HOSTWAY®
THE TRUSTED CLOUD

HOSTWAY SERVICES, INC.

SOC 2 REPORT

FOR THE

CLOUD AND MANAGED HOSTING SERVICES

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

NOVEMBER 1, 2016, TO JULY 31, 2017

Attestation and Compliance Services

schellman
Quality, above all.

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

If 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.

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Hostway Services, Inc.:

Scope

We have examined the attached description of Hostway Services, Inc.'s ("Hostway" or the "service organization") Cloud and Managed Hosting Services system for the period November 1, 2016, to July 31, 2017, (the "description") based on the criteria set forth in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* ("description criteria") and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security and availability principles set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* ("applicable trust services criteria"), throughout the period November 1, 2016, to July 31, 2017.

In Section 5, Hostway has provided additional information that is not a part of Hostway's description. Information about Hostway's management's responses to exceptions noted has not been subjected to the procedures applied in the examination of the description and the suitability of the design and operating effectiveness of controls to meet the applicable trust services criteria.

Service organization's responsibilities

Hostway has provided the attached assertion, in Section 2, about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Hostway is responsible for preparing the description of the service organization's system and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description of the service organization's system; selecting the trust services principle(s) addressed by the engagement and stating the applicable trust services criteria and related controls in the description of the service organization's system; identifying the risks that would prevent the applicable trust services criteria from being met; identifying any applicable trust services criteria related to the principle(s) being reported on that have been omitted from the description and explaining the reason for the omission; and designing, implementing, and documenting controls to meet the applicable trust services criteria.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period November 1, 2016, to July 31, 2017.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and that the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period November 1, 2016, to July 31, 2017. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the

presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Explanatory Paragraph

The accompany description of Hostway's system states that a review of user access is performed on an annual basis. However, as noted in Section 4, (the "Testing Matrices"), a review of user access was not performed during the review period. As a result, the controls were not operating effectively to meet a portion of the criterion CC5.1, "Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability." during the period November 1, 2016, to July 31, 2017.

Opinion

In our opinion, except for the matter described in the preceding paragraph, based on the description criteria identified in Hostway's assertion and the applicable trust services criteria, in all material respects

a. the description fairly presents the system that was designed and implemented throughout the period November 1, 2016, to July 31, 2017;

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period November 1, 2016, to July 31, 2017; and

c. the controls that were tested, which were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period November 1, 2016, to July 31, 2017.

Description of test of controls

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

Restricted use

This report, including the description of tests of controls and results thereof in section 4 are intended solely for the information and use of Hostway; user entities of Hostway's Cloud and Managed Hosting Services system during some or all of the period November 1, 2016, to July 31, 2017; and prospective user entities, independent auditors and practitioners providing services to such user entities, 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, subservice organizations, or other parties;
- Internal control and its limitations;
- The nature of user entity controls responsibilities and their role in the user entities internal control as it relates to, and how they interact with, related controls at the service organization;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the applicable trust services criteria 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.

Schellman & Company, LLC

Tampa, Florida
October 17, 2017

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the attached description of Hostway's Cloud and Managed Hosting Services system for the period November 1, 2016, to July 31, 2017, (the "description") based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (the "description criteria"). The description is intended to provide users with information about the Cloud and Managed Hosting Services system, particularly system controls intended to meet the criteria for the security and availability principles set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* ("applicable trust services criteria"). We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the Cloud and Managed Hosting Services system throughout the period November 1, 2016, to July 31, 2017, based on the following description criteria:

   i. The description contains the following information:

      1.) The types of services provided;

      2.) The components of the system used to provide the services, which are the following:

         a.) *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks)

         b.) *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities)

         c.) *People*. The personnel involved in the governance, operation and use of a system (developers, operators, entity users, vendor personnel, and managers)

         d.) *Procedures.* The automated and manual procedures

         e.) *Data*. Transaction streams, files, databases, tables, and output used or processed by a system;

      3.) The boundaries or aspects of the system covered by the description;

      4.) For information provided to, or received from, subservice organizations and other parties

         a.) How such information is provided or received and the role of the subservice organizations and other parties

         b.) The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls;

      5.) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

         a.) Complementary user entity controls contemplated in the design of the service organization's system

         b.) When the inclusive method is used to present a subservice organization, controls at the subservice organization;

      6.) If the service organization presents the subservice organization using the carve-out method

         a.) The nature of the services provided by the subservice organization

         b.) Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria;

      7.) Any applicable trust services criteria that are not addressed by a control and the reasons; and

8.) In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs.

b. the controls stated in the description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. the controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

We state in our description that a review of user access is performed on an annual basis. However, a review of user access was not performed during the review period. As a result, the controls were not operating effectively to meet a portion of the criterion CC5.1, "Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability." during the review period November 1, 2016, to July 31, 2017.

Section 3

Description of the System

OVERVIEW OF OPERATIONS

Company Background

Hostway Services, Inc. (Hostway) is a cloud and managed hosting services provider with a direct presence in 13 countries, 14 worldwide operation centers and over 300 employees. Founded in 1998 and headquartered in Chicago, Illinois, Hostway provides managed and dedicated hosting, cloud hosting services, software as a service (SaaS) hosting, network services, web design, e-mail hosting, and domain name registration to over 1.4 million websites and 470,000 customers worldwide.

Hostway provides services to a broad range of customers, single application hosting, to large, complex and compliant online hosted computing configurations. It operates over 250,000 square feet of data centers.

Description of Services Provided

Hostway offers dedicated servers managed hosting services, cloud computing and storage, colocation to online technology companies, SaaS providers, major corporations, and other companies who outsource the hosting of computing and network operations.

Hostway's North American operations maintains data center operations in Austin, Texas; Tampa, Florida; Chicago, Illinois; and Vancouver, British Columbia. The data centers are designed and maintained to ensure high availability and uninterrupted service to customers. The data centers house dedicated servers and related equipment, which are purchased and owned by Hostway and which are made available to customers in exchange for monthly usage fees.

Hostway maintains a team of dedicated engineering, systems, and support personnel to help provide service and support to customers on a 24x7x365 basis. In addition, some facilities provide colocation facilities, in which customer computer and network equipment may be located either in shared or dedicated cabinets, or in assigned cage facilities.

System Boundaries

The scope of this examination includes the Cloud and Managed Hosting Services system performed at Hostway's North American data centers located in Austin, Texas (Waller and Trade Center data centers); Tampa, Florida (Madison and Franklin data centers); Chicago, Illinois; and Vancouver, British Columbia. Additionally, Hostway maintains an operations center in Sofia, Bulgaria, for monitoring and support of the six North American data center facilities. The data centers in Seoul, South Korea and Hanover, Germany, were not part of the scope of the report.

As outlined in the 2016 TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* a system is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) 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.

Infrastructure and Software

Dedicated Servers

When a new dedicated server is provisioned, an administrative (root access) account is created for the customer, including a username and password. This information is communicated to the customer via a welcome letter. Hostway does not retain a record of changes to the customer access credentials after the initial administrative

account creation. The operating system of each new server is configured during the build process to minimize the threat of unauthorized access consistent with the standard security settings.

Hostway provides management and support services to customers of its dedicated server products. Dedicated server support personnel may from time to time require logical access to customer servers in order to properly manage and support those servers, including hardware and software upgrades requested by the customer, remedial services, and custom programming or support services.

For Linux operating system servers, a secure socket shell (SSH) key system is used to control access to customer servers. The key server used to access customer servers is only accessible from inside the internal corporate network. When a new server is commissioned, SSH keys are installed on it allowing access to Hostway personnel. This access is not mandatory, and customers are entitled and empowered to remove the Hostway access to their servers. Hostway support personnel have permissions in the key system as required by their responsibilities. Access to the key system is logged and available to the administrator or SSH connections are logged by internal routers.

For Windows operating system servers, an SSH key system in conjunction with a password database file is used to control access to customer servers. Hostway support personnel have permissions in the key system and password database file as required by their responsibilities. Hostway support personnel have separate credentials for the key system and password database file. Access to the key system and database password file is logged and available to the administrator or SSH connections are logged by internal routers. Hostway may create an administrative account for use in supporting the customer and providing managed services. The access credentials to the administrative accounts are maintained in a secure system that limits access to those credentials to authorized personnel whose job responsibilities include supporting customer servers. For Windows based servers for which no central administrative account is available and on other servers for which the SSH keys have been removed by the customer, no central access is available to Hostway personnel. In this instance, the customer is requested to provide temporary access credentials either when support is requested, or proactively when Hostway personnel detect a problem with the customer's servers that requires intervention.

FlexCloud™ Servers

FlexCloud™ Servers (FlexCloud™) is one of Hostway's proprietary public and private cloud offerings running on a dynamically scalable virtualization platform. FlexCloud™ enables customers to have one or more virtual dedicated server instances running on physical host computers. Logical access to the physical host computers is controlled by a domain controller. Customers do not have logical access to the physical host computers.

FlexCloud™ may store images of the customer virtual machines (VMs) on a storage array network or other shared storage array. The images for multiple customers may be stored on the storage area network (SAN) or another array. Logical access to the SAN or shared array is only available within the internal data center network. Customers do not have logical access to the SAN or shared array.

A virtual server management console controls the operation of the VMs, the physical host computers, and the SAN or storage arrays. Logical access to the management tools is controlled by a domain controller and key server.

Network Devices

Hostway provides for a shared firewall service to restrict external (Internet) access to customer servers. Hostway manages the shared servers that provide the firewall service. Access to the settings for each customer is managed via an SSH key system in conjunction with a password database file. Hostway support personnel have permissions in the key system and password database file as required by their responsibilities. Hostway support personnel have separate credentials for the key system and password database file. Access to the key system and database password file is logged and available to the administrator or SSH connections are logged by internal routers. The default settings of the shared firewall are configured to conform to the standard Hostway template which is designed to minimize the threat of unauthorized access to the customers' environment.

