green cloud
TECHNOLOGIES
CUSTOM SOLUTIONS. CHANNEL ONLY.

Green Cloud Technologies

SOC 3 Report on Green Cloud Technologies' Secure Cloud Platform Relevant to Security and Availability

For the period January 1, 2018 to March 31, 2019

Table of Contents

Section One
Independent Service Auditor’s Report

DHG
DIXON HUGHES GOODMAN LLP

4350 Congress Street
Suite 900
Charlotte, NC 28209
P 704.367.7020
F 704.367.7760
dhg.com

Independent Service Auditor’s Report

Green Cloud Technologies
Greenville, South Carolina

Scope

We have examined Green Cloud Technologies’ (Green Cloud) accompanying assertion titled "Management’s Assertion" (assertion) that the controls within Green Cloud’s Secure Cloud Platform (system) were effective throughout the period January 1, 2018 to March 31, 2019, to provide reasonable assurance that Green Cloud’s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP 100*, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Criteria).*

Service Organization's Responsibilities

Green Cloud is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Green Cloud’s service commitments and system requirements were achieved. Green Cloud has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Green Cloud is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Green Cloud’s service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Green Cloud’s service commitments and system requirements based the applicable trust services criteria

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Green Cloud’s Secure Cloud Platform (system) were effective throughout the period January 1, 2018, to March 31, 2019, to provide reasonable assurance that Green Cloud's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Dixon Hughes Goodman LLP

Charlotte, North Carolina
May 30, 2019

Section Two
Management's Assertion

Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Green Cloud Technologies' (Green Cloud) Secure Cloud Platform (system) throughout the period January 1, 2018, to March 31, 2019, to provide reasonable assurance that Green Cloud's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in Section Three and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2018, to March 31, 2019, to provide reasonable assurance that Green Cloud's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100*, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (*AICPA*, Trust Services Criteria)*. Green Cloud's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section Three.

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

We assert that the controls within the system were effective throughout the period January 1, 2018, to March 31, 2019, to provide reasonable assurance that Green Cloud's service commitments and system requirements were achieved based on the applicable trust services criteria.

Green Cloud Technologies

Section Three
Description of Green Cloud Technologies Secure Cloud Platform

Overview of Operations

GCT Operating Company, dba Green Cloud Technologies, LLC ("Green Cloud", "the Company") is a technology services company that delivers managed Infrastructure as a Service (IaaS), Disaster Recovery as a Service (DRaaS), Backup as a Service (BaaS), and Desktop as a Service (DaaS) solutions. Green Cloud works exclusively with channel partners and value-added resellers ("Partners") to provide those businesses and their end-customers with turnkey cloud solutions including multi-tenant and private virtual server environments, off-premise business continuity solutions, comprehensive networking and security products, and complementary professional services for installation and migration.

Green Cloud Service Catalog

Infrastructure as a Service (IaaS)
Powered by VMware, IaaS provides Green Cloud Partners with a public or private multi-tenant architecture leveraging dedicated or shared storage, compute, and memory resources. Complementary networking and security features provide a powerful blend of dependability, scalability, and ease-of-use in a VMware-based computing environment. The environment is ideal for deploying classic and cloud-based applications without requiring a significant investment in a private data center.

Disaster Recovery as a Service (DRaaS)
DRaaS with Zerto
Powered by Zerto Virtual replication, this disaster recovery service is real-time replication that protects virtual servers by replicating virtual machine data to a secondary data center. DRaaS with Zerto combines replication with block-level, application-consistent data protection across both hosts and storage.

DRaaS with StorageCraft
Powered by StorageCraft, this disaster recovery service provides local and off-site server backup with recovery to Green Cloud's IaaS environment. The service is managed remotely by Green Cloud and leverages the use of an on premise network attached storage device (NAS) and locally installed management software.

