. Network managed services are available at all Flexential locations.

Principal Service Commitments and System Requirements

Flexential designs its processes and procedures to meet its objectives for its 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 Data Center and Cloud Operations services, and the financial, operational, and compliance requirements that Flexential has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offerings provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles are built into the fundamental design of the services provided by Flexential and uses role-based access control based on the principal of least privilege.

Flexential establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. 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 and trained. 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 services.

Components of the System

Infrastructure and *Software*

Primary infrastructure and software used to provide Flexential's Data Center and Cloud Operations Services System includes the following:

Primary Infrastructure and Software		
Hardware	**Type**	**Purpose**
Badge Card Access System	Entrapass, Genetec, C-CURE	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 data center 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 2 factor authentication prior to granting access to the data center facilities and the raised floor within the data center facilities.
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.
Management Services Backup Servers	CommVault	Automated backup system software and network of servers that provide backup and recovery for subscribing customers.
Routers and Switches	Cisco NXOS	Routers and switches 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 6.0)	VMware ESX hosts for running customer virtual machines.
Web Portal	Embotics vCommander, ClientCetner, vCloud Director	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 services 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
- Service delivery - 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

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Flexential policies and procedures that define how services should be delivered. These are located on the Company’s intranet and can be accessed by any Flexential team member.

Physical Security

General 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 facilities personnel 24x7x365.

Physical access to each of the Flexential data centers is controlled through various preventative measures. To help ensure that only authorized employees, customers, or vendors have access to the data centers, Flexential has implemented electronic card key systems. In order for any one individual to access the raised floor area, the individual must have a valid and approved access card for that specific data center. After an individual scans his or her card, the individual must also have knowledge of the PIN or the correct biometric reading associated with the badge in order to gain entry to the raised floor area.

After an individual authenticates to the raised floor area, he or she must also have access to the customer’s equipment through the use of another lock and key, badge, PIN, or biometric reader. Each customer is allocated his or her own space through the use of secured racks, cages, or suites.

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

Data is recorded based on activity/motion, up to available memory capacity. The minimum data retention period for critical areas is 90 days online with 1 year backed up. Data center 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. All camera activity is fed to the technical assistance center and monitored by facility personnel. Data center personnel perform facility rounds multiple times throughout the day 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.

Vendor and Customer Access

Customers are accountable to identify individuals, employees or vendors, authorized to access Flexential facilities on their behalf. Access authorization is managed through the customer portal by a customer designated administrator. The customer portal notifies, via a ticket, data center facilities staff that a day or permanent badge needs to be issued. Badges are not issued until the customer representative arrives on-site. At that time, the individual must present a valid government-issued picture ID and sign the data center rules and accountability form, agreeing to the rules of the data center. Vendors who are pre-authorized through the ticketing system must also present a valid ID and sign the data center rules and accountability form.

Physical Security Access Reviews

Physical access reviews are performed quarterly to help ensure that only authorized employees retain physical access. Physical access lists are generated from each data center and are compared to current authorizations and HR reports. Any exceptions noted are recorded and tracked to resolution.

Additionally, management performs quarterly logical access reviews on users who have administrative access to the various physical access badging systems. This review consists of inspecting the user base of administrators to verify that no terminated employees have access to the systems and to verify that users' current access rights are still required and appropriate based on job changes or roles they are currently fulfilling within the organization. Any exceptions identified by management are sent to the administrators of the respective systems for resolution, and the changed access lists are revalidated for completion of the review by management.

Customer Cage Access

Within each data center, customer environments are physically secured within a locked cage, cabinet, or suite. Customer cabinets and cages are secured by keyed locks (keys secured via lock box), combination locks, card readers, biometric devices, and/or keypads per the customer's choice.

Master keys are kept in a secure environment not accessible to customers or vendors. Onsite operational personnel are required to carry master keys, as are data center managers and their direct reports (i.e., those who perform customer installations).