An optional managed hardware firewall service is available which is dedicated to the customer's server equipment. The dedicated firewall supports additional control over how the customer's servers are accessed by the outside world and supports advanced features such as virtual private networks (VPNs) as required by the customer. As part of the on-boarding process, Hostway personnel consult with the customer to determine the

configuration and settings of the firewall. Hostway support personnel then install and configure the settings of the firewall to meet these requirements. Unless otherwise directed by the customer, the settings of the managed firewall are configured to conform to the standard Hostway template which is designed to minimize the threat of unauthorized access to the customers' servers. Managed firewall access credentials for each customer firewall are maintained by Hostway in a secure system that limits access to those credentials to Hostway personnel whose job responsibilities include managing the firewall settings. Changes to the firewall configuration may be requested by the customer and follow the standard change management process.

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

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
Corporate network domain	Network domain that is used to control access to internal systems, including customer management, material and equipment inventory, intranet, and electronic mail	Microsoft Windows operating system	Chicago data center facility
FlexCloud™ network domains	Network domains used to control internal user access to the FlexCloud™ customer environment	Microsoft Windows operating system	Chicago data center facility
Jump server	Used to control internal user access to the dedicated customer environment, including the SSH key system for Linux operating systems and the password database containing the passwords to customer support accounts on Windows operating system and network devices	Linux operating system	Chicago data center facility
Virtual server management console	Management console used administering FlexCloud™ virtual servers within the customer environment	Microsoft Windows operating system	Chicago data center facility

Additionally, multiple security and availability monitoring applications are utilized to monitor and protect the network and customer systems:

- ScienceLogic, Nagios, and System Center Operations Manager (SCOM) are utilized to monitor operational statistics of production servers and network devices for performance and availability
- OSSEC is utilized as a host based intrusion detection system (IDS) to analyze report on possible or actual network security breaches
- DOSMan monitoring application and Internet Relay Chat (IRC) traffic monitoring scripts are used to protect the network from traffic related attacks

People

The following personnel are responsible for providing services related to the Cloud and Managed Hosting Services system:

- Management personnel – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- Enterprise command center (ECC) and information technology (IT) operations personnel – responsible for managing, monitoring, and supporting internal Hostway and user entities' information and systems from unauthorized access and use while maintaining integrity and availability.

- Facilities personnel – responsible for maintaining physical assets related to the data center facilities.
- Customer support personnel – responsible for providing user entities with assistance during initial setup and continued support.

Procedures

Hostway has implemented policies and procedures to help guide internal personnel in the security and availability commitments and associated system requirements. These policies and procedures are developed, maintained, reviewed, and approved by the chief security officer (CSO). Changes to policies and procedures occur whenever significant changes to the system requirements or security and availability commitments. The policies are communicated to personnel via the company intranet.

Security and availability commitments, and associated system requirements are communicated to external users of the system via master services agreements and terms of service. These agreements are updated upon significant change to the system and included within an agreement addendum.

Security and availability commitments communicated to external users include, but are not limited to, the following:

- Detection, classification, and remediation of security events which are:
    - isolated within the client account;
    - associated with the client's virtual machines, operating systems, applications, client data and other content;
    - surfaced through vulnerability scanning tools; or
    - required for compliance or certification programs
- Use of industry standard measures to detect and prevent unauthorized third parties from accessing Hostway systems
- Update and repair Hostway systems to prevent downtime caused by outdated components or malfunction of systems
- Provide capacity management of the client's virtual machines, applications, code, client data and other content, and purchased resources
- Provide network availability to customers in accordance to defined service level agreements, including delivery of uninterrupted electrical power to system servers
- For customers subscribed to managed backup services:
    - configure backup settings with a set backup schedule and data retention period; and
    - perform backup restorations upon the client's request

<u>Access Authentication, Authorization, and Revocation</u>

Access to internal corporate systems is managed through a centralized lightweight directory access protocol (LDAP) database which is administered by the corporate IT systems group. Employees are granted access permissions as required by their job responsibilities. Network and operations personnel may also have access to internal systems that monitor and control network and customer equipment, physical access and security, and environmental systems. Access to these systems is controlled by the administrator of the specific system and permissions are granted to employees as required by their job responsibilities. Upon separation of an employee from the company, an employee termination checklist is completed and access to in-scope systems is disabled. Additionally, a user access review of access privileges to in-scope systems is performed on an annual basis to help ensure that access to data is limited to authorized personnel.

User account and minimum password requirements are established for the in-scope primary systems. Additionally, administrative access privileges to systems is controlled and limited to specific authorized management personnel.

Change Management

Dedicated Servers

The customer server build and firewall configuration processes are managed locally in each facility through a formal build and configuration process that ensures that each new system is constructed according to a consistent, well defined set of implementation steps. To ensure consistency and integrity of the initial installation of customer server builds, an automated install is used which burns a pre-configured image (Linux) or executes a script (Windows) of the operating system and commonly installed third party application software. Firewalls are configured by technicians who have demonstrated competency in their installation and maintenance. The images for customer server builds are pre-tested and approved by Hostway senior-level data center staff, enabling quick server builds and consistent results. New customer orders for customer server builds and firewalls are subjected to a quality assurance (QA) process to ensure that the equipment and software are working properly prior to releasing to the customer. The QA process requires that for customer server builds and firewall configurations the work be performed and/or reviewed by personnel who are qualified on that specific component.

FlexCloud™ Servers

There is an automated process that prepares the server using a pre-tested image. For the automated build process, internal software has been tested to ensure that servers prepared using the automated build will work properly when made available to the customer. Hostway maintains an intranet (internal web site) which includes a wiki and other repositories for hardware and software documentation.

One of the key security requirements for servers connected to the Internet is to keep the operating system software updated with the latest manufacturer's updates and security fixes. For versions of the operating systems offered with dedicated servers, the Hostway build team enables the auto update function of the operating system to enable downloading of updates and security fixes automatically when posted by the manufacturer. Customers may request changes to their server configurations, firewall settings, backup systems, or other system components controlled by Hostway. Requests can be made by trouble ticket through the web portal, by phone, or by e-mail. Customers are authenticated using the current confidential account information in the customer management system. Authorization for any reasonable request is assumed to be valid if submitted by anyone with proper authentication.

Physical Security

Physical access to data center facilities is tightly controlled to ensure the integrity of Hostway and customer data, equipment, and electronic transmissions. Access to Austin, Tampa, and Chicago data center facilities is controlled by an electronic badge system managed by Hostway. The badge access system for the Vancouver data center is owned and managed by the third party building manager. Multiple security checkpoints ensure that personnel and visitors are limited to secure areas for which they require access. These checkpoints are controlled by the electronic badge system, which controls access to specific areas based on responsibilities and authorization level of the badge holders. The badge system's administrative terminals are in secured areas with access limited to user accounts accessible by authorized personnel. The facilities offering colocation services for customers are segmented from the Hostway managed services main server rooms. Individual colocation space is secured by locked cabinet or cage, and colocation customers' access is restricted to the area in which their space is located.

Hostway maintains a physical security policy, and employees are required to be familiar with and adhere to the access policies. Among other items, the access policies define acceptable use of employee and visitor badges. Sharing of badges is prohibited per policy and failure to conform to the access policies is grounds for disciplinary action up to and including termination. Hostway employees, contractors and visitors are required to carry their badges when on the Hostway premises. Non-employee visitors are required to sign-in on a visitor's log and be escorted by an employee while within the data center floor. Only internal systems personnel, network administrators, and authorized contractors/vendors are allowed access to server and network equipment rooms. Any badges issued to non-employees that are unreturned are deactivated at the end of the term.

Data centers are monitored on a 24 hour per day basis by ECC and local operations personnel through closed circuit video surveillance cameras. Entries and exits are recorded by the video surveillance system and retained for a minimum of three months. The video recording equipment is in secured areas with access restricted to authorized personnel.

Environmental Security

Data center facilities are cooled by minimum N + 1 redundant air conditioning units, which are designed to ensure that equipment rooms are maintained at ambient temperatures suitable to commercial electronic computing and networking equipment. The air conditioning units are inspected quarterly in accordance with manufacturer's recommendations and air filters are replaced as required.

Environmental hazard detectors have been installed to respond to potentially dangerous conditions including excess temperatures, smoke, and floor water. Alarms for systems including air conditioning, fire, and generator / fuel, generate an audible alert, e-mail alert notifications to ECC personnel. Onsite operations personnel are trained to respond to alarms and to take actions based on the severity of the alarm. Fire detection and suppression systems are installed in office and equipment areas to mitigate the risk of damage from fires. Fire detection and suppression systems are inspected at least annually and repairs and recommended maintenance performed as required.

Commercial power to each data center facility is backed up by diesel generators capable of powering network and customer computing equipment, air conditioning systems, and security systems. Generators are inspected and tested on a quarterly basis by a commercial third party provider and serviced as required to ensure availability in the event of emergency. At the Trade Center and Franklin data centers only, connection facilities are available externally on the building for connection of portable generation equipment to augment or replace the permanent generators in the event of generator failure. On-site fuel reserves ensure a minimum of 48 hours of generator operation for each facility before refueling is required, except for Vancouver and Chicago facilities where the building management controls the on-site fuel reserves. Uninterruptable power supply (UPS) systems provide instantaneous failover to mitigate the impact of power fluctuations or failure. UPS systems are self-inspected monthly, vendor inspected quarterly, and serviced according to the manufacturers' recommended procedures.

Data Backup

Hostway provides multiple mechanisms to ensure that customer files and configuration data are backed up and protected, and readily available in the event of data loss whether from hardware or software failure, human error, or other unforeseen circumstances.

Hostway offers a managed backup service based on software which automates the process of archiving data from customers' servers. Each customer who subscribes to this service is provided with a quota, or limit on the amount of backup storage space available for his server or servers. Quotas are determined based on the level of service purchased by the customer. Backups are automatically performed on an incremental basis to create restore points based on the Hostway backup and retention policies in effect at the time. In the event of data loss, the customer can contact Hostway's technical support for assistance in recovering specific files or folders, or in restoring the entire server (bare metal restoration). An optional web interface is available to enable customers to perform their own restore operations.

