Green Cloud Technologies

Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security, Availability, and CCM Criteria on the Secure Cloud Platform System (SOC 3)

For the period April 1, 2019 to March 31, 2020

DHG

An Independent Service Auditor Report issued by
Dixon Hughes Goodman LLP

table of contents

This report, including the description of tests of controls and results thereof, is intended solely for the information and use of the Company; user entities of the Company's system during some or all of the specified period and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding. This report is not intended to be, and should not be, used by anyone other than these specified parties.

DIXON HUGHES GOODMAN LLP

section I: independent service auditor's report

To: Management of 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 its Secure Cloud Platform system (system) were effective throughout the period April 1, 2019, to March 31, 2020, to provide reasonable assurance that (a) 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*); and (b) the criteria set forth in the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) Version 3.0.1 control specifications ("CCM criteria") were achieved.

Green Cloud uses subservice organizations to provide data center services and antivirus management. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Green Cloud, to achieve Green Cloud's service commitments and system requirements based on the applicable trust services criteria. The description presents Green Cloud's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Green Cloud's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Green Cloud, to achieve Green Cloud's service commitments and system requirements based on the applicable trust services criteria. The description presents Green Cloud's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Green Cloud's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

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 (a) Green Cloud's service commitments and system requirements were achieved; and (b) the CCM criteria 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 services 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 management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that (a) the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria; and (b) the CCM criteria were achieved. 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 and CCM 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 and CCM 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 (a) the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria; and (b) the CCM criteria were achieved. 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 April 1, 2019, to March 31, 2020, to provide reasonable assurance that (a) Green Cloud's service commitments and system requirements were achieved based on the applicable trust services criteria; and (b) the CCM criteria were achieved is fairly stated, in all material respects.

Dixon Hughes Goodman LLP

Greenville, South Carolina

May 27, 2020

section II: management's assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Green Cloud's Secure Cloud Platform system (system) throughout the period April 1, 2019, to March 31, 2020, to provide reasonable assurance that (a) Green Cloud's service commitments and system requirements relevant to security and availability were achieved; and (b) the CCM criteria were achieved. Our description of the boundaries of the system is presented in Section III 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 April 1, 2019, to March 31, 2020, to provide reasonable assurance that (a) 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*); and (b) the criteria set forth in the Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) Version 3.0.1 control specifications ("CCM criteria") were achieved. Green Cloud's objectives for the system in applying the applicable trust services criteria and CCM criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria and CCM criteria. The principal service commitments and system requirements related to the applicable trust services criteria and CCM criteria are presented in Section III.

Green Cloud uses subservice organizations to provide data center services and antivirus management. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Green Cloud, to achieve Green Cloud's service commitments and system requirements based on the applicable trust services criteria. The description presents Green Cloud's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Green Cloud's controls. The description does not disclose the actual controls at the subservice organization.

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

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

We assert that the controls within the system were effective throughout the period April 1, 2019, to March 31, 2020, to provide reasonable assurance that (a) Green Cloud's service commitments and system requirements were achieved based on the applicable trust services criteria; and (b) the CCM criteria were achieved.

Green Cloud Technologies

section III: management's description of its system and controls

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, security, and backup features provide a powerful blend of dependability, scalability, resiliency, 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)

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
Greenville, South Carolina	Immedion
Houston, Texas	CyrusOne
Phoenix, Arizona	Iron Mountain
Dallas, Texas	QTS
Minneapolis, Minnesota	Novel Coworking (environmental controls only)

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.