Logical Access - Colocation Services

New or Modified User Access

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. Human Resources provides the hiring manager 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.

Terminated Users

The employee's manager initiates the employee termination process by contacting the Human Resources department. Human Resources processes the termination in Workday which creates a parent ServiceNow ticket for the Technology Services department. Technology Services then revokes the employee's logical access to the Flexential corporate domain. The Human Resources department and/or the employee's manager conducts an exit interview with the terminated employee and collects all Flexential assets. Child tickets are generated from the parent ServiceNow ticket that are assigned to relevant departments to revoke access from all other Flexential facilities, network devices, and systems.

User Access Reviews

To help ensure that access to systems, applications, and network devices remains authorized and appropriate over time, management performs 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 and appropriate 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.

Privileged User Access

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 TACACS+, which is administered via Cisco Access Control Server (ACS). ACS 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 the network devices. Authentication to TACACS+ is controlled through Cisco Secure ACS. 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. Rivest-Shamir-Adleman (RSA) SecurID two-factor authentication is also used for authentication to the network devices. All users have unique usernames and PINs in addition to the token. Authentication tokens change on a fixed interval of 30, 60, or 120 seconds. PINs are not required to change on any fixed schedule.

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 IP addresses to connect to the device.

Password Controls and Security

Access to the network and supporting tools (i.e., the ticketing system) within the colocation environment is restricted by using password authentication guidelines requiring that passwords be a minimum length, conform to complexity requirements, expire periodically, and differ from a previous number of passwords to help prevent unauthorized access.

Network devices are accessed from Flexential-approved IP addresses. The IP addresses are defined on each network device through the use of ACLs. After a user connects to the device from an authorized IP address, the user must authenticate to the device using his or her TACACS+ credentials. The TACACS+ servers require a username and password to access the network device.

Logical Access - Managed and Cloud Services

Access to resources within the managed services environment is controlled via Windows Active Directory domain membership. To access customer servers, Flexential personnel are assigned access to Windows groups, which are then assigned rights on customer servers. To access customer network devices and firewalls, ACLs on each device restrict access to allow only certain IP addresses the ability to connect to the device. The user must also be defined to a specific AD group configured on the ACS tool in order to administer the network devices using Radius. These configurations are defined on each network device. Access to the Flexential Customer Portal uses multi-factor authentication and is granted via membership within the ticketing system, which for Flexential employees uses authentication via the Flexential managed services domain.

New User Access

Permission levels on the managed services and cloud domains are further restricted by different group assignments. Access to the domains is based on the necessity of the job function and must be approved by the employee's manager and/or the security and/or IT operations department before access is granted.

Terminated Users

The employee's manager initiates the employee termination process by contacting the Human Resources department. Human Resources processes the termination in Workday which creates a parent ServiceNow ticket for the Technology Services department who then revokes the employee's logical access to the Flexential corporate domain. Child tickets are generated from the parent ServiceNow ticket that are assigned to relevant departments to revoke access from all other Flexential facilities, network devices, and systems, including the managed services and cloud domains, which effectively disables access to all other tool and resources impacting customer environments.

Privileged User Access and Customer Server Access

For managed services, customer servers utilize either a customer-managed domain or the managed services domain. Administrative access to servers on customer-managed domains is controlled by the customer and the customer is responsible for administering account access to Flexential.

Administrative access to servers managed on the Flexential managed services domain is controlled by Flexential, and access is restricted through domain group membership. Administrative access to Linux servers is controlled via Public Key Infrastructure, and keys are granted to a limited number of Linux engineers who require access to maintain the servers.

User Access Reviews

To help ensure that access to customer systems related to managed services remains authorized and appropriate over time, management performs quarterly logical access reviews on users who have access to the managed services domain and Radius. To help ensure that access to customer systems related to the cloud services remains authorized and appropriate over time, management performs quarterly logical access reviews over users with access to the cloud services domains, and customer Windows and Linux servers.