For customers who require more control over their data, have large volumes to back up, or have specific requirements, Hostway offers a dedicated, self-managed option in which the backup software is deployed on one or more servers that are dedicated to that customer. In this case, the customer has administrative access and can set policies for backup frequency, retention, alerts, and other advanced functionality.

The shared backup systems are managed and maintained by the technical support team in each data center. Administrative access is limited to authorized support personnel. Dedicated server plans include a self-managed backup option. This consists of an assigned quota of file transfer protocol (FTP) space on a shared file system managed by Hostway. The FTP space for each customer is password protected. The FTP space is maintained on a redundant array of independent disks (RAID) protected disk array.

Hostway automatically backs up customer server images for FlexCloud™ Servers according to a standard frequency and maintains these backups according to a standard retention period. In addition to backup of customer data, Hostway backs up the configuration information for each customer server or network for the shared firewall or hardware firewall. This minimizes downtime and effort to restore in the event of a failure in a firewall system. Configuration of Hostway internal switches and routers, or their deployment infrastructure, are backed up following configuration changes to ensure service continuity.

Disaster Recovery

Hostway has developed a comprehensive IT disaster recovery plan that is derived from the results of the annual risk assessment performed to identify significant risks to the in-scope services during an unexpected service plan disruption or loss of power and the necessary requirements for an effective disaster recovery procedure. The disaster recovery plan is tested in a simulated environment at least annually to ensure that management and staff understand how to implement the plan in an emergency situation. Backup restorations are performed upon customer request and as a component of the annual disaster recovery testing. The disaster recovery and business continuity plan is reviewed by employees upon hire and during the annual security awareness training.

Incident Response

ECC personnel are staffed 24 hours per day to respond to customer issues and support incidents. Customer support requests are initiated via a web portal, telephone, or e-mail, and documented in a ticketing system. ECC personnel will also respond to alarms generated by internal network and customer server monitoring systems. The ECC is staffed with senior support technicians who have access to higher tier support and engineering personnel as well as third party vendor support. An escalation policy and procedures are in place to help ensure that customer issues are handled by personnel with the appropriate skill level and with management oversight. Tier II and III resources are available to assist customers in purging unauthorized access from applications or operating systems on customer servers.

Enterprise monitoring applications are utilized to monitor operational statistics of production servers and network devices for performance and availability on a real-time basis. Network monitoring software is configured to monitor the production network for suspicious traffic and alert ECC personnel in the event that predefined thresholds are exceeded. The system is integrated with core Hostway business systems to ensure synchronization of customer, service, and account data. A ticketing system is utilized to document, escalate, and track resolution of customer inquiries and technical issues. Tickets are prioritized in multiple queues by brand, customer type, and issue characteristics. Operations support personnel are trained to respond to and diagnose hardware and software faults and to take corrective action.

Equipment spares are kept onsite at the data center facilities to help ensure prompt repair or replacement of hardware failures. Trained staff is available to dispatch to replace or repair faulty hardware in any data center.

System Monitoring

Routers are configured for redundancy such that if one fails, network connectivity is still available to customers. ECC personnel are staffed 24 hours per day to monitor production systems and respond to incidents affecting the network or supporting systems. A ticketing system is utilized to document, escalate, and track resolution of incidents and network outages. An escalation policy and procedures are in place to help ensure that network incidents are handled by personnel with the appropriate skill level and with management oversight.

In order to protect customer communications, Hostway maintains an acceptable terms of use policy that is part of customer contracts for dedicated servers, managed services, and colocation. The terms of use help ensure that customers do not engage in practices that could jeopardize the availability or performance of the network for other customers. It prohibits spamming and other practices that are illegal or unacceptable to the norms of the Internet industry. Violation of the terms of use is grounds for termination of Hostway services. A network monitoring application is utilized to monitor and enforce the terms of use via network bandwidth and traffic reports, upstream carrier monitoring and feedback.

Denial of service or distributed denial of service (DDoS) attacks are a significant threat to Internet based businesses and can result in severe network degradation or complete outages. In a hosted environment, a DDoS attack on one web site in a multi-tenant data center can have severe repercussions for tenants in that data center, potentially usurping capacity on one or more external routes. A network monitoring application is utilized to provide protection from DDoS attacks against the production network.

Data

Hostway has documented data classification policies and procedures in place and define data within the following categories:

- Public – applies to information that is available to the general public and intended for distribution outside the organizations. This information may be freely disseminated without potential harm.
- Confidential – applies to information that is intended for use within the organization. Its unauthorized disclosure could adversely impact the organization, its employees and its business partners. Information that some people would consider private is included in this classification.
- Restricted Confidential – applies to the most sensitive medical and business information that is intended strictly for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization, its employees and its business partners
- For Internal Use Only – applies to any other information that does not clearly fit into the other classifications. The unauthorized disclosure, modification or destruction of this information is not expected to seriously or adversely impact the organization, its employees, or its business partners.

Data stored and maintained within the Cloud and Managed Hosting Services system includes customer profile and billing information, system configuration and audit logs. Data included within the scope of this examination is defined as confidential.

The enterprise monitoring and ticketing systems may contain data that relate to customer systems; however, customer data was not included in the scope of this examination as Hostway is not responsible for the creation or processing of data stored on customer systems.

Significant Changes During the Review Period

No relevant changes to the Cloud and Managed Hosting Services system occurred during the review period.

Subservice Organizations

No subservice organizations were included in the scope of this assessment. Therefore, the description does not address the criteria in Section 2, items (a)(i)(4), (a)(i)(5)(b) and (a)(i)(6).

CONTROL ENVIRONMENT

The control environment at Hostway 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 the board of directors and operations management.

Integrity and Ethical Values

Hostway has a formal code of conduct that dictates the ethical and responsible behavior of employees, and assists in defining a culture of professionalism and accountability. The Hostway corporate values include the following:

- Build trust and credibility
- Respect for the individual

- Culture of open and honest communication
- Set tone at the top
- Uphold the law
- Ethical, fair, and vigorous competition
- Respect and protect proprietary information
- No selective disclosure of material information
- Avoid conflicts of interest
- Set metrics and report results accurately
- Do the right thing

Executive Management and Board of Directors Oversight

The board of directors meets on a regular basis to review company operations and oversee the activities of the management team. Board members include select members of the management team and outside directors who proactively ensure appropriate corporate governance.

The management team is actively involved in aspects of the company operations, and ensures that corporate and business unit objectives guide activities for employees. Managers communicate regularly with supervisors and other employees, and review formal and ad hoc reports and information sources to validate the results of operations and ongoing activities. The management team is involved in corporate and business unit planning processes and participates in an incentive program that rewards both individual and company performance.

Organizational Structure and Assignment of Authority and Responsibility

Hostway operations are divided into three lines of business:

- Retail and small business
- Wholesale and private label
- Enterprise services

Each line of business overseen by functional corporate management, including sales, marketing, operations, and customer service. Supporting functions, including finance and administration, engineering, and accounting, are provided at the corporate level by personnel dedicated to these functions. The office facilities in Austin, Texas; Tampa, Florida; Chicago, Illinois; and Vancouver, British Columbia, include a local management structure as well as reporting relationships into one or more of the lines of business. Job responsibilities are aligned with corporate and business unit objectives and priorities. Local managers supervise and report on local operations, and results are rolled up to the corporate level.

Commitment to Competence

Hostway has formal hiring practices designed to ensure that new employees are qualified for their job responsibilities. Each new-position hiring must be jointly approved by the human resources (HR) department and the manager of the department requiring the employee. Offer letters are generated by the HR department. Hiring policies include requiring that prospective employees meet minimum education and experience requirements as appropriate for their position, that written references be submitted, and that employees execute confidentiality statements. The organization also performs background investigations and drug testing of prospective employees.

Accountability

Hostway believes that its employees are one of its most valuable assets, and formal practices are in place to ensure that employees are treated fairly and consistently. HR practices include a written employee handbook that is delivered to each new employee and maintained on a corporate intranet for reference at any time. An automated HR management information system maintains reporting relationships and assists in tracking performance reviews, time off schedules, employee benefits, and other important HR related information. The HR system includes a corporate intranet where key documents, notices, and other content are maintained. Employees receive a formal performance review at least annually and these reviews are maintained in the employee's personnel file. Supervisors and managers are responsible for ensuring that employees in their organization are competent and performing at the expected level.

RISK ASSESSMENT

Risk Identification

Hostway continually assesses risks associated with the operation of the network and data center infrastructure. This includes assessing physical, computing, and supporting systems to identify potential points of failure or degradation as follows:

- Network traffic levels and quality of service are constantly monitored
- Service level agreements are maintained for the benefit of customers
- System enhancements are initiated to reduce changes of failure
- Feedback from customers is reported to and reviewed by management

Hostway maintains in-house legal counsel on staff to review contracts, compliance, and other corporate matters. Contracts are submitted to legal review during negotiations and prior to execution.

Each year, Hostway undergoes a formal budget development, review, and approval process, involving key management from each of the business units, the finance and accounting departments, and other participants as required. The annual budget is an operating plan that incorporates explicit assumptions about the strategy of the business, major trends and new initiatives, and other pertinent information about how the business is to be run in the coming year. The budget is a financial roadmap that provides a consensus view of the key metric expectations and quantitative targets. The actual results of operations are reviewed against the budget on a monthly basis, enabling the identification of abnormalities, inaccurate assumptions, and emerging trends.

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

Risk Analysis

Hostway maintains formal policies and controls over key decisions and actions to ensure that such decisions and actions are consistent with corporate standards, including the following controls:

- Formal policies covering the signing of contracts, including officer approval and financial limits
- Hiring of employees and commitments to those employees are centralized in the HR department
- Major expenditures are approved by the chief executive officer (CEO) or his designee
- Employee expense reports are approved by the employee's supervisor and verified by the accounting department

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 and availability principles.