Desktop as a Service (DaaS)
Powered by Horizon DaaS from VMware, Green Cloud DaaS provides a complete virtual workspace from the cloud, delivering Windows desktops and applications as an easily managed, unified cloud service. Partners have with the ability to manage and administrate multiple desktop configurations from a centralized point, allowing for simpler software, configuration, and compliance management for many end-users.

Backup as a Service (Baas)
Powered by Veeam Cloud Connect, BaaS provides an offsite backup repository for partners to manage offsite data backups from the end-users' local server environment. The backup repositories are completely isolated from one another, and backups can be encrypted at the source - before data leaves the customer premise to ensure confidentiality of the data.

The Components of the System Used to Provide the Services

Infrastructure

Green Cloud outsources data center facility management and physical facility security from various professional data center operating companies. Green Cloud ensures that all subservice organizations have sufficient availability and security controls in place and monitors adherence to those processes and procedures.

Data Center Locations Covered by this Report:

Location	Third Party Data Center Provider
Atlanta, Georgia	QTS
Nashville, Tennessee	Flexential (Formerly Peak 10)
Greenville, South Carolina	Immedion
Houston, Texas	CyrusOne
Phoenix, Arizona	Iron Mountain (Formerly IO)
Dallas, Texas	QTS
Minneapolis, Minnesota	n/a (Green Cloud owned)

Underlying infrastructure includes:

- Facilities (HVAC, power, cages, cabinets)
- Switches, routers, firewalls
- Storage Arrays and Storage servers
- Unified Computing System servers
- Hypervisor systems
- Network Management System

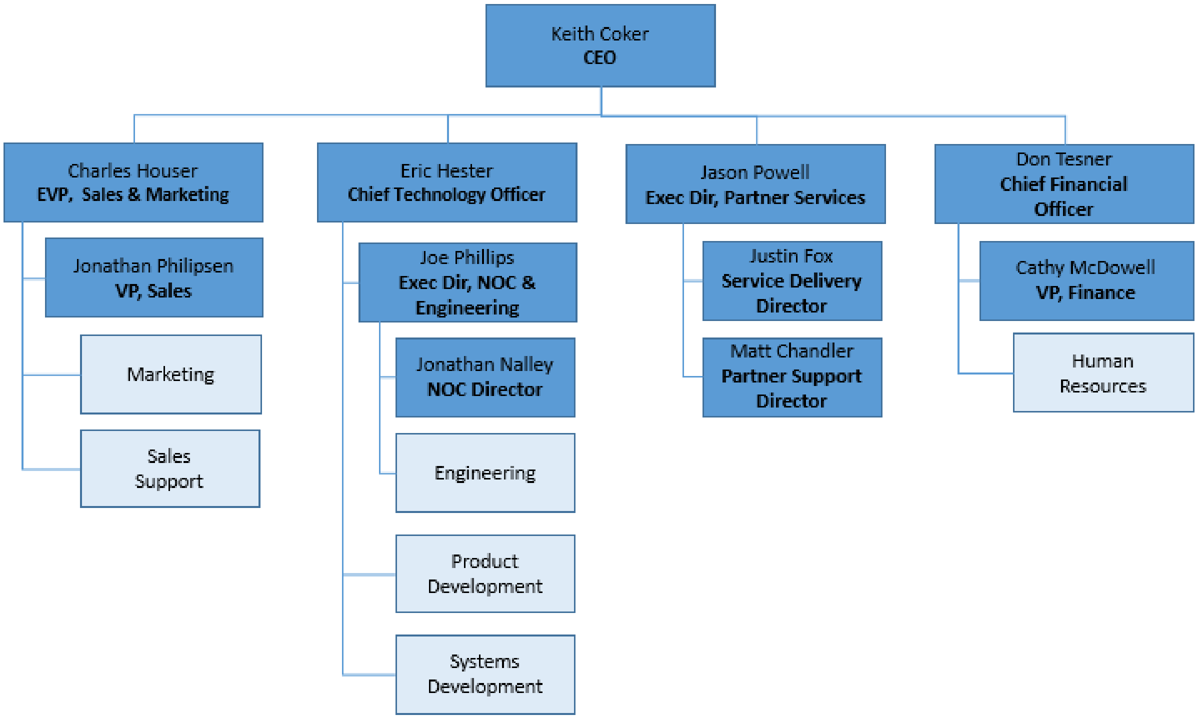
Green Cloud works exclusively with well-established Managed Services Providers (MSPs) and Value-Added Resellers (VARs) to sell its products and services. The MSPs and VARs (Partners) provide sales services and end-user support, and Green Cloud supports the Partner with marketing materials, sales support, and partner technical support.