These reviews consist of inspecting membership to the user bases along with key groups to verify that no terminated employees have access to the systems, and to verify that users' current access rights are still required and appropriate 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.

Password Controls and Security

Access to the managed services and cloud domains and supporting tools is restricted by using password authentication guidelines requiring that passwords be a minimum length, conform to complexity requirements, expire periodically, and differ from a previous number of passwords to help prevent unauthorized access.

Managed Services: Customer-Specific Firewall Security

Customer-specific firewall devices are used within the Managed Services environment. The IP addresses are defined on each device through the use of firewall policies. Each customer firewall is configured with Flexential's default policies and configurations, which restrict access to the minimum monitoring tools and operations personnel necessary. Only customer approved changes will be made to customer firewalls, whether during the initial onboarding or anytime thereafter. Access to customer servers and network devices, including firewalls, is restricted to limited personnel as noted above.

Computer Operations - Backups

All Flexential network devices are backed up nightly. Flexential uses RANCID and Net Line Dancer to track changes to the network device configurations and maintain the most up-to-date copies of the configurations. Flexential uses EMC Avamar, Commvault, Restore24 and Rubrik for monitoring customer server backups. All backups of internal Flexential and subscribing customers' data are replicated to a secondary data center within the Flexential environment. Customer's may subscribe to backup and storage services, which includes tape rotations, automatic backups, and data replication across multiple data centers. Tools are configured to provide alerting to Flexential personnel regarding any incidents or failures related to backups for internal Flexential and subscribing customers' data. Flexential personnel work in tandem with customers to resolve any root cause issues so that backups can be completed successfully going forward.

Network and Internet Availability

Flexential Internet access solutions provide the flexibility and scalability necessary to manage expanding communications and data requirements. These services leverage industry-leading technology to optimize traffic routing to external networks to ensure availability and performance over the Internet. Flexential network services is a fully redundant network with multiple paths for internet and connectivity to other Flexential data centers and third-party carrier hotels.

In addition to bandwidth, value-add and add-on services are available for utilization monitoring, domain name service (DNS) management and IP failover services.

Features include:

- Multiple physical connectivity options including 100 Mbps, 1 Gbps and 10 Gbps network ports in addition to cloud connectivity
- Rapid installation, implementation and service change turnaround times
- Carrier neutrality for private networking needs used to connect Flexential housed resources to other corporate resources and third parties
- Comprehensive, web-based portal for bandwidth usage reporting
- Burstable and fixed limit subscription options
- Add-on managed security services, including firewall, virtual private network (VPN), and intrusion detection systems
- Traffic traverses Flexential's private network without affecting Internet bandwidth usage
- Multiple 10 Gbps private connections between Flexential facilities

Each data center maintains redundant links to the internet and other Flexential data centers. Devices are configured to be monitored in the monitoring tool and are not accessible for management access outside the Flexential network. Additionally, the network design supports redundancy for critical network components, and 24x7 monitoring procedures are in place to monitor Flexential and customer systems. Monitoring systems are redundant to provide failover capability, and current network diagrams are available for use by authorized users.

Change Control

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.

A Change Advisory Board (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. Outages are posted on the Customer Support portal.

Non-routine changes are tested in a test lab and approved by an appropriate manager. To minimize network device configuration problems, tools such as RANCID and Net Line Dancer are utilized to create snapshots of each device configuration. Each night, these tools pull the device configurations in order to have an updated “snapshot” of the device configurations.

Daily, these tools generate e-mail notifications of any devices that have changed since the previous day’s snapshot of configurations. These e-mail notifications go to the network operations team, which reviews these e-mails to verify that appropriate activity is occurring on the network devices.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a 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 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 of 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.

Authorized employees may access the corporate network remotely through the use of leading VPN technology, that requires multifactor authentication. Employees are authenticated into the cloud services system via the virtual desktop infrastructure (vDI) environment, which also requires multifactor authentication for access.