Selection and Development of Control Activities

The applicable trust 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 criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Hostway'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 and availability principles are applicable to the Cloud and Managed Hosting Services system. Therefore, the description does not address the (a)(i)(7) criteria in Section 2.

Information and Communication Systems

Relevant Information

Hostway maintains a broad array of information and communication systems to ensure that operations are managed efficiently and to provide key information and reports to employees and managers. The Hostway customer management system monitors the activities of customer service personnel, including extensive quantitative statistics on telephone support operations. Reports are available online and in real-time to ensure that customer contacts are handled promptly and that staff is assigned where required based on call volumes. Formal issue management and resolution systems are leveraged to record errors in internal software applications, issues with customer orders or services, and other critical background issues requiring follow-up. This system is accessed and updated by systems, software development, customer service, product management, and other stakeholders. Issues are prioritized and tracked to completion.

An HR system automates activities and provides reporting of hiring and terminations, vacation and paid time off, performance review dates, and key HR policies and information. Back office systems automate service orders, provisioning and de-provisioning of services, management of customer accounts, creation and tracking of trouble tickets, billing, and customer access to their accounts. Specialized tools and system assist in managing service inventories, building of customer servers, monitoring, tracking of events, web site statistics, and other functional activities. A centralized data warehouse consolidates information across Hostway and enables reporting and analysis of historical data. A business intelligence “dashboard” provides instant access to key business parameters and operating statistics to provide a summarized view of the sales and operations. A corporate inventory system manages and tracks purchases of equipment, software, and outside services and generates purchase orders and vendor advice.

Communication

Communications are a key component of running an effective organization. Hostway has extensive internal and external communications systems and processes designed to ensure that important information is communicated to required internal and external stakeholders. Hostway maintains a corporate e-mail system to enable communication amongst employees and between employees and outside parties. E-mail is augmented by a corporate-wide instant messaging facility that enables employees to communicate with one another immediately, streamlining communications and fostering real-time response and resolution. Additionally, internal web sites are used extensively on a departmental / functional level to communicate key information and processes. A variety of technologies are used for these intranets, including Wikis. An event tracking system (ETS) facilitates real-time notices of issues, including customer impacting events. Each ETS is updated as new information is available, enabling operations and customer service to react and provide updated status to customers.

Monitoring

Monitoring Activities

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

Additionally, extensive monitoring of real-time and historic statistics is performed using a broad array of automated systems including the following:

- ECC personnel monitor servers, network equipment, and environmental controls and alerts responsible parties when alarms are detected.
- Performance monitoring systems analyze the performance and availability of key applications.
- Phone and automatic call distribution system reports are generated to track performance of customer services departments.
- Customer servers are monitored to detect problems.
- Local data center systems analyze traffic patterns and load to detect anomalies.

Internal and External Auditing

Hostway supports many user entities in their efforts to meet the regulatory demands of their industry or governing agency. Hostway has assisted user entities by successfully meeting the requirements of many certifications and regulatory demands, including:

- Type 2 SOC 1 examination
- Type 2 SOC 2 examination
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)

Evaluating and Communicating Deficiencies

Deficiencies in an entity's internal control system surface from many sources, including the company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure that findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and make the decision for addressing deficiencies based on whether the incident was isolated or requires a change in the company's procedures or personnel.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the applicable trust services criteria. Therefore, the description does not address the (a)(i)(5)(a) criteria in Section 2.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Cloud and Managed Hosting Services system provided by Hostway. The scope of the testing was restricted to the Cloud and Managed Hosting Services system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period November 1, 2016, to July 31, 2017.

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 review 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.

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.

SECURITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.0: Common Criteria Related to Organization and Management			
CC1.1: The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability.			
CC1.1.1	Hostway utilizes an organization chart to track employee and supervisory relationships.	Inspect2ed the organization chart to determine that an organization chart was utilized to track employee and supervisory relationships.	No exceptions noted.
CC1.1.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for jobs.	Inspected the documented position descriptions for a sample of employees hired during the review period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employee sampled.	No exceptions noted.
CC1.2: Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.			
CC1.2.1	Hostway utilizes an organization chart to track employee and supervisory relationships.	Inspected the organization chart to determine that an organization chart was utilized to track employee and supervisory relationships.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for jobs.	Inspected the documented position descriptions for a sample of employees hired during the review period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employee sampled.	No exceptions noted.
CC1.2.3	The employee handbook is updated and communicated to employees via the human resources management system.	Inspected the employee handbook and human resources management system to determine that the employee handbook was updated and communicated to employees via the human resources management system.	No exceptions noted.
CC1.3: The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities.			
CC1.3.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for jobs.	Inspected the documented position descriptions for a sample of employees hired during the review period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for each employee sampled.	No exceptions noted.
CC1.3.2	Documented employee hiring policies and procedures are in place to guide personnel in activities related to the hiring process.	Inspected the onboarding policies and procedures to determine that documented employee hiring policies and procedures were in place to guide personnel in activities related to the hiring process.	No exceptions noted.
CC1.3.3	Pre-hire screening procedures are performed for employees as a component of the hiring process.	Inspected evidence of completed background checks and pre-hire screening for a sample of employees hired during the review period to determine that each employee sampled underwent pre-hire screening procedures as a component of the hiring process.	No exceptions noted.
CC1.3.4	Employees sign an acknowledgment form indicating that they have been given the employee handbook, containing the corporate policies and procedures and employee code of conduct, and understand their responsibility for adhering to the associated organization and security requirements.	Inspected the employee handbook to determine that the employee handbook contained the corporate policies and procedures and employee code of conduct.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the signed acknowledgment form for a sample of employees hired during review period to determine that each employee sampled signed an acknowledgment form indicating that they had been given the employee handbook, containing the corporate policies and procedures and employee code of conduct, and understood their responsibility for adhering to the associated organization and security requirements.	No exceptions noted.
CC1.3.5	Employees are required to complete security awareness training upon hire and on an annual basis to help ensure understanding of their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected evidence of completed security awareness training for a sample of employees hired during the review period and a sample of current employees to determine that security awareness training was completed upon hire for each new employee sampled and during the review period for each current employee sampled.	The test of the control activity disclosed that security awareness training was not completed during the review period for two of 40 current employees sampled.
CC1.4: The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and availability.			
CC1.4.1	Pre-hire screening procedures are performed for employees as a component of the hiring process.	Inspected evidence of completed background checks and pre-hire screening for a sample of employees hired during the review period to determine that each employee sampled underwent pre-hire screening procedures as a component of the hiring process.	No exceptions noted.
CC1.4.2	Employees sign an acknowledgment form indicating that they have been given the employee handbook, containing the corporate policies and procedures and employee code of conduct, and understand their responsibility for adhering to the associated organization and security requirements.	Inspected the employee handbook to determine that the employee handbook contained the corporate policies and procedures and employee code of conduct.	No exceptions noted.
		Inspected the signed acknowledgment form for a sample of employees hired during review period to determine that each employee sampled signed an acknowledgment form indicating that they had been given the employee handbook, containing the corporate policies and procedures and employee code of conduct, and understood their responsibility for adhering to the associated organization and security requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.3	Employees are required to complete security awareness training upon hire and on an annual basis to help ensure understanding of their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected evidence of completed security awareness training for a sample of employees hired during the review period and a sample of current employees to determine that security awareness training was completed upon hire for each new employee sampled and during the review period for each current employee sampled.	The test of the control activity disclosed that security awareness training was not completed during the review period for two of 40 current employees sampled.
CC1.4.4	Documented policies are in place to guide compliance personnel in applying sanctions to employees who fail to comply with security policies.	Inspected the acceptable use policies to determine that documented policies were in place to guide compliance personnel in applying sanctions to employees who failed to comply with security policies.	No exceptions noted.
CC2.0: Common Criteria Related to Communications			
CC2.1: Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.			
CC2.1.1	A system description is 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 internal and external users.	Inquired of the director of security and premier support services regarding the system description to determine that a system description was documented that included the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems; and that the system description was communicated to authorized internal and external users.	No exceptions noted.
		Inspected the Hostway system description to determine that a system description was documented that included the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems.	No exceptions noted.
CC2.2: The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.			
CC2.2.1	The entity’s security and availability commitments and the associated system requirements are documented in master service agreements.	Inspected the master service agreement and supplemental terms of service to determine that the entity’s security and availability commitments and the associated system requirements were documented in master service agreements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.2	Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements and that they were communicated to internal personnel via the company intranet.	No exceptions noted.
CC2.2.3	Employees sign an acknowledgment form indicating that they have been given the employee handbook, containing the corporate policies and procedures and employee code of conduct, and understand their responsibility for adhering to the associated organization and security requirements.	Inspected the employee handbook to determine that the employee handbook contained the corporate policies and procedures and employee code of conduct.	No exceptions noted.
		Inspected the signed acknowledgment form for a sample of employees hired during review period to determine that each employee sampled signed an acknowledgment form indicating that they had been given the employee handbook, containing the corporate policies and procedures and employee code of conduct, and understood their responsibility for adhering to the associated organization and security requirements.	No exceptions noted.
CC2.3: The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.			
CC2.3.1	The entity's security and availability commitments and the associated system requirements are documented in master service agreements.	Inspected the master service agreement and supplemental terms of service to determine that the entity's security and availability commitments and the associated system requirements were documented in master service agreements.	No exceptions noted.
CC2.3.2	Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements and that they were communicated to internal personnel via the company intranet.	No exceptions noted.
CC2.3.3	Employees sign an acknowledgment form indicating that they have been given the employee handbook, containing the corporate policies and procedures and employee code of	Inspected the employee handbook to determine that the employee handbook contained the corporate policies and procedures and employee code of conduct.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	conduct, and understand their responsibility for adhering to the associated organization and security requirements.	Inspected the signed acknowledgment form for a sample of employees hired during review period to determine that each employee sampled signed an acknowledgment form indicating that they had been given the employee handbook, containing the corporate policies and procedures and employee code of conduct, and understood their responsibility for adhering to the associated organization and security requirements.	No exceptions noted.
CC2.3.4	Employees are required to complete security awareness training upon hire and on an annual basis to help ensure understanding of their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected evidence of completed security awareness training for a sample of employees hired during the review period and a sample of current employees to determine that security awareness training was completed upon hire for each new employee sampled and during the review period for each current employee sampled.	The test of the control activity disclosed that security awareness training was not completed during the review period for two of 40 current employees sampled.
CC2.4: Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.			
CC2.4.1	The entity's security and availability commitments and the associated system requirements are documented in master service agreements.	Inspected the master service agreement and supplemental terms of service to determine that the entity's security and availability commitments and the associated system requirements were documented in master service agreements.	No exceptions noted.
CC2.4.2	Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements and that they were communicated to internal personnel via the company intranet.	No exceptions noted.
CC2.4.3	Employees sign an acknowledgment form indicating that they have been given the employee handbook, containing the corporate policies and procedures and employee code of	Inspected the employee handbook to determine that the employee handbook contained the corporate policies and procedures and employee code of conduct.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	conduct, and understand their responsibility for adhering to the associated organization and security requirements.	Inspected the signed acknowledgment form for a sample of employees hired during review period to determine that each employee sampled signed an acknowledgment form indicating that they had been given the employee handbook, containing the corporate policies and procedures and employee code of conduct, and understood their responsibility for adhering to the associated organization and security requirements.	No exceptions noted.
CC2.4.4	Employees are required to complete security awareness training upon hire and on an annual basis to help ensure understanding of their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected evidence of completed security awareness training for a sample of employees hired during the review period and a sample of current employees to determine that security awareness training was completed upon hire for each new employee sampled and during the review period for each current employee sampled.	The test of the control activity disclosed that security awareness training was not completed during the review period for two of 40 current employees sampled.
CC2.5: Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.			
CC2.5.1	An escalation policy and procedures are in place to help ensure that customer issues are handled by personnel with the appropriate skill level and with management oversight.	Inspected the escalation policy and recurring key performance indicator meeting invite to determine that an escalation policy and procedures were in place to help ensure that customer issues were handled by personnel with the appropriate skill level and with management oversight.	No exceptions noted.
CC2.5.2	Employees are required to complete security awareness training upon hire and on an annual basis to help ensure understanding of their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected evidence of completed security awareness training for a sample of employees hired during the review period and a sample of current employees to determine that security awareness training was completed upon hire for each new employee sampled and during the review period for each current employee sampled.	The test of the control activity disclosed that security awareness training was not completed during the review period for two of 40 current employees sampled.
CC2.5.3	Responsibilities for reporting suspected and actual security events related to information security and availability are communicated via master service agreements.	Inspected the master service agreement to determine that responsibilities for reporting suspected and actual security events related to information security and availability were communicated via master service agreements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.6: System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.			
CC2.6.1	Hostway utilizes an organization chart to track employee and supervisory relationships.	Inspected the organization chart to determine that an organization chart was utilized to track employee and supervisory relationships.	No exceptions noted.
CC2.6.2	Documented policies and procedures are in place to guide personnel in the entity's security and availability commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the company intranet.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place to guide personnel in the entity's security and availability commitments and the associated system requirements and that they were communicated to internal personnel via the company intranet.	No exceptions noted.
CC2.6.3	The CSO is designated to develop, maintain, review, and approve the security policies.	Inspected the information security policies and procedures to determine that the CSO was designated to develop, maintain, review, and approve the security policies.	No exceptions noted.
CC2.6.4	The entity's security and availability commitments and the associated system requirements are documented in master service agreements. The agreements are updated upon significant change to the commitments and system requirements.	Inquired of the director of security and premier support services regarding the master services agreements to determine that the agreements were updated upon significant change to the commitments and system requirements.	No exceptions noted.
		Inspected the master service agreement and supplemental terms of service to determine that the entity's security and availability commitments and the associated system requirements were documented in master service agreements.	No exceptions noted.
CC3.0: Common Criteria Related to Risk Management and Design and Implementation of Controls			
CC3.1: The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.			
CC3.1.1	An inventory listing of hardware and software included within the scope of services is maintained and reviewed by management as part of the annual risk assessment process.	Inspected the inventory listing to determine that a listing of hardware and software included within the scope of services is maintained and reviewed by management as part of the annual risk assessment process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.2	Documented policies and procedures are in place to guide personnel in performing the risk assessment process.	Inspected the risk assessment procedures to determine that documented policies and procedures were in place to guide personnel in performing the risk assessment process.	No exceptions noted.
CC3.1.3	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks were formally documented for management review.	No exceptions noted.
CC3.1.4	The entity's IT security group monitors the security impact of emerging technologies and the impact of applicable laws or regulations are considered by senior management.	Inspected security updates and notifications to determine that the entity's IT security group monitored the security impact of emerging technologies and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
CC3.2: The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.			
CC3.2.1	Documented policies and procedures are in place to guide personnel in performing the risk assessment process.	Inspected the risk assessment procedures to determine that documented policies and procedures were in place to guide personnel in performing the risk assessment process.	No exceptions noted.
CC3.2.2	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks were formally documented for management review.	No exceptions noted.
CC3.2.3	The entity's IT security group monitors the security impact of emerging technologies and the impact of applicable laws or regulations are considered by senior management.	Inspected security updates and notifications to determine that the entity's IT security group monitored the security impact of emerging technologies and the impact of applicable laws or regulations were considered by senior management.	No exceptions noted.