Software

Green Cloud's vCloud IaaS offering leverages the VMware ESXi Hypervisor platform in conjunction with VMware vCloud Director. VMware ESXi provides the underlying abstraction of hardware used to deliver virtual data center instances to customers, and vCloud Director provides an interface for partners to manage their virtual environment. This includes the ability to provision and decommission servers and network edges, as well as provide direct console access for operating system configuration and management. The vCloud Director portal manages the virtual firewall configuration used to segment and protect customer virtual machines from other internal resources as well as the public Internet.

People

Organizational Structure



Keith Coker is co-founder and CEO of Green Cloud Technologies. Keith leverages over 15 years of experience in leadership positions, including Chief Technology Officer at two telecommunications organizations where he managed $275 million of network infrastructure deployment, capital expenditures, and operating expenses.

Eric Hester is co-founder and Chief Technology Officer. Eric has over 20 years of experience in the technology field and prior to co-founding Green Cloud, Hester also served as Technical Director at Sonus Networks, where he designed and implemented some of the largest enterprise Unified Communications infrastructures in the world.

Charles L. Houser is co-founder and EVP of Sales and Marketing. Charles is responsible for growing the Green Cloud partner base and sales and brings 18 years of experience as an entrepreneur and senior manager in the telecommunications industry to Green Cloud.

Don Tesner is Green Cloud's Chief Financial Officer. Don is a Certified Public Accountant (CPA) with over 30 years' experience and is a Certified Global Management Accountant, a designation that distinguishes professionals who have advanced proficiency in finance, operations, strategy and management.

Technical Operations Department
The Green Cloud Technical Operations (CTO) group maintains highly skilled and competent individuals with appropriate training and certifications relevant to job function. Operations employee certifications include:

- ITIL Foundation
- Cisco CCNP, CCNA
- VMware VCP-Cloud, VCP, VCA, VTSP, VSP, VCNP
- Microsoft MCITP, MCSE, MCSE, MCTS
- ISC2 CISSP
- Security+, A+

Assignment of Authority and Responsibility
The management team continually monitors progress toward achieving business goals. Management team members are responsible for developing plans to achieve the objectives assigned to them. The authority and responsibility to execute on tasks flows from management to managers and then to line personnel.

The management team uses various methods of communication and control to help ensure that employees understand their individual roles and responsibilities as well as the authority carried by their positions and their ascending and descending reporting relationships. Methods include:

- new-hire training
- annual privacy and security training covering individual responsibilities for compliance with information privacy and security policies, protection practices, and procedures
- individual performance reviews
- group-specific training as well instruction on the use of new products and services, as needed

Human Resources Policies and Practices
Human Resources is responsible for staffing, employee orientation, managing compensation, recognition, and benefits, and administrative and employment-related programs, practices, and policies.

The staffing process begins with vetting of applicants through multiple interviews, investigation of past employment, and confirmation of educational credentials. New hires must pass a pre-employment background screening.

New employees go through an orientation program to communicate policies on security, privacy, proprietary information, workplace harassment, equal employment opportunity, and employee conduct, in addition to other policies.

Procedures

Procedures are in place to manage the security and availability of customer data. Please refer to the following sections for specifics on the procedures involved with: Service Lifecycle, Risk Assessment, Support, Availability Safeguards, and Control Monitoring.