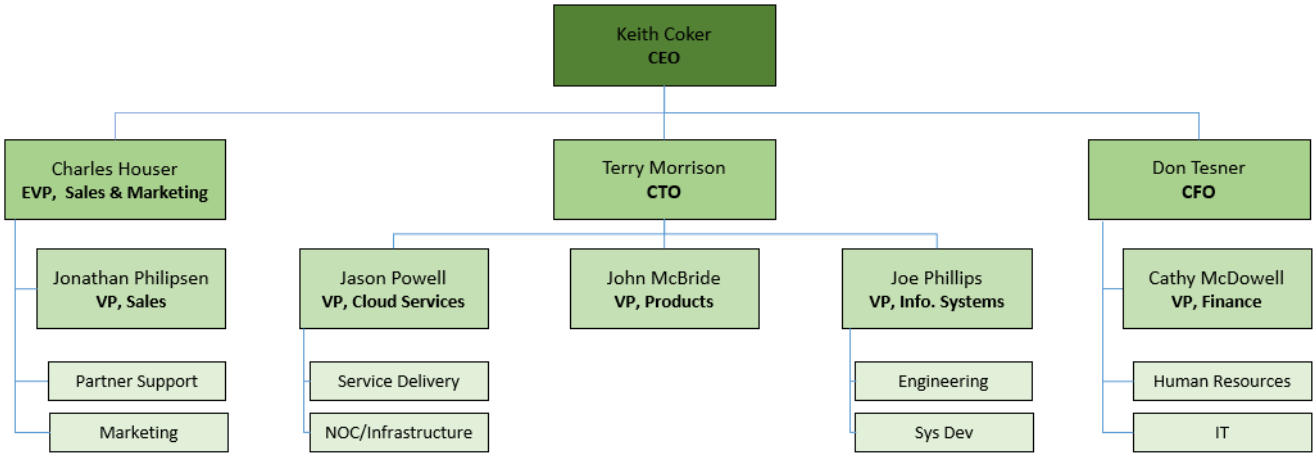
Software

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. Green Cloud partners can only access their IaaS environments through the vCloud Director web interface.

Green Cloud also offers a Partner Portal, through which users can request quotes, view service usage, review and pay invoices, and communicate on service requests or service incidents. Green Cloud does not currently offer an API for Partners to access or manage services directly, however, internal APIs are used to pull various usage statistics and data points into the Portal for status reporting.

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.

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.

Terry Morrison in Green Cloud's Chief Technology Officer. Terry has over 23 years of experience in the technology industry and most recently served as Chief Technology Officer for St. Louis based TierPoint where he was responsible for the company's hybrid IT solutions and management of the organization's IT, network design and engineering architecture teams. Prior to that, Morrison was Senior Vice President of Technology for Perimeter Technology Center, a company he co-founded until Perimeter was acquired by TierPoint in 2011.

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, 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. Access to and data transfer from the system requires a secure connection protocol, such as IPsec VPN, PCoIP, SSL, and/or TLS, depending on the service interface.

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 OS or 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.

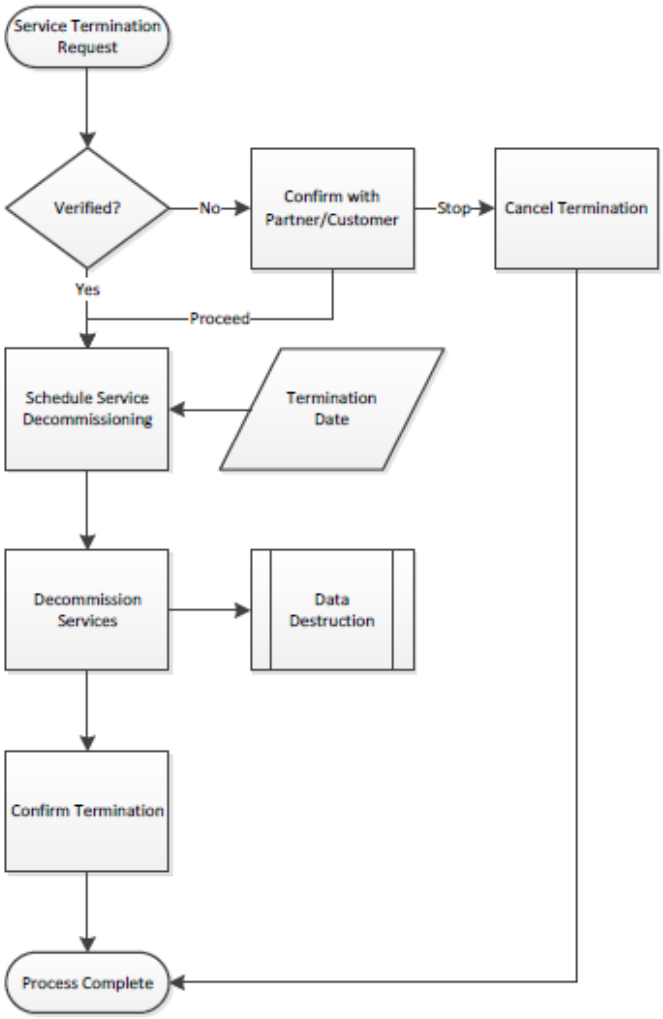
Service Modification

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 IV 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.

