COMPUTER
GUIDANCE
CORPORATION

Independent Service Auditors' Report

Computer Guidance Corporation

Independent Service Auditors' Report on Computer Guidance Corporation's Description of Its eCMS Hosting Services System, and on the Suitability of the Design and Operating Effectiveness of Controls Relevant to the Security, Availability & Confidentiality Trust Services Criteria

Reporting for the Period

CliftonLarsonAllen LLP
20 East Thomas Road, Suite 2300
Phoenix, AZ 85012

CLACONNECT.COM

WEALTH ADVISORY

OUTSOURCING

AUDIT, TAX, AND
CONSULTING

COMPUTER GUIDANCE CORPORATION
TABLE OF CONTENTS

I. Independent Service Auditors' Report

Management
Computer Guidance Corporation
Scottsdale, Arizona

Scope

We have examined Computer Guidance Corporation's (CGC) description of its eCMS Hosting Services system entitled "Computer Guidance Corporation's Description of Its eCMS Hosting Services System" throughout the period October 1, 2018 to December 31, 2019 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria), and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description throughout the period October 1, 2018 to December 31, 2019, to provide reasonable assurance that CGC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The information included in section V, "Other Information Provided by Computer Guidance Corporation That Is Not Covered by the Service Auditor's Report" is presented by CGC's management to provide additional information and is not a part of CGC's description of its eCMS Hosting Services system made available to user entities throughout the period October 1, 2018 to December 31, 2019. Information about CGC's management responses has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

CGC uses a subservice organization to provide colocation data center services. The description includes only the control objectives and related controls of CGC and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by CGC can be achieved only if complementary subservice organization controls assumed in the design of CGC's controls are suitably designed and operating effectively, along with the related controls at CGC. Our examination did not extend to controls of 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 control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of CGC's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

CGC 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 CGC's service commitments and system requirements were achieved. CGC has provided the accompanying assertion titled "Assertion of the Management of Computer Guidance Corporation" regarding its eCMS Hosting Services system (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. CGC is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the services organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

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

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

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in section IV.

Opinion

In our opinion, in all material respects -

a. the description fairly presents CGC’s eCMS Hosting Services system that was designed and implemented throughout the period October 1, 2018 to December 31, 2019 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 1, 2018 to December 31, 2019 to provide reasonable assurance that CGC’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if it controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of CGC’s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period October 1, 2018 to December 31, 2019 to provide reasonable assurance that CGC’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization and user entity controls assumed in the design of CGC’s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of management of CGC, user entities of CGC’s eCMS Hosting Services System during some or all of the period October 1, 2018 to December 31, 2019, business partners of CGC subject to risks arising from interactions with the eCMS Hosting Services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization’s system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations

- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

April 21, 2020
Phoenix, Arizona

II. Assertion of the Management of Computer Guidance Corporation

Assertion of the Management of Computer Guidance Corporation (CGC) Regarding Its eCMS Hosting Services for the Period October 1, 2018 to December 31, 2019

We have prepared the accompanying description of Computer Guidance Corporation's eCMS Hosting Services system entitled, "Computer Guidance Corporation's Description of Its eCMS Hosting Services System," throughout the period October 1, 2018, to December 31, 2019 (description) based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about the eCMS Hosting Services system that may be useful when assessing the risks arising from interactions with CGC's system, particularly information about system controls that CGC has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, (AICPA, Trust Services Criteria).

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

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

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

a) the description presents CGC's eCMS Hosting Services system that was designed and implemented throughout the period October 1, 2018 to December 31, 2019, in accordance with the description criteria.

b) the controls stated in the description were suitably designed throughout the period October 1, 2018 to December 31, 2019, to provide reasonable assurance that CGC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of CGC's controls throughout that period.

c) the controls stated in the description operated effectively throughout the period October 1, 2018 to December 31, 2019, to provide reasonable assurance that CGC's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of CGC's controls operated effectively throughout that period.

III. Computer Guidance Corporation's Description of Its eCMS Hosting Services System

Organization Background

Company Profile

Computer Guidance Corporation (CGC) is a privately held software development company headquartered in Scottsdale, Arizona. Established in 1981 and incorporated in 1984, CGC is currently a wholly-owned subsidiary of JDM Technology Group. CGC is a trusted provider of construction management software for the commercial construction industry, setting industry standards in financial and project management software development for North America's leading construction companies.