Data

Green Cloud provides a cloud computing environment for a wide range of business enterprises. The infrastructure is built on enterprise-class hardware, offering customers HIPAA and PCI compliant options for all or part of their business requirements. Green Cloud's products and services allow Partners to deliver a wide range of continuity services from simple off-site backup to full infrastructure recovery in the event of a disaster.

Information Ownership
All data stored within the Green Cloud system is property of the end-customer. Green Cloud does not require logical access to the data residing within customer operating system environments. Customers have the ability to move data into and out of the system without Green Cloud approval or assistance. Customers are responsible for data lifecycle management within their virtual environments, including data classification, handling, and encryption. At the time of service decommissioning, all customer data is deleted from Green Cloud systems. It is the customer's responsibility to transfer data out of the Green Cloud systems or coordinate data offloading before terminating services.

Service Lifecycle

On-boarding
Once the Partner has entered into a service agreement for IaaS, a virtual datacenter is provisioned through the administrative interface of the vCloud Director portal and access credentials are provided to the Partner. From here, the Partner can self-provision individual virtual machines within their organization upon demand using allocated resources. This onboarding process is handled by the Service Delivery team through both manual and automated systems.

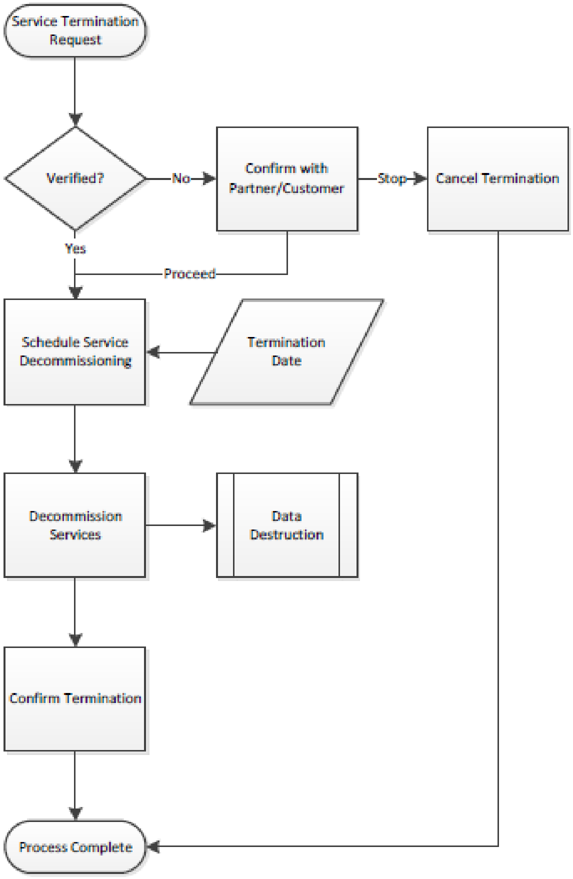
Resources are allocated to a virtual datacenter based on the contracted resources in the service agreement with the customer. This allows the customer to consume up to the allocated resources in their datacenter as needed. Resources can be modified by submitting a service request or change order.

Service Provisioning
Partners have the ability to self-provision virtual machines through the vCloud Director interface. Partners can request provisioning of additional services such as backup, replication, and application licenses through the help desk (Partner Support) by opening a Service Request. Staff will initiate the appropriate workflows and verify with the requester when complete. Partners and end-customers maintain their own authentication and access control policies and systems within their virtual environments. Green Cloud does not require or maintain permanent access accounts within Partner or customer environments.

Service Modification
As their end-customer environments or needs grow and change, Green Cloud delivers additional or new resources to the Partner. This change process is handled by the Service Delivery and Partner Services teams through both manual and automated systems, upon receipt of a Service Request or Change Order.