Boundaries of the System

The scope of this report includes the Data Center and Cloud Operations Services System performed in the following facilities:

Data Center	Address
1. Allentown	744 Robel Road, Allentown, PA 18109
2. Atlanta - Alpharetta	12655 Edison Drive, Alpharetta, GA 30022
3. Atlanta - Norcross	2775 Northwoods Parkway, Norcross, GA 30071

4. Charlotte - North	10105 David Taylor Drive, Charlotte NC 28262
5. Charlotte - South	8910 Lenox Pointe Drive, Charlotte, NC 28273
6. Cincinnati	5307 Muhlhauser Road, West Chester Township, OH 45011
7. Dallas - Downtown	1950 North Stemmons Freeway, Suite 2033, Dallas, TX 75207
8. Dallas - Plano	3500 East Plano Parkway, Plano, TX 75074
9. Dallas - Richardson	3010 Waterview Parkway, Richardson, TX 75080
10. Denver - Aurora	11900 East Cornell Avenue, Suite A, Aurora, CO 80014
11. Denver - Centennial	12500 East Arapahoe Road, Suite C, Centennial, CO 80112
12. Denver - Downtown	1500 Champa Street, Suite 100, Denver, CO 80202
13. Denver - Englewood	8636 S Peoria Street, Englewood CO 80112
14. Fort Lauderdale	5301 NW 33rd Ave, Fort Lauderdale, FL 33309
15. Jacksonville	4905 Belfort Road, Suite 145, Jacksonville FL 32256
16. Las Vegas - Downtown	302 East Carson Avenue, Suite 100 DC, Suite 370, Las Vegas, NV 89101
17. Las Vegas - Downtown	304 East Carson Avenue, Las Vegas, NV 89101
18. Las Vegas - North	3330 East Lone Mountain Road, North Las Vegas, NV 89081
19. Louisville - Downtown	752 Barret Avenue, Louisville, KY 40204
20. Louisville - East	2101 Nelson Miller Parkway, Louisville, KY 40223
21. Minneapolis - Chaska	3500 Lyman Blvd, Chaska, MN 55318
22. Nashville - Brentwood	7100 Commerce Way, Brentwood, TN 37027
23. Nashville - Cool Springs	425 Duke Drive, Franklin, TN 37067
24. Nashville - Franklin	4600 Carothers Parkway, Franklin, TN 37067
25. Philadelphia - Collegeville	101 Troutman Rd, Collegeville, PA 19426
26. Phoenix - Deer Valley	1850 W. Deer Valley Road, Phoenix, AZ 85027
27. Portland - Hillsboro 1	3935 NW Aloclek Place, Bldg.C-100, Hillsboro, OR 97124
28. Portland - Hillsboro 2	5737 NE Huffman Street, Hillsboro OR 97124
29. Raleigh	5150 McCrimmon Parkway, Morrisville, NC 27560
30. Richmond	8851-B Park Central Drive, Richmond, VA 23227
31. Salt Lake City - Cottonwood	6340 South 3000 East, Suite 150, Salt Lake City, UT 84121

32. Salt Lake City - Downtown	572 South Delong Street, Salt Lake City, UT 84104
33. Salt Lake City - Fair Park	118 South 1000 West, Salt Lake City, UT 84104
34. Salt Lake City - Lindon	333 South 520 West, Suite 150, Lindon, UT 84042
35. Salt Lake City - Millcreek	3949 South 200 East, Suite B1, Murray, UT 84107
36. Salt Lake City - South Valley	7202 South Campus View Drive, West Jordan, UT 84084
37. Tampa - North	8350 Park Edge Dr, Tampa, FL 33637
38. Tampa - West	9417 Corporate Lake Dr, Tampa, FL 33634
39. Amsterdam (Equinix)	Luttenbergweg 4, 1101 EC Amsterdam NL (Equinix)
40. Seattle (The Westin Building)	2001 6th Avenue, Seattle, WA 98121 (Westin)

This report does not include the managed security monitoring services provided by BAE Systems, Inc. or the colocation services provided by Equinix, Inc. and The Westin Building.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

Integrity and strong ethical values are essential business qualities and are fundamental to the success of Flexential. Employees and contingent workers demonstrate their commitment to these values in their daily work performance, sensitive information handling, abiding by non-disclosure agreements, and compliance with all Flexential policies and procedures. Potential violations or exceptions to these values must be immediately reported to the Employee Ethics & Compliance hotline.