Novel Coworking

Novel Coworking provides the physical data center facility for the Minneapolis, MN data center. Novel Coworking is responsible for physical security, environmental control, and power delivery. Green Cloud maintains responsibility for facility access lists and Green Cloud does not utilize Novel 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.

Internal Changes

For internal information system changes that do not impact or modify the service infrastructure, such as those relevant to the Partner Portal, Green Cloud may invoke the Change Management process and/or the Software Development Life Cycle. Such changes may address bug fixes or enhancements to feature/functionality offered to the Partner via the Portal. Prior to any Portal update, developers first modify the code base in a test environment (branch), publish to a quality assurance environment and perform unit testing, and finally release to production.

Vulnerability Management

Green Cloud's technical vulnerability management policy addresses those internal and external threats to the system. Patches and updates will typically be issued by software and Operating System vendors on a regular schedule as cumulative packages or as 'hot fixes' to address certain issues. Green Cloud has established controls to obtain copies of the software updates when they are issued by the vendor and schedules of the installation of updates depending upon a number of factors, including but not limited to:

- The criticality of the systems being updated
- The expected time taken to install the updates (and requirements for service outages to users)
- The degree of risk associated with any vulnerabilities that are closed by the updates
- Co-ordination of the updating of related components of the infrastructure
- Dependencies between systems

Infrastructure upgrades, system firmware patches, and critical vendor updates resulting from the vulnerability management process are governed by the Change Management process.

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.

Network Security

Green Cloud addresses network security through a variety of complementary processes and services. In addition to basic bandwidth and throughput network monitoring, Green Cloud employs next generation firewalls, intrusion detection services, security information and event management (SIEM), weekly vulnerability scanning, and third-party penetration testing. Firewall standards are reviewed annually and both configuration and change logs are updated and announced upon any rule or access list change. The intrusion detection, PCI-ASV vulnerability scanning, and SIEM services feed critical alerts directly into the Incident Management process are reviewed quarterly in the Information Security review. Finally, annual penetration testing performed by an external third-party provides validation of the security hardening practices employed by Green Cloud.

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication

Organizational Control Environment

Green Cloud acknowledges and emphasizes the importance of controls and ethical behavior throughout the organization. Green Cloud management has established a control environment that sets the tone for internal activities and processes. Key elements of the control environment include:

- Integrity and ethical values
- Commitment to competence
- Management's philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resources policies and practices

Integrity and Ethical Values

Green Cloud has established programs and policies designed to promote and support integrity and ethical values within the organization. New employees are required to attend orientation and review the Employee Handbook, which covers employee responsibilities. Employees are required to sign a form acknowledging receipt and

understanding of the contents of the Employee Handbook. The Employee Handbook is provided to all new employees and is accessible by all current employees via the internal document management system at all times. Updates to the employee handbook are communicated to the staff via email.

Commitment to Competence

Having people with appropriate skill sets in each job is important for the effectiveness of the internal controls. Through years of experience, management has determined the levels of experience and training required for the various job functions. Green Cloud follows a documented hiring process in which the hiring manager develops the position description and works through Human Resources' recruiters to find the right person.

An annual performance evaluation process confirms the maintenance of employees' skills and adherence to established policies and procedures. Each employee receives a review by his or her immediate supervisor. Supervisors document the evaluations and provide results to Human Resources. Appropriate managers and executives subsequently review the forms as needed. Performance evaluations may influence compensation, job placement, or remediation plans as appropriate.

Green Cloud provides access to necessary training, including offerings that technical support, security awareness, and other key areas. Access is provided to external, vendor provided training that may be required to obtain or improve skillsets.

Management's Philosophy and Operating Style

Green Cloud operations proceed under direction from senior division leadership. Senior leadership meets at least monthly to set direction and review status of ongoing operational or strategic concerns. Financial reviews occur at least monthly.