Service Decommissioning
Services may be decommissioned as part of a normal service lifecycle or due in part to an agreement termination. If the decommissioning is a normal lifecycle event, the Partner can manage removal of their servers and data themselves from within the portal. Complementary and ancillary services, such as licensing and backup, must be terminated via a Service Request.

In the event of agreement termination, Green Cloud will decommission all services and reclaim all resources as of the effective date of termination. This includes deletion of the virtual data center and virtual machines and appliances, thereby removing all customer data. The following graphic summarizes the process to decommission customer services.



Boundaries of the Green Cloud System

This report includes the Green Cloud infrastructure and the service offerings as described above. Any other Green Cloud services are not included within the scope of this report. The accompanying description references only the policies, procedures, and control activities at Green Cloud and does not include the specific policies, procedures, and control activities for any subservice organizations or vendors.

The boundaries of the Green Cloud system are the specific aspects of the Company's infrastructure, software, people, procedures, and data that are directly necessary to provide the IaaS, DRaaS, DaaS, and BaaS offerings as described above. Any infrastructure, software, people, procedures and data that indirectly support the services provided to Partners are not included within the boundaries of the system. The covered system specifically does not include the virtual or physical servers and systems within the Partner or end-customer environments that may be used to access, connect to, or utilize Green Cloud's services. End-customer virtual machines within their provided virtual data center environment are the sole responsibility of the Partner and/or end-customer.

Monitoring of Subservice Organizations

Green Cloud outsources data center facility management from professional data center operating companies (subservice organizations). Section Four of this report and the description of the system only cover the common criteria categories relevant to Green Cloud and exclude the related controls of the subservice organizations. Through the review of the subservice organizations' SOC 2 or other security policies, processes, and reports, Green Cloud ensures that all subservice organizations have sufficient availability and security controls in place and monitor adherence to those processes and procedures. Certain applicable common criteria can only be met if physical security and environmental controls at the subservice organizations are designed and operating effectively.

Data Center Facility Providers

Green Cloud's data center service providers offer geographic diversity in conjunction with state-of-the-art facilities. Designed and built with reliability, security, and resiliency in mind, they provide fully redundant high-density power and cooling capacities, fully integrated UPS systems, site-wide security and fire protection systems, and access control through customer portals.

Quality Technology Services (QTS)

QTS provides the physical data center facility for the Atlanta, GA and Dallas, TX data centers. QTS is responsible for physical security, environmental control, and power delivery. Green Cloud maintains responsibility for facility access lists that QTS enforces. Green Cloud does not utilize QTS for any computing or consulting services.

Iron Mountain

Iron Mountain provides the physical data center facility for the Phoenix, AZ data center. Iron Mountain is responsible for physical security, environmental control, and power delivery. Green Cloud maintains responsibility for facility access lists that Iron Mountain enforces. Green Cloud does not utilize Iron Mountain for any computing or consulting services.

Flexential

Flexential provides the physical data center facility for the Nashville, TN data center. Flexential is responsible for physical security, environmental control, and power delivery. Green Cloud maintains responsibility for facility access lists that Flexential enforces. Green Cloud does not utilize Flexential for any computing or consulting services.

CyrusOne

CyrusOne provides the physical data center facility for the Houston, TX data center. CyrusOne is responsible for physical security, environmental control, and power delivery. Green Cloud maintains responsibility for facility access lists that CyrusOne enforces. Green Cloud does not utilize CyrusOne for any computing or consulting services.

Immedion

Immedion provides the physical data center facility for the Greenville, SC data center. Immedion is responsible for physical security, environmental control, and power delivery. Green Cloud maintains responsibility for facility access lists that Immedion enforces. Green Cloud does not utilize Immedion for any computing or consulting services.

Noval CoWorking

Noval CoWorking provides the physical data center facility for the Minneapolis, MN data center. Noval CoWorking is responsible for physical security, environmental control, and power delivery. Green Cloud maintains responsibility for facility access lists that Noval CoWorking enforces. Green Cloud does not utilize Noval CoWorking for any computing or consulting services.