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.

Management's Philosophy and Operating Style

Flexential's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific 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 to discuss major initiatives and issues that affect the business as a whole

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 appropriate business practices, knowledge, and experience required of key personnel and resources are communicated to employees for carrying out their duties.

Human Resources Policies and Practices

The Human Resources 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's approach to customer service begins with its staff. The organization has attracted and retained a diversified group of experienced professionals. Flexential's hiring practices are designed to help ensure that new employees are qualified for their job responsibilities. Flexential's hiring policies and guidelines assist in selecting qualified applicants for specific job responsibilities. Employee training is accomplished through supervised on-the-job training, formal in-house training courses, online learning, and external continuing education programs. Department managers are responsible for overseeing the training and development of qualified employees for current and future responsibilities.

Background checks are required for Flexential employees, regardless of job function. Applicants first complete an application and an Authorization Check Form (for the background check). The background check is sent to a third-party vendor, which then runs Social Security, criminal (local, national, and federal), and Office of Foreign Assets Control (OFAC) checks; employment history verification; and a motor vehicle check on the individual. Credit checks are conducted for potential employees in certain finance roles. Background checks are obtained prior to the finalization of an offer. In addition, offer letters mention that offers are pending satisfactory background and reference checks in case an issue arises in the future.

Formal performance reviews are conducted on a regular basis. During these reviews, employees are evaluated based upon the responsibilities of their particular job and the values of the company.

Employees are required to meet stated performance and attendance standards and to follow Flexential's policies and procedures.

New hires meet with the Human Resources Department within their first two days and review new hire information, including the confidentiality agreement. If the agreement is not signed within 48 hours of hiring, the new employee cannot report to work until the document has been signed.

All Flexential personnel are required to attend security training. Additional training in facilities operations, safety, and security is also required for staff in data center operational support roles. Required training must be completed, and management's approval for permanent access is required to document and track permanent data center access authorizations. Also, periodic security update training decks are created by management and distributed to employees.

Risk Assessment Process

Flexential has placed into operation a risk assessment process to identify and manage risks that could affect Flexential's ability to provide services to its customers. This process requires management to identify significant risks in its areas of responsibility and to implement appropriate measures to address these risks. Operations management meets periodically, usually monthly, 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 bi-monthly meetings to discuss any issues that occurred during the prior weeks and what improvements can be made in operations to help prevent the issue from occurring again. The meeting consists of team leads, managers, and directors from Flexential's Operations group.

Information accumulated and discussed during monthly operations and weekly meetings is also fed into the other meetings that are held quarterly, such as the security governance 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 and availability obligations to its customers. The meetings consist of individuals from various groups throughout the organization, but primarily consist of representatives from Legal, Security, Information Technology, Human Resources, Engineering, and Operations.

Integration with Risk Assessment

Along with assessing risks, Flexential has identified and put into effect actions needed to address those risks. Risks are addressed through control activities that 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 those objectives.

Information and Communications Systems

Flexential has implemented mechanisms to track and record operational data to make strategic decisions and ensure objectives are consistently achieved. Information gathered from systems enable Flexential to understand business trends in order to maximize efforts and provide optimal services.

Monitoring Controls

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:

1. Capacity:
    - Power
    - Space
    - Cooling
    - Generator
    - Network
    - Servers
2. Quality of service:
    - Network uptime
    - Backbone availability
    - Facility uptime
3. Operations Center:
    - Support call answer speeds
    - Support call volumes
    - Average talk time

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 appropriate measures. Monitoring of risks is coordinated through various security and operational committees.