Risk Assessment

Risk assessment requires that management consider the impact of possible changes in or to the system that may render an internal control ineffective. On an annual basis a risk assessment is performed to identify threats and vulnerabilities, likelihood of occurrence, and mitigating controls.

Assess and Manage Information Technology Risks

Governance processes have been built on a risk management framework. The framework identifies, analyzes, and assesses the potential impacts of unplanned events. Green Cloud adopts risk mitigation strategies to reduce residual risk to an acceptable level. The risk assessment considers the risk tolerance of key stakeholders.

The principal elements of the risk management framework include:

- Information technology and business risk management
- Event identification
- Risk assessment
- Risk response
- Maintenance and monitoring of risk action plans

Information Technology and Business Risk Management

Green Cloud has established an integrated information technology governance, risk management, and control framework within its risk management framework. This includes alignment with the organization's risk tolerance level.

Event Identification

Management identifies events that may impact the goals or operations of the enterprise while considering business, regulatory, legal, technology, human resources, and operational aspects.

Risk Response

The management team maintains a risk response process that identifies a risk owner and affected process owners. The process ensures that cost-effective controls and security measures continually mitigate exposures to risks.

Maintenance and Monitoring of Risk Action Plan

The management team prioritizes and plans control activities to implement risk responses and to identify costs, benefits, and responsibilities for execution. Management assesses all identified risks for recommended actions and acceptance of any residual risk. The team monitors execution plans and reports deviations to management.

Information and Communication

Various methods of communication are in place to ensure that all employees understand their individual roles and responsibilities. These methods include always-on messaging applications, email bulletins, regular all-hands staff meetings, management meetings, WIKI style intranet sites, and periodic training programs for educating employees on internal developments, industry trends, and organizational development activities.

Green Cloud internally communicates information, including objectives and responsibilities for job tasks necessary to support the functioning of internal controls. Regular meetings are held which enable senior management to maintain contact with and consistently emphasize appropriate behavior and communicate objectives to operating personnel.

Green Cloud communicates with external parties regarding matters affecting the functioning of internal control, and utilizes business reviews, sales conferences, trade shows and more traditional email and telephone communication with its subservice organizations and vendors such that the roles and responsibilities are understood. Partners and Vendors are subject to the terms and conditions of their respective Services Agreements.

Green Cloud communicates with its partners through traditional email and telephone communication during the sales and onboarding phases, through help desk applications for issues and service requests, and via Status Page (status.grncld.net) notifications for both maintenance and service level interruptions. Marketing and industry announcements are made through the public Green Cloud web site (www.gogreencloud.com). Additionally, Partners have access to the Partner Portal (portal.gogreencloud.com) to place orders, request updates to open service requests and incidents, and view and pay invoices.

Support

In the event that Partners need support for services, Green Cloud offers three primary methods of contact and varying levels of issue severity.

Severity Definitions

The severity level is a measure of the relative impact of the technical issue on Partner systems. Accurately defining the severity ensures a timely response and helps Green Cloud understand the nature of the issue.

Urgent

Urgent ("Critical", or Severity 1) means there is a critical production issue affecting all users, including system unavailability and data integrity issues with no workaround available. Examples include:

- Service is down or unavailable
- A critical part of the infrastructure is unavailable or inaccessible, resulting in total disruption of work or critical business impact
- Service crashes or hangs indefinitely causing unacceptable or indefinite delays for resources or response
- Data corrupted or lost and must restore from backup
- A critical documented feature / function is not available

High

High ("Major", or Severity 2) occurs when a major functionality is impacted, or significant performance degradation is experienced. The issue is persistent and affects many users and/or major functionality. No reasonable workaround is available. Examples include:

- Service is operational but highly degraded performance to the point of major impact on usage
- Important features of the service offering are unavailable with no acceptable workaround; however, operations can continue in a restricted fashion

Medium

Medium ("Minor", or Severity 3) involves a system performance issue or bug affecting some but not all users. Short-term workaround is available, but not scalable. Examples include:

- Service is operational but partially degraded for some or all customers, and an acceptable workaround or solution exists
- Problem with non-critical feature or functionality

Low

Low ("Operational", or Severity 4) refers to an inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation, or configuration; bug affecting a small number of users. Acceptable workaround is available. Examples include:

- Minor problem not impacting service functionality
- Enhancement requests, missing or erroneous documentation
- Minor problem or question that does not affect delivery of service

Support Contact Methods

Green Cloud offers multiple methods for inputting service tickets. Customers may choose to enter tickets in the most convenient method for them, taking into account issue severity.