Commitments and System Requirements

Commitments

Commitments are declarations made by management to Partners, referred to as "Customers" in contracts, regarding the performance of the System. Commitments are communicated and made publicly available in the Service Level Agreement and Maintenance Policy. The Company's primary Service Level Agreement (SLA) is as follows:

"Green Cloud commits to Customer that the Green Cloud network and the Green Cloud infrastructure supporting Cloud Services will be available at all times (100% uptime), excluding maintenance periods."

Green Cloud also makes supporting commitments for some service performance benchmarks referred to as Service Level Objectives (SLOs) as described in that specific products' Service Description. These include, for example, IOPs based on storage service profile, restore time objectives for Disaster Recovery and response time objectives in the Incident Management process.

System Requirements

System requirements are specifications regarding how the infrastructure should function to meet the Company's commitments to Partners. Requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls such as use of user IDs and passwords to access systems
- Risk assessment standards
- Change management controls
- Monitoring controls

Changes to the System

Green Cloud invokes the Change Management process during all stages of system and product development lifecycles and when there are security or availability commitments at risk. The Change Management process may also be invoked to introduce repairs or system enhancements that mitigate deficiencies or vulnerabilities. Changes are classified as minor, standard, major, or emergency.

A Minor change is one which has not been pre-classified as a standard change or service request (e.g. no pre-existing Method of Procedure), is not an emergency, and does not meet the criteria for a major change. Minor changes will be subject to the Peer Review process and will be logged against the relevant configuration item.

A Standard change is a low or medium risk change that can be implemented using an approved Method of Procedure (MOP). Standard changes require a change request to be assessed and approved by the Change Advisory Board (CAB) and will be logged against the relevant configuration item(s). Standard changes are requested by users via the Service Request process. Service requests that are out of scope of the change management process (see above) will be processed according to the Service Request Fulfillment Process.

Changes that have the potential to have a High or Very High impact on a production service are treated as Major change requests and tracked via the change management process, and guided by the Service Design and Transition Process in cases where new services are being introduced or existing services retired. These specific changes to services are planned and managed as projects. Major changes require a change request to be assessed and approved by the Change Advisory Board (CAB) and are logged against the relevant configuration item(s).

Emergency changes are changes which are urgently required in order to resolve an Urgent service impacting Incident and High Impact and/or Problems with Urgent priority. These are expedited through the change management process and provided additional resources where required. Note that a failure in forward planning to log a minor change in enough time to obtain approval does not constitute an emergency change and is not be treated as such.

Availability
The availability principle refers to the accessibility of the system or services as committed by the Company's service level agreement. The availability of the infrastructure is dependent on many aspects of the Company's operations. Availability includes consideration of risks during normal business operations, during routine failover of redundant elements of the system, as well as risks related to the continuity of business operations during a disaster.

The Company has designed its controls to address the following availability risks:

- Insufficient capacity (compute, storage, network)
- Power interruptions
- Carrier outages
- Natural Disaster (loss of physical site)

In evaluating the suitability of the design of availability controls, the Company considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of recovery procedures, the reliability of the restoration process, and the access required to restore data or devices. In evaluating the design of data availability controls, the Company considers that most data loss does not result from disasters but, rather, from routine processing errors and failures of system components.

A number of controls are in place to address the availability risks described above. For example, the network management system is utilized to monitor infrastructure availability and performance and generates alerts when specific predefined thresholds are met. All management infrastructure is backed up daily by an automated system and replicated off-site. An automated backup system is in place to perform customer backups based on subscription. The automated backup system is configured to alert the Network Operations Center and/or Partner Support teams, depending on the type and severity of an operational failure. A documented Service Continuity plan is in place (also known as a Business Continuity Plan or Disaster Recovery plan. The primary components of the disaster recovery process are scheduled to be performed on at least an annual basis, such as testing recovery of the critical and redundant management and networking appliances and virtual servers in another cabinet, chassis, or data center.