Reporting 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 internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incident Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common, Availability, and Confidentiality criterion were applicable to the Flexential Data Center and Cloud Operations Services System.

Subservice Organizations

This report does not include the managed security monitoring services provided by BAE Systems, Inc. or the colocation services provided by Equinix, Inc. and The Westin Building.

Subservice Description of Services

BAE Systems, Inc. provides security appliances, network monitoring and security services including intrusion detection, logging, monitoring, and reporting through a staffed security operations center.

Equinix, Inc. and The Westin Building provides Colocation Services supporting Flexential operations in data centers as noted above.

Complementary Subservice Organization Controls

Flexential's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organizations controls.
It is not feasible for all of the control objectives related to Flexential's services to be solely achieved by Flexential control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Flexential.

The following subservice organization controls should be implemented by BAE Systems, Inc., Equinix, Inc. and The Westin Building to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - BAE Systems, Inc.		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.1, CC6.6, CC6.7,	An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.

Subservice Organization - BAE Systems, Inc.		
Category	**Criteria**	**Control**
	CC7.1, CC7.2	The IDS is configured to notify personnel upon intrusion detection.

Subservice Organizations - Equinix, Inc. and The Westin Building		
Category	Criteria	Control
Common Criteria/Security	CC6.4	Physical access control systems are in place 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.
		Procedures exist and are followed to establish and make changes to physical access privileges for customers.
		For visitors, customers, vendors, and contractors, security personnel review a government issued ID prior to allowing access to the facilities.
		A termination form is completed, and physical access is revoked for employees as a component of the employee termination process.
Availability	A1.2	Fire detection and suppression equipment is in place at each facility.
		Scheduled maintenance procedures are performed to ensure that fire detection and suppression equipment is working properly.
		Power management equipment is in place for each facility.
		Scheduled maintenance procedures are performed to test and confirm the operation of the power management systems.
		Temperature and humidity is monitored and required temperature is maintained throughout the facilities through the use of air conditioning and ventilation equipment.
		Scheduled maintenance procedures are performed to help ensure that HVAC equipment, cooling equipment, and leak detection sensors are working properly.
		Facilities are monitored 24x7 by facilities engineers. Staff are in place either on-site or on call 24x7 who are alerted by the BMS for system exceptions.
		Emergency procedures are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.

Flexential management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as service level agreements. In addition, Flexential performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations
- Reviewing attestation reports over services provided by vendors and subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

Flexential’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Flexential’s services to be solely achieved by Flexential control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Flexential.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities’ locations, user entities’ auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for following the physical access procedures outlined in the customer agreement for visits to all data centers, and ensuring their cabinets are locked and their equipment is secured prior to leaving the premises. User entities are responsible for maintaining their own system(s) of record.
2. User entities are responsible for timely response to known or suspected incidents reported by Flexential personnel.
3. User entities are responsible for testing and performing backup restorations.
4. User entities are responsible for implementing their own access control and authentication systems on their infrastructure.
5. User entities are responsible for implementing monitoring controls to detect and alert the user entity of actual or attempted security breaches to their network(s) and infrastructure.
6. User entities are responsible for ensuring that firewall and system logging are enabled and sufficient for their purposes.
7. User entities are responsible for ensuring that the impact of scheduled maintenance activities to their production processes and jobs is sufficiently mitigated.
8. User entities are responsible for notifying or denying requested infrastructure changes in a timely manner.
9. User entities are responsible for providing and maintaining the list of personnel authorized to submit information and/or requests to Flexential.
10. User entities are responsible for ensuring that only authorized individuals have knowledge of their designated authentication questions and answers.
11. User entities are responsible for creating and maintaining authentication questions and answers that are sufficiently complex and not easily compromised.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security, Availability, and Confidentiality Categories)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.