Phone Support

Phone support is available at all times for submitting support requests. Customers are encouraged to report all critical (severity 1) incidents directly by telephone.

Email Support

Customers may email the support center at any point to enter tickets. Any support tickets that are submitted via email are treated as if received at 8 AM the following business day (Monday – Friday excluding major holidays).

Capacity Management

Effective management of data center capacity is crucial to meeting availability and service level objectives. Green Cloud utilizes several systems to manage different aspects of capacity in the data centers. The Network Operations Center and Engineering groups manage capacity of the following systems:

Compute Capacity

Green Cloud measures and reports on capacity of each production compute node. Measurements factor in both CPU and RAM usage across hosts in the resource and management clusters. New systems are procured and provisioned in advance to ensure N+1 host redundancy at minimum as well as capacity for new customer onboarding.

Storage Capacity

Storage consumption is monitoried in both physical and virtual terms. vCloud allocation of storage and provisioning is monitored through vCloud Director. Physical storage usage is managed through storage vendor management software. This information is used to ensure procurement of additional storage to back the system as well as storage allocation amongst volumes within the vCloud environment.

Network Capacity

A variety of tools are used in concert to monitor and report on capacity of the core networking systems and external Internet connections. This information is used to ensure performance of the network system and prevent network bottlenecks and latency from impacting customer services. Green Cloud also utilizes the provider monitoring systems on the direct Internet links to ensure there are no bottlenecks to customer traffic.

Data Center Power Capacity

Power is managed through PDU vendor management software as well as through power usage information provided by the physical data center vendors in use. Power usage is monitored to ensure redundant circuits are not oversubscribed.

Data Center Physical Space

Compute, storage, and power capacity numbers are used along with sales plans to predict growth and future space requirements. Space is procured in advance of required system deployment. Data center locations are chosen with expansion ability as a key factor to support the ability to expand its footprint in preparation for continued growth.

Business Continuity and Disaster Recovery

The CTO oversees development of a coordinated service continuity plan (Disaster Recovery Plan) to enable proper action before, during, and after an emergency affecting services or operations. The plans ensure that the transition to the plan is seamless and that service to customers will continue to meet expected levels.

A response consists of three distinct phases - emergency response, recovery, and restoration – each with its own set of objectives. The duration of each phase depends on the nature of the event and its effect on business processes and applications.

Emergency Response

During the unfolding of an event, the organization first takes action to protect life and property. After that, the priority shifts to mitigation of damage, preservation of property, and initial assessment of the effects. The operations team decides whether to declare a disaster, based on the event's effect on critical business functions, applications, customers, and business associates.

Green Cloud's Business Continuity Plan incorporates hardware failure, network failure, carrier failure, and natural disaster. While not feasible to test the loss of a complete data center location, the underlying system components are tested at least annually for failover capabilities and constraints. More common issues, such as a single host, network element, or storage array failure, have redundancies build into the standard design and capacity management plan.

Incident Response

The CTO manages those with the primary responsibilities concerning the incident response process. The Incident Management process controls the communication and response plan for non-security related issues (e.g. infrastructure, network interruptions, and service level degradations).

For Security Incidents, all Green Cloud employees are responsible for reporting any suspected concerns to the Information Security group for further investigation. The Information Security Manager is available 24x7 for reporting suspected security incidents. Tabletop testing of the Security Incident Response processes is performed quarterly and updates to process and systems made accordingly.

Green Cloud recorded two relatively minor potential security incidents during the examination period, one of which was cleared (no data breach or loss) following the theft of a company-owned laptop, and the other mitigated (corporate headquarter video surveillance system went offline for a short period).

Recovery

As soon as the operations team declares a disaster, efforts to recover from it begin. The objective of recovery is continuation of functions and applications to support customers and critical internal operations. The phase continues until restoration of all services is complete and operations are ready to return to normal.

Restoration

The organization performs the tasks required to rebuild damaged facilities and restore original business functionality. Restoration runs concurrently with recovery operations.