CC3.2.4	Penetration testing is performed by a third party specialist on an annual basis. Remediation plans are proposed and monitored through resolution.	Inquired of the director of security and premier support services regarding penetration testing to determine that penetration testing was performed by a third party specialist on an annual basis and that remediation plans were proposed and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the results of the most recently completed penetration test to determine that penetration testing was performed during the review period that remediation plans were proposed and monitored through resolution.	No exceptions noted.
CC4.0: Common Criteria Related to Monitoring Controls			
CC4.1: The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.			
CC4.1.1	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks were formally documented for management review.	No exceptions noted.
CC4.1.2	Penetration testing is performed by a third party specialist on an annual basis. Remediation plans are proposed and monitored through resolution.	Inquired of the director of security and premier support services regarding penetration testing to determine that penetration testing was performed by a third party specialist on an annual basis and that remediation plans were proposed and monitored through resolution.	No exceptions noted.
		Inspected the results of the most recently completed penetration test to determine that penetration testing was performed during the review period that remediation plans were proposed and monitored through resolution.	No exceptions noted.
CC4.1.3	An IDS is in place to analyze network device logs and report on possible or actual network security breaches.	Inspected the IDS configurations and an example IDS notification generated during the review period to determine that an IDS was in place to analyze network device logs and report on possible or actual network security breaches.	No exceptions noted.
CC4.1.4	Network monitoring software is configured to monitor the production network for suspicious traffic and alert ECC personnel in the event that predefined thresholds are exceeded.	Inspected the network monitoring software system configurations and example e-mail alert notifications generated during the review period to determine that monitoring software was configured to monitor the network for suspicious traffic and alert ECC personnel in the event that predefined thresholds were exceeded.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.5	Enterprise monitoring applications are utilized to monitor operational statistics of production servers and network devices for performance and availability on a real-time basis.	Inspected the enterprise monitoring applications' configurations to determine that enterprise monitoring applications were utilized to monitor operational statistics of production servers and network devices for performance and availability on a real-time basis.	No exceptions noted.
CC4.1.6	ECC personnel are staffed 24 hours per day to monitor production systems and respond to incidents affecting the network or supporting systems.	Inspected the data center staff shift schedules for a sample of months during the review period to determine that ECC personnel were staffed 24 hours per day to monitor production systems and respond to incidents affecting the network or supporting systems.	No exceptions noted.
CC4.1.7	An escalation policy and procedures are in place to help ensure that customer issues are handled by personnel with the appropriate skill level and with management oversight.	Inspected the escalation policy and recurring key performance indicator meeting invite to determine that an escalation policy and procedures were in place to help ensure that customer issues were handled by personnel with the appropriate skill level and with management oversight.	No exceptions noted.
CC4.1.8	A ticketing system is utilized to document, escalate, and track resolution of customer inquiries and technical issues.	Inspected the support tickets for a sample of customer support incidents resolved during the review period to determine that a ticketing system was utilized to document and track customer inquiries and technical issues.	No exceptions noted.
CC5.0: Common Criteria Related to Logical and Physical Access Controls			
CC5.1: Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.1.1	Documented standard build procedures are in place to guide personnel in the installation and maintenance of customer implementations.	Inspected the standard build procedures to determine that documented standard build procedures were in place to guide personnel in the installation and maintenance of customer implementations.	No exceptions noted.
CC5.1.2	Documented information security policies and procedures are in place to guide personnel in activities related to the authorization and provisioning of access commensurate with job responsibilities.	Inspected the information security policies and procedures to determine that information security policies and procedures were in place to guide personnel in activities related to the authorization and provisioning of access commensurate with job responsibilities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.3	User access requests are approved by management prior to being granted access to production systems.	Inspected evidence of management approval for a sample of employees hired during the review period to determine that user access requests were approved by management prior to being granted access to production systems.	No exceptions noted.
CC5.1.4	User access reviews are performed on an annual basis to help ensure that access to data is restricted to authorized personnel.	Inquired of the director of security and premier support services regarding user access reviews to determine that user access reviews were performed on an annual basis to help ensure that access to data is restricted to authorized personnel.	No exceptions noted.
		Inspected evidence of the most recently completed user access review and evidence of revocation to determine that user access reviews were performed during the review period.	The test of the control activity disclosed that a review of user access to the corporate and FlexCloud™ network domains was not performed during the review period.
CC5.1.5	The following in-scope systems are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements: • Corporate network domain • FlexCloud™ network domains • Jump server operating system • Virtual server management console	Inspected the authentication configurations for the in-scope systems to determine that the following in-scope systems were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements: • Corporate network domain • FlexCloud™ network domains • Jump server operating system • Virtual server management console	No exceptions noted.
CC5.1.6	Users are required to authenticate with a valid user account and password before being granted access to the customer FTP space.	Inspected the authentication configurations for the customer FTP space to determine that users were required to authenticate with a valid user account and password before being granted access to the customer FTP space.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.7	Administrative access privileges to the following in-scope systems are restricted to user accounts accessible by authorized personnel: • Corporate network domain • FlexCloud™ network domains • Jump server operating system • Virtual server management console	Inspected the administrative access privileges with the assistance of the senior director of network operations to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel: • Corporate network domain • FlexCloud™ network domains • Jump server operating system • Virtual server management console	No exceptions noted.
CC5.1.8	Administrative access privileges to the Linux operating system key system is restricted to user accounts accessible by authorized personnel.	Inspected the key system administrative access privileges with assistance of the network administrator to determine that administrative access privileges to the Linux operating system key system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC5.1.9	Administrative access privileges to the customer SAN is restricted to user accounts accessible by authorized personnel.	Inspected the customer SAN administrative access privileges with assistance of the senior director of network operations to determine that administrative access privileges to the customer SAN was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC5.1.10	The Linux operating system key system and Windows operating system password database are configured to log user account logon events.	Inspected the Linux operating system key system and Windows operating system password database audit logs generated during the review period to determine that the Linux operating system key system and Windows operating system password database were configured to log user account logon events.	No exceptions noted.
CC5.1.11	VPN encryption is enforced for remote access to production systems.	Inspected the VPN encryption configurations to determine that VPN encryption was enforced for remote access to production systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2: New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC5.2.1	User access requests are approved by management prior to being granted access to production systems.	Inspected evidence of management approval for a sample of employees hired during the review period to determine that user access requests were approved by management prior to being granted access to production systems.	No exceptions noted.
CC5.2.2	User access reviews are performed on an annual basis to help ensure that access to data is restricted to authorized personnel.	Inquired of the director of security and premier support services regarding user access reviews to determine that user access reviews were performed on an annual basis to help ensure that access to data is restricted to authorized personnel.	No exceptions noted.
		Inspected evidence of the most recently completed user access review and evidence of revocation to determine that user access reviews were performed during the review period.	The test of the control activity disclosed that a review of user access to the corporate and FlexCloud™ network domains was not performed during the review period.
CC5.2.3	The following in-scope systems are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements: • Corporate network domain • FlexCloud™ network domains • Jump server operating system • Virtual server management console	Inspected the authentication configurations for the in-scope systems to determine that the following in-scope systems were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements: • Corporate network domain • FlexCloud™ network domains • Jump server operating system • Virtual server management console	No exceptions noted.
CC5.2.4	Users are required to authenticate with a valid user account and password before being granted access to the customer FTP space.	Inspected the authentication configurations for the customer FTP space to determine that users were required to authenticate with a valid user account and password before being granted access to the customer FTP space.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.5	The Linux operating system key system and Windows operating system password database are configured to log user account logon events.	Inspected the Linux operating system key system and Windows operating system password database audit logs generated during the review period to determine that the Linux operating system key system and Windows operating system password database were configured to log user account logon events.	No exceptions noted.
CC5.2.6	IT personnel complete a termination checklist as part of the termination process.	Inspected the termination checklist for a sample of employees terminated during the review period to determine that IT personnel completed a termination checklist as part of the termination process for each employee sampled.	No exceptions noted.
CC5.2.7	IT personnel revoke production system access upon notification of employee termination from HR as part of the termination process.	Inspected the system user access privileges for a sample of employees terminated during the review period to determine that IT personnel revoked production system access upon notification of employee termination from HR as part of the termination process for each employee sampled.	The test of the control activity disclosed that IT personnel did not revoke production system access to the network domains for two of 36 terminated employees sampled.
CC5.3: Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.3.1	The following in-scope systems are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements: • Corporate network domain • FlexCloud™ network domains • Jump server operating system • Virtual server management console	Inspected the authentication configurations for the in-scope systems to determine that the following in-scope systems were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements: • Corporate network domain • FlexCloud™ network domains • Jump server operating system • Virtual server management console	No exceptions noted.
CC5.3.2	Users are required to authenticate with a valid user account and password before being granted access to the customer FTP space.	Inspected the authentication configurations for the customer FTP space to determine that users were required to authenticate with a valid user account and password before being granted access to the customer FTP space.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.3	Administrative access privileges to the following in-scope systems are restricted to user accounts accessible by authorized personnel: • Corporate network domain • FlexCloud™ network domains • Jump server operating system • Virtual server management console	Inspected the administrative access privileges with the assistance of the senior director of network operations to determine that administrative access privileges to the following in-scope systems were restricted to user accounts accessible by authorized personnel: • Corporate network domain • FlexCloud™ network domains • Jump server operating system • Virtual server management console	No exceptions noted.
CC5.3.4	Administrative access privileges to the Linux operating system key system is restricted to user accounts accessible by authorized personnel.	Inspected the key system administrative access privileges with assistance of the network administrator to determine that administrative access privileges to the Linux operating system key system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC5.3.5	Administrative access privileges to the customer SAN is restricted to user accounts accessible by authorized personnel.	Inspected the customer SAN administrative access privileges with assistance of the senior director of network operations to determine that administrative access privileges to the customer SAN was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC5.3.6	The Linux operating system key system and Windows operating system password database are configured to log user account logon events.	Inspected the Linux operating system key system and Windows operating system password database audit logs generated during the review period to determine that the Linux operating system key system and Windows operating system password database were configured to log user account logon events.	No exceptions noted.
CC5.4: Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.4.1	User access requests are approved by management prior to being granted access to production systems.	Inspected evidence of management approval for a sample of employees hired during the review period to determine that user access requests were approved by management prior to being granted access to production systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.4.2	User access reviews are performed on an annual basis to help ensure that access to data is restricted to authorized personnel.	Inquired of the director of security and premier support services regarding user access reviews to determine that user access reviews were performed on an annual basis to help ensure that access to data is restricted to authorized personnel.	No exceptions noted.
		Inspected evidence of the most recently completed user access review and evidence of revocation to determine that user access reviews were performed during the review period.	The test of the control activity disclosed that a review of user access to the corporate and FlexCloud™ network domains was not performed during the review period.
CC5.4.3	IT personnel revoke production system access upon notification of employee termination from HR as part of the termination process.	Inspected the system user access privileges for a sample of employees terminated during the review period to determine that IT personnel revoked production system access upon notification of employee termination from HR as part of the termination process for each employee sampled.	The test of the control activity disclosed that IT personnel did not revoke production system access to the network domains for two of 36 terminated employees sampled.
CC5.5: Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.5.1	A badge access system is utilized to control access to the data center facilities.	Observed the badge access system to the data center facilities to determine that a badge access system was utilized to control access to the data center facilities.	No exceptions noted.
		Inspected the badge access system user access privileges, access zone definitions and an example badge access system log generated during the review period to determine that a badge access system were utilized to control access to and within the data center facilities.	No exceptions noted.
CC5.5.2	Employees are assigned badge access privileges to physical security zones through the use of predefined access groups.	Inspected the badge access system access zone definitions to determine that employees were assigned badge access privileges to physical security zones through the use of predefined access groups.	No exceptions noted.
CC5.5.3	Administrative access privileges to the badge access system is restricted to user accounts accessible by authorized personnel.	Inspected the badge access system administrative access privileges with the assistance of the site operations manager to determine that administrative access privileges to the badge access system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.5.4	Individual colocation space is secured by locked cabinet or cage, and colocation customers' access is restricted to the area in which their space is located.	Inquired of the director of security and premier support services regarding colocation space to determined that individual colocation space was secured by locked cabinet or cage and colocation customers' access was restricted to the area in which their space was located.	No exceptions noted.
		Observed colocation space at the data center facilities to determine that individual colocation space was secured by locked cabinet or cage.	No exceptions noted.
CC5.5.5	Visitors are required to sign a visitor log prior to gaining access to the data center facilities.	Observed the data center visitor access procedures to determine that visitors were required to sign a visitor log prior to gaining access to the data center facilities.	No exceptions noted.