Control Monitoring

To help determine effectiveness of controls, Green Cloud management performs regular ongoing monitoring as well as external audits. Monitoring includes:

Data Center Operations

Using a variety of commercial automated monitoring tools, the Network Operations Center is responsible for continuous monitoring of infrastructure and applications necessary for delivering or supporting service operation.

Business Impact Analysis

Green Cloud leadership annually reviews the known threats and identified vulnerabilities to the system, as they pertain to business critical functions such as demand generation, business continuity, revenue, and information security. Processes, systems, and/or personnel enhancements may be required to mitigate unacceptable business risks and are tracked as individual projects or tasks.

Independent Control Evaluations

Green Cloud contracts with an external audit firm on an annual basis to provide independent testing and third-party attestation of internal control relevance and adherence.

Trust Services Criteria and Related Controls

Green Cloud has specified the applicable trust services criteria and identified the controls that are designed to achieve the applicable trust services criteria.

Subservice Organizations

Subservice organizations were not subject to examination by Dixon Hughes Goodman LLP.

Complementary Subservice Organization Controls

The following table presents the nature of services provided by each subservice organization and the applicable trust services criteria that are intended to be met by controls at the subservice organization alone or in combination with controls at Green Cloud. The following table describes the types of subservice organizations used by Green Cloud.

Subservice Organization	Service(s) Provided	Relevant Criteria Addressed
QTS	A service provider used to assist in data storage co-location and physical security services in Atlanta, GA and Dallas, TX. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for assuring that only appropriate personnel maintain access to the physical equipment and that environmental controls are maintained	CC 6.0 A 1.0
Flexential	A service provider used to assist in data storage co-location and physical security services in Nashville, TN. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for assuring that only appropriate personnel maintain access to the physical equipment and that environmental controls are maintained	CC 6.0 A 1.0

Subservice Organization	Service(s) Provided	Relevant Criteria Addressed
CyrusOne	A service provider used to assist in data storage co-location and physical security services in Houston, TX. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for assuring that only appropriate personnel maintain access to the physical equipment and that environmental controls are maintained	CC 6.0 A 1.0
Iron Mountain	A service provider used to assist in data storage co-location and physical security services in Phoenix, AZ. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for assuring that only appropriate personnel maintain access to the physical equipment and that environmental controls are maintained	CC 6.0 A 1.0
Immedion	A service provider used to assist in data storage co-location and physical security services in Greenville, SC. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for assuring that only appropriate personnel maintain access to the physical equipment and that environmental controls are maintained	CC 6.0 A 1.0
Novel Coworking	A service provider used to assist in data storage co-location and environmental services in Minneapolis, MN. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for assuring that environmental controls are maintained	CC 6.0 A 1.0

Subservice Organization	Service(s) Provided	Relevant Criteria Addressed
Cylance	A service provider used to assist in antivirus management and monitoring services. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for assuring that Green Cloud assets have antivirus installed and are configured to receive updated antivirus signatures on a periodic basis	CC 6.0

Complementary User Entity Controls

Green Cloud's processes were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve certain criteria included in this report. This section describes additional internal controls that should be in operation at user organizations to complement internal controls. The complementary user entity controls below do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations.

Complementary User Entity Controls (CUECs)	Related Criteria
User organizations are responsible for ensuring access to the external infrastructure portal(s) is restricted to authorized employees and that user names and passwords are kept confidential.	CC 6.1
User organizations are responsible for performing annual user access reviews to Green Cloud's services.	CC 6.2
User organizations are responsible for confirming access to the Green Cloud services is immediately disabled for terminated user-entity personnel.	CC 6.2
User organizations are responsible for changing passwords to Green Cloud Systems periodically – at least every 90 days.	CC 6.1
User organizations are responsible for implementing data life-cycle management procedures, including data classification, handling, and encryption.	CC 6.1
User organizations are responsible for deleting their personal data from Green Cloud resources when necessary.	CC 6.5
User organizations are responsible for creating and reviewing rule sets for customer-managed virtual firewall systems.	CC 6.6
For user organizations maintaining their own hardware, user organizations are responsible for patching and updates.	CC 8.1
User organizations are responsible for notifying Green Cloud of any issues, problems, or needed changes.	CC 8.1
User organizations are responsible for their own backups, unless they are contracted for BaaS.	A 1.2