		Inspected the data center visitors log for a sample of months during the review period to determine that a visitor's log was utilized and included visitor signatures for each month sampled.	No exceptions noted.
CC5.6: Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.			
CC5.6.1	Firewall systems are in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall logs with the assistance of the director of security and premier support services to determine that a firewall system was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
CC5.6.2	Routers are configured for redundancy such that if one fails, network connectivity is still available to customers.	Inspected the data center network diagrams to determine that routers were configured for redundancy such that if one fails, network connectivity was still available to customers.	No exceptions noted.
CC5.6.3	A network monitoring application is utilized to monitor and enforce the terms of use via network bandwidth and traffic reports, upstream carrier monitoring and feedback.	Inspected the IRC traffic monitoring application configurations to determine that a network monitoring application was utilized to monitor and enforce the terms of use via network bandwidth and traffic reports, upstream carrier monitoring and feedback.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.6.4	An IDS is in place to analyze network device logs and report on possible or actual network security breaches.	Inspected the IDS configurations and an example IDS notification generated during the review period to determine that an IDS was in place to analyze network device logs and report on possible or actual network security breaches.	No exceptions noted.
CC5.6.5	Network monitoring software is configured to monitor the production network for suspicious traffic and alert ECC personnel in the event that predefined thresholds are exceeded.	Inspected the network monitoring software system configurations and example e-mail alert notifications generated during the review period to determine that monitoring software was configured to monitor the network for suspicious traffic and alert ECC personnel in the event that predefined thresholds were exceeded.	No exceptions noted.
CC5.7: The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.			
CC5.7.1	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 written supervisory procedures manual to determine that policies were in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	No exceptions noted.
CC5.7.2	The ability to access backup media is restricted to user accounts accessible by authorized personnel.	Inspected the backup media access privileges with assistance of the system administrator to determine that the ability to access backup media was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC5.7.3	VPN encryption is enforced for remote access to production systems.	Inspected the VPN encryption configurations to determine that VPN encryption was enforced for remote access to production systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.8: Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.8.1	Central antivirus software is configured on in-scope systems to protect registered production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions • Scan for updates to registered clients	Inspected the antivirus software configurations and listing of registered clients to determine that central antivirus software was configured on in-scope systems to protect registered production Windows servers and workstations with the following configurations: • Scan for updates to antivirus definitions • Scan for updates to registered clients	No exceptions noted.
CC6.0: Common Criteria Related to System Operations			
CC6.1: Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability.			
CC6.1.1	Network monitoring software is configured to monitor the production network for suspicious traffic and alert ECC personnel in the event that predefined thresholds are exceeded.	Inspected the network monitoring software system configurations and example e-mail alert notifications generated during the review period to determine that monitoring software was configured to monitor the network for suspicious traffic and alert ECC personnel in the event that predefined thresholds were exceeded.	No exceptions noted.
CC6.1.2	A network monitoring application is utilized to monitor and enforce the terms of use via network bandwidth and traffic reports, upstream carrier monitoring and feedback.	Inspected the IRC traffic monitoring application configurations to determine that a network monitoring application was utilized to monitor and enforce the terms of use via network bandwidth and traffic reports, upstream carrier monitoring and feedback.	No exceptions noted.
CC6.1.3	The Linux operating system key system and Windows operating system password database are configured to log user account logon events.	Inspected the Linux operating system key system and Windows operating system password database audit logs generated during the review period to determine that the Linux operating system key system and Windows operating system password database were configured to log user account logon events.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.4	The automated backup systems are configured to perform daily incremental backups of customer data and systems.	Inspected the automated backup systems' configurations and an example backup log generated during the review period to determine that the automated backup systems were configured to perform daily incremental backups of customer data and systems.	No exceptions noted.
CC6.1.5	Routers are configured for redundancy such that if one fails, network connectivity is still available to customers.	Inspected the data center network diagrams to determine that routers were configured for redundancy such that if one fails, network connectivity was still available to customers.	No exceptions noted.
CC6.1.6	Equipment spares are kept onsite at the data center facilities to help ensure prompt repair or replacement of hardware failures.	Observed the data center facilities to determine that equipment spares were kept onsite at the data center facilities to help ensure prompt repair or replacement of hardware failures.	No exceptions noted.
CC6.1.7	A ticketing system is utilized to document, escalate, and track resolution of incidents and network outages.	Inspected escalation procedures and the tickets for a sample of network incidents during the review period to determine that a ticketing system was utilized to document, escalate, and track resolution for each network incident sampled.	No exceptions noted.
CC6.1.8	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks were formally documented for management review.	No exceptions noted.
CC6.1.9	Penetration testing is performed by a third party specialist on an annual basis. Remediation plans are proposed and monitored through resolution.	Inquired of the director of security and premier support services regarding penetration testing to determine that penetration testing was performed by a third party specialist on an annual basis and that remediation plans were proposed and monitored through resolution.	No exceptions noted.
		Inspected the results of the most recently completed penetration test to determine that penetration testing was performed during the review period that remediation plans were proposed and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2: Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.			
CC6.2.1	An escalation policy and procedures are in place to help ensure that customer issues are handled by personnel with the appropriate skill level and with management oversight.	Inspected the escalation policy and recurring key performance indicator meeting invite to determine that an escalation policy and procedures were in place to help ensure that customer issues were handled by personnel with the appropriate skill level and with management oversight.	No exceptions noted.
CC6.2.2	Network monitoring software is configured to monitor the production network for suspicious traffic and alert ECC personnel in the event that predefined thresholds are exceeded.	Inspected the network monitoring software system configurations and example e-mail alert notifications generated during the review period to determine that monitoring software was configured to monitor the network for suspicious traffic and alert ECC personnel in the event that predefined thresholds were exceeded.	No exceptions noted.
CC6.2.3	Enterprise monitoring applications are utilized to monitor operational statistics of production servers and network devices for performance and availability on a real-time basis.	Inspected the enterprise monitoring applications' configurations to determine that enterprise monitoring applications were utilized to monitor operational statistics of production servers and network devices for performance and availability on a real-time basis.	No exceptions noted.
CC6.2.4	Customer support requests are initiated via a web portal, telephone, or e-mail, and documented in a ticketing system.	Inspected the web portal and support tickets a sample of customer support incidents resolved during the review period to determine that each customer support incident sampled was initiated via a web portal, telephone, or e-mail, and documented in a ticketing system.	No exceptions noted.
CC6.2.5	ECC personnel are staffed 24 hours per day to monitor production systems and respond to incidents affecting the network or supporting systems.	Inspected the data center staff shift schedules for a sample of months during the review period to determine that ECC personnel were staffed 24 hours per day to monitor production systems and respond to incidents affecting the network or supporting systems.	No exceptions noted.
CC6.2.6	A ticketing system is utilized to document, escalate, and track resolution of incidents and network outages.	Inspected escalation procedures and the tickets for a sample of network incidents during the review period to determine that a ticketing system was utilized to document, escalate, and track resolution for each network incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.7	Employees sign an acknowledgment form indicating that they have been given the employee handbook, containing the corporate policies and procedures and employee code of conduct, and understand their responsibility for adhering to the associated organization and security requirements.	Inspected the employee handbook to determine that the employee handbook contained the corporate policies and procedures and employee code of conduct.	No exceptions noted.
		Inspected the signed acknowledgment form for a sample of employees hired during review period to determine that each employee sampled signed an acknowledgment form indicating that they had been given the employee handbook, containing the corporate policies and procedures and employee code of conduct, and understood their responsibility for adhering to the associated organization and security requirements.	No exceptions noted.
CC7.0: Common Criteria Related to Change Management			
CC7.1: The entity's commitments and system requirements, as they relate to security and availability, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.			
CC7.1.1	Documented change management procedures are in place to guide personnel in activities related to the change management process.	Inspected the change management policies and procedures to determine that documented change management procedures were in place to guide personnel in activities related to the change management process.	No exceptions noted.
CC7.1.2	A change management ticketing system is utilized to document and track system change requests, testing, and approvals.	Inspected the change tickets for a sample of customer dedicated server and firewall builds implemented during the review period to determine that a change management ticketing system was utilized to document and track system change requests, testing, and approvals for each change sampled.	No exceptions noted.
CC7.1.3	The image for customer dedicated server and FlexCloud™ builds are pre-tested and approved by management personnel.	Inquired of the site operations manager regarding imaging to determine that the image for customer dedicated server and FlexCloud™ builds were pre-tested and approved by management personnel.	No exceptions noted.
		Inspected the customer dedicated server and FlexCloud™ build process to determine that a pre-tested and approved image was utilized for customer server and FlexCloud™ builds.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2: Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability.			
CC7.2.1	A formal risk assessment is performed on an annual basis. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks were formally documented for management review.	No exceptions noted.
CC7.2.2	ECC personnel are staffed 24 hours per day to monitor production systems and respond to incidents affecting the network or supporting systems.	Inspected the data center staff shift schedules for a sample of months during the review period to determine that ECC personnel were staffed 24 hours per day to monitor production systems and respond to incidents affecting the network or supporting systems.	No exceptions noted.
CC7.2.3	The employee handbook is updated and communicated to employees via the human resources management system.	Inspected the employee handbook and human resources management system to determine that the employee handbook was updated and communicated to employees via the human resources management system.	No exceptions noted.
CC7.2.4	The CSO is designated to develop, maintain, review, and approve the security policies.	Inspected the information security policies and procedures to determine that the CSO was designated to develop, maintain, review, and approve the security policies.	No exceptions noted.
CC7.2.5	The entity's security and availability commitments and the associated system requirements are documented in master service agreements. The agreements are updated upon significant change to the commitments and system requirements.	Inquired of the director of security and premier support services regarding the master services agreements to determine that the agreements were updated upon significant change to the commitments and system requirements.	No exceptions noted.
		Inspected the master service agreement and supplemental terms of service to determine that the entity's security and availability commitments and the associated system requirements were documented in master service agreements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3: Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.			
CC7.3.1	An escalation policy and procedures are in place to help ensure that customer issues are handled by personnel with the appropriate skill level and with management oversight.	Inspected the escalation policy and recurring key performance indicator meeting invite to determine that an escalation policy and procedures were in place to help ensure that customer issues were handled by personnel with the appropriate skill level and with management oversight.	No exceptions noted.
CC7.3.2	A change management ticketing system is utilized to document and track system change requests, testing, and approvals.	Inspected the change tickets for a sample of customer dedicated server and firewall builds implemented during the review period to determine that a change management ticketing system was utilized to document and track system change requests, testing, and approvals for each change sampled.	No exceptions noted.
CC7.3.3	Customer support requests are initiated via a web portal, telephone, or e-mail, and documented in a ticketing system.	Inspected the web portal and support tickets a sample of customer support incidents resolved during the review period to determine that each customer support incident sampled was initiated via a web portal, telephone, or e-mail, and documented in a ticketing system.	No exceptions noted.
CC7.3.4	A ticketing system is utilized to document, escalate, and track resolution of customer inquiries and technical issues.	Inspected the support tickets for a sample of customer support incidents resolved during the review period to determine that a ticketing system was utilized to document and track customer inquiries and technical issues.	No exceptions noted.
CC7.3.5	A ticketing system is utilized to document, escalate, and track resolution of incidents and network outages.	Inspected escalation procedures and the tickets for a sample of network incidents during the review period to determine that a ticketing system was utilized to document, escalate, and track resolution for each network incident sampled.	No exceptions noted.
CC7.4: Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.			
CC7.4.1	Documented change management procedures are in place to guide personnel in activities related to the change management process.	Inspected the change management policies and procedures to determine that documented change management procedures were in place to guide personnel in activities related to the change management process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.2	Documented standard build procedures are in place to guide personnel in the installation and maintenance of customer implementations.	Inspected the standard build procedures to determine that documented standard build procedures were in place to guide personnel in the installation and maintenance of customer implementations.	No exceptions noted.
CC7.4.3	A change management ticketing system is utilized to document and track system change requests, testing, and approvals.	Inspected the change tickets for a sample of customer dedicated server and firewall builds implemented during the review period to determine that a change management ticketing system was utilized to document and track system change requests, testing, and approvals for each change sampled.	No exceptions noted.
CC7.4.4	The image for customer dedicated server and FlexCloud™ builds are pre-tested and approved by management personnel.	Inquired of the site operations manager regarding imaging to determine that the image for customer dedicated server and FlexCloud™ builds were pre-tested and approved by management personnel.	No exceptions noted.
		Inspected the customer dedicated server and FlexCloud™ build process to determine that a pre-tested and approved image was utilized for customer server and FlexCloud™ builds.	No exceptions noted.
CC7.4.5	An automated backup system is utilized to perform backups prior to configuration changes to infrastructure.	Inspected the automated backup system configurations to determine that an automated backup system was configured to perform backups prior to configuration changes to infrastructure.	No exceptions noted.
CC7.4.6	The ability to implement system changes is restricted to user account accessible by authorized personnel.	Inspected the jump server operating system administrative access privileges to determine that the ability to implement system changes was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

[Intentionally Blank]

AVAILABILITY PRINCIPLE AND CRITERIA TABLE

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1: Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.			
A1.1.1	Enterprise monitoring applications are utilized to monitor operational statistics of production servers and network devices for performance and availability on a real-time basis.	Inspected the enterprise monitoring applications' configurations to determine that enterprise monitoring applications were utilized to monitor operational statistics of production servers and network devices for performance and availability on a real-time basis.	No exceptions noted.
A1.1.2	A network monitoring application is utilized to monitor and enforce the terms of use via network bandwidth and traffic reports, upstream carrier monitoring and feedback.	Inspected the IRC traffic monitoring application configurations to determine that a network monitoring application was utilized to monitor and enforce the terms of use via network bandwidth and traffic reports, upstream carrier monitoring and feedback.	No exceptions noted.
A1.1.3	ECC personnel are staffed 24 hours per day to monitor production systems and respond to incidents affecting the network or supporting systems.	Inspected the data center staff shift schedules for a sample of months during the review period to determine that ECC personnel were staffed 24 hours per day to monitor production systems and respond to incidents affecting the network or supporting systems.	No exceptions noted.
A1.1.4	A ticketing system is utilized to document, escalate, and track resolution of incidents and network outages.	Inspected escalation procedures and the tickets for a sample of network incidents during the review period to determine that a ticketing system was utilized to document, escalate, and track resolution for each network incident sampled.	No exceptions noted.
A1.2: Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.			
A1.2.1	Documented data backup policies and procedures are in place to guide personnel in activities related to backup scheduling and data recovery.	Inspected policies and procedures to determine that documented data backup policies and procedures were in place to guide personnel in activities related to backup scheduling and data recovery.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.2	The automated backup systems are configured to perform daily incremental backups of customer data and systems.	Inspected the automated backup systems' configurations and an example backup log generated during the review period to determine that the automated backup systems were configured to perform daily incremental backups of customer data and systems.	No exceptions noted.
A1.2.3	ECC personnel monitor the status of backup jobs on a daily basis.	Inquired of the systems administrator regarding monitoring of backup jobs to determine that ECC personnel monitored the status of backup jobs on a daily basis.	No exceptions noted.
		Inspected an example audit log to determine that ECC personnel monitored the status of backup jobs.	No exceptions noted.
A1.2.4	Routers are configured for redundancy such that if one fails, network connectivity is still available to customers.	Inspected the data center network diagrams to determine that routers were configured for redundancy such that if one fails, network connectivity was still available to customers.	No exceptions noted.
A1.2.5	Equipment spares are kept onsite at the data center facilities to help ensure prompt repair or replacement of hardware failures.	Observed the data center facilities to determine that equipment spares were kept onsite at the data center facilities to help ensure prompt repair or replacement of hardware failures.	No exceptions noted.
A1.2.6	The data center facilities are protected by fire detection and suppression controls that include the following: • Audible and visual fire alarms • Fire and smoke detectors • Dry pipe fire sprinkler system • Hand-held fire extinguishers	Observed the fire detection and suppression equipment within the data center facilities to determine that the data center facilities were protected by fire detection and suppression controls that included the following: • Audible and visual fire alarms • Fire and smoke detectors • Dry pipe fire sprinkler system • Hand-held fire extinguishers	No exceptions noted.
A1.2.7	An environmental monitoring application is utilized to monitor the environmental conditions within the data center facilities that include, but are not limited to, the following: • Temperature • Humidity • Leak detection	Inspected the environmental monitoring application configurations to determine that an environmental monitoring application was in place to monitor the environmental conditions within the data center facilities that included the following: • Temperature • Humidity • Leak detection	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.8	The environmental monitoring application is configured to send e-mail alert notifications to facilities personnel when predefined thresholds are exceeded on monitored systems.	Inspected the environmental monitoring application alert configurations and an example e-mail alert notification generated during the review period to determine that the environmental monitoring application was configured to send e-mail alert notifications to facilities personnel when predefined thresholds were exceeded on monitored systems.	No exceptions noted.
A1.2.9	Air conditioning units are in place to control air temperature and air quality within the data center facilities.	Observed the air conditioning units within the data center facilities to determine that air conditioning units were in place.	No exceptions noted.
A1.2.10	Equipment within the data center facilities is connected to multiple UPS systems to provide temporary electricity in the event of a power outage and to mitigate the risk of power surges impacting infrastructure within the data centers.	Inquired of the facilities manager regarding UPS equipment to determine that equipment within the data center facilities was connected to multiple UPS systems to provide temporary electricity in the event of a power outage and to mitigate the risk of power surges impacting infrastructure within the data centers.	No exceptions noted.
		Observed the UPS systems within the data center facilities to determine that UPS systems were in place.	No exceptions noted.
A1.2.11	The data center facilities are equipped with multiple generators to provide electricity to the data centers in the event of a power outage.	Observed the generators supporting the data center facilities to determine that the data center facilities were equipped with multiple generators.	No exceptions noted.
A1.2.12	Management obtains inspection reports as evidence that maintenance inspections are performed on the fire suppression system and hand-held fire extinguishers on an annual basis.	Inspected the most recent fire system inspection report and fire extinguisher inspection tags for example hand-held fire extinguishers to determine that management obtained inspection reports evidencing that a maintenance inspection was performed on the fire suppression system and hand-held fire extinguishers during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.13	Management obtains inspection reports as evidence that maintenance is periodically performed on the following equipment: • Air conditioning units • UPS systems • Generators	Inspected the results of the inspection reports obtained for a sample of quarters to determine that management obtained quarterly inspection reports as evidence that maintenance was performed on the following equipment for each quarter sampled: • Air conditioning units • UPS systems • Generators	No exceptions noted.
A1.2.14	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the disaster recovery policies and procedures to determine that disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by unexpected events.	No exceptions noted.
A1.3: Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.			
A1.3.1	Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the disaster recovery policies and procedures to determine that disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by unexpected events.	No exceptions noted.
A1.3.2	Disaster recovery plans are tested on an annual basis and results are reviewed by management.	Inspected the most recently completed disaster recovery test results to determine that disaster recovery plans were tested on an annual basis and the results were reviewed by management.	No exceptions noted.
A1.3.3	Backup restoration procedures are tested at least annually as a component of annual disaster recovery plan testing.	Inspected the results of the most recently completed backup restoration to determine that backup restoration procedures were tested at least annually as a component of annual disaster recovery plan testing.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY MANAGEMENT

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS AND QUALIFICATION

Security Principle

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3: The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities. CC1.4: The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and availability. CC2.3: The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties. CC2.4: Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities. CC2.5: Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.			
CC1.3.5 CC1.4.3 CC2.3.4 CC2.4.4 CC2.5.2	Employees are required to complete security awareness training upon hire and on an annual basis to help ensure understanding of their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected evidence of completed security awareness training for a sample of employees hired during the review period and a sample of current employees to determine that security awareness training was completed upon hire for each new employee sampled and during the review period for each current employee sampled.	The test of the control activity disclosed that security awareness training was not completed during the review period for two of 40 current employees sampled.
Management's Response:	The two employees noted above did not complete the training by the deadline, but did complete it subsequently. All employees have completed security training as of August 2nd, 2017. Hostway has modified its process so that evidence of completion of security awareness training by all employees must be provided to the Corporate Security team within 30 days of hire and within 30 days of annual retraining		

[Intentionally Blank]

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1: Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability. CC5.2: New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. CC5.4: Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.1.4 CC5.2.2 CC5.4.2	User access reviews are performed on an annual basis to help ensure that access to data is restricted to authorized personnel.	Inspected evidence of the most recently completed user access review and evidence of revocation to determine that user access reviews were performed during the review period.	The test of the control activity disclosed that a review of user access to the corporate and FlexCloud™ network domains was not performed during the review period.
Management's Response:	Hostway performs periodic reviews of access to the corporate and FlexCloud™ network domains, but those reviews were not properly documented during the audit period. Hostway has updated its procedure to properly document the access review procedure on at least a quarterly basis.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2: New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. CC5.4: Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.			
CC5.2.7 CC5.4.3	IT personnel revoke production system access upon notification of employee termination from HR as part of the termination process.	Inspected the system user access privileges for a sample of employees terminated during the review period to determine that IT personnel revoked production system access upon notification of employee termination from HR as part of the termination process for each employee sampled.	The test of the control activity disclosed that IT personnel did not revoke production system access to the network domains for two of 36 terminated employees sampled.
Management's Response:	Access to the FlexCloud™ domain is only possible via physical network access or through VPN. VPN access is controlled by a separate network domain in which both noted employee's accounts were disabled immediately at the time of separation, thus contemporaneously removing their ability to access the FlexCloud™ network domain. However, even though none of the employees could possibly access the FlexCloud™ infrastructure, Hostway has modified its employee separation process to further verify that terminated users are disabled or removed from the FlexCloud™ network domain, and other similar domains		