As a leading provider of construction management software for the commercial construction industry, our software package is a fully integrated Enterprise Resource Planning solution with accompanying productivity tools that consistently deliver precise, mission-critical information that empowers organizations with complete, real-time visibility and control across their enterprise. Administration of the application is performed by the enterprise Infrastructure & Cloud Services (ICS) team within CGC.

Business Services - Overview

This solution suite is offered with a comprehensive set of solution services including, but not limited to:

1. business process consultation,
2. functional review and process re-engineering,
3. product implementation,
4. managed hosted cloud services, also referred to as Software as a Service (SaaS),
5. disaster recovery services,
6. application support,
7. custom programs and BI functionality development, and
8. world-class solutions training.

eCMS® Enterprise Resource Planning

The centerpiece in the Computer Guidance family of solutions, eCMS® (eCMS), was developed with the input of leading North American construction companies. This browser-based financial accounting solution delivers mission-critical information that empowers organizations with complete, real-time visibility and control across their organization. eCMS is a solution for any construction company seeking a financial software suite. This solution suite is offered with a comprehensive set of solution services including, but not limited to, product implementation, hardware solutions configuration, disaster recovery services, dedicated customer support center, and world-class solutions training.

Business Services Contractual Agreement(s)

All relationships and terms of business between CGC and clients for business services are documented in written contracts, agreements, and amendments. Service requirements and restrictions, along with reporting obligations, contact information, pricing, and data conversion instructions, (all of which are set forth in the executed contract and/or attachments thereto) provide the information necessary to initiate services.

Key Business Areas:

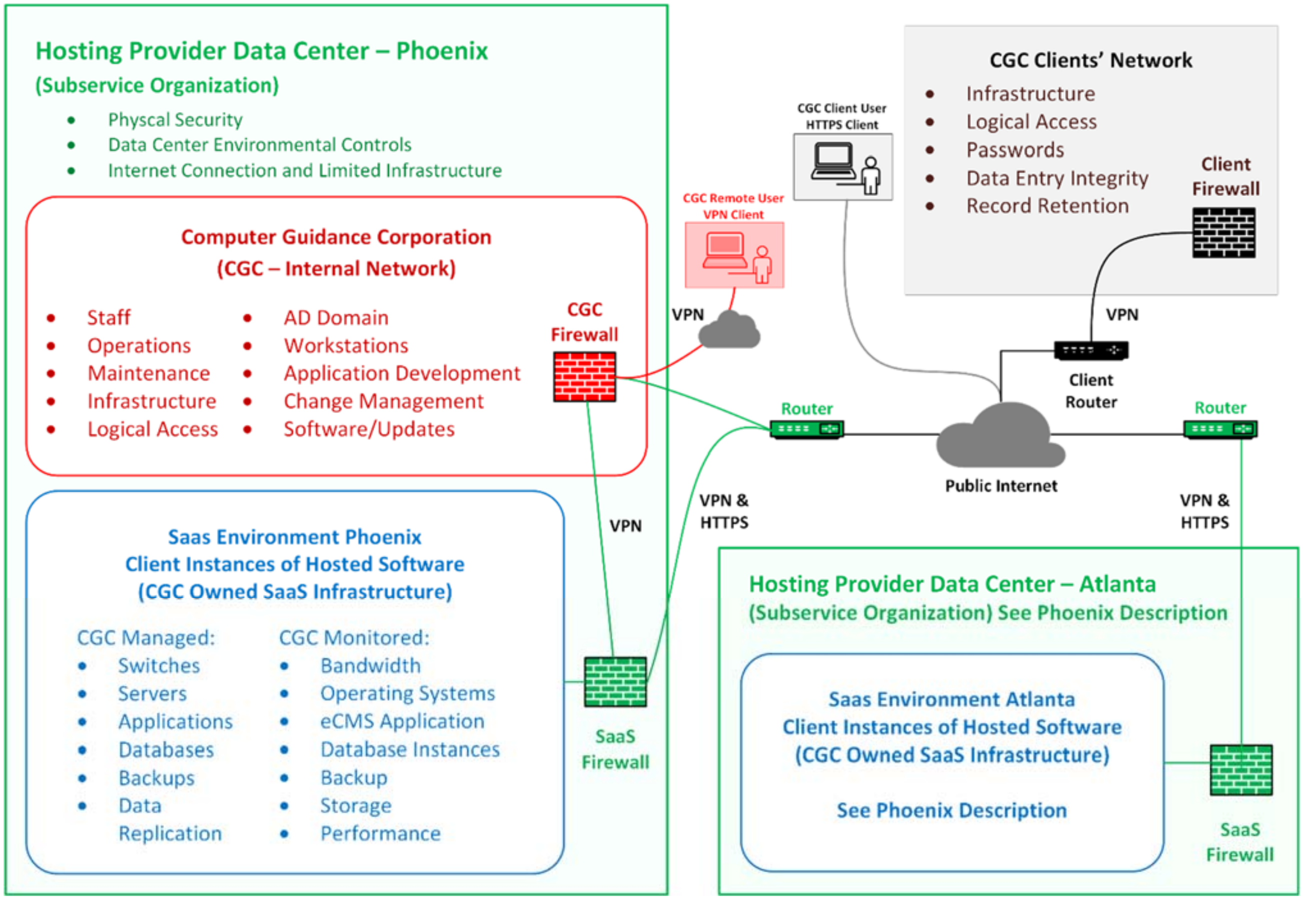
Operations related to the delivery of CGC’s products and/or services are supported by the following functional business areas:

- Application Support;
- Technical Services;
- Professional Services;
- Software Development;
- Software Delivery.

System Description

System Illustration

The following diagrams illustrate the system architecture associated with hosting services:



It is important to note that the scope of this SOC engagement is limited to reporting on controls that are the responsibility of CGC as identified in **red** and **blue** in the above illustration.

Controls that are illustrated as **green** are the responsibility of a Subservice Organization with **black** being the responsibility of the CGC client user.

System Environment

Infrastructure

The physical and hardware components of a system (facilities, equipment, and networks)

Facilities

Headquarters

CGC operates from professional offices located in Scottsdale, Arizona which function as the company's headquarters. The majority of CGC employees work from these offices when they are not working from their home office or other remote location(s).

Hosting Partner Data Centers

CGC has contracted with Tech Data Corporation to provide two physical data centers, operated by third party subservice organizations (Hosting Partner), in two distinct geographical regions in the United States. The CGC operations environment, the development environment, and a significant number of the servers dedicated to the SaaS environment, are located at the Phoenix, Arizona data center.

The second data center is in Atlanta, Georgia; and hosts servers dedicated to the SaaS environment. Physical access is managed by the respective Hosting Partner data center based on the aforementioned contracts.

Equipment

CGC maintains an inventory of all equipment within each of the Hosting Partner data centers including identification of the manufacturer, model, serial number, and purpose for item of equipment that is owned and managed by CGC. The manufacturer's warranty covers equipment purchased by CGC. Categories of equipment utilized by CGC include the following:

Communications Equipment

Internal Corporate Networks at Hosting Partner Data Centers

Routers, switches, and other communication devices have been installed within CGC hosted network environment to manage data traffic on the internal corporate network.

SaaS Networks at Hosting Partner Data Centers

Routers, switches, and other communication devices to manage traffic to/from both CGC and the clients' networks to the hosting partner data centers for access to the eCMS SaaS application are installed, managed, and monitored by Hosting Partner data center staff according to the terms and conditions of our contract with them.

Server(s)

CGC utilizes the IBM® (IBM) i operating system, running on IBM hardware (iSeries), and Microsoft Windows™ Server operating systems to support the eCMS application in the hosted SaaS environment.

The iSeries operating system and Windows Server operating system have been installed on production data servers as applicable to the platform. Server hardware is owned and managed by CGC, in addition to the operating system that is licensed to CGC and maintained by the ICS team.

User Computing Device(s) for CGC Personnel

CGC primarily uses desktop workstations; but has a limited number of laptops and mobile devices that are used by individuals for both workstation/productivity purposes, and to allow for remote access to corporate resources while out of the office.

Desktop and laptop systems run Microsoft Windows operating systems for personal computers, Apple Macintosh operating system ("macOS" or "OSX") for personal computers, or Apple iOS for mobile devices.

Network

Overview

CGC Internal Corporate Environment

Management of the CGC internal corporate network, within the Hosting Partner's data center, is the responsibility of the ICS team within CGC.

eCMS Hosting Partner Environment

Management of the SaaS network that allows CGC clients to access the eCMS application, which is within the Hosting Partner Environment, is the responsibility of the Hosting Partner's data center staff.

Security Device(s)

CGC Internal Corporate Environment

Network connections to the CGC internal corporate network are protected by firewalls that are managed and monitored the ICS team staff, within CGC.

eCMS Hosting Partner Environment

Network connections from the collocation facility to client locations are protected by firewalls that are owned, managed, and monitored by the Hosting Partner's data center staff.

CGC Employee(s) Logical Access to the eCMS Hosting Partners' Environment

Access for CGC employees to the eCMS Hosting Partners' environment is initiated via a security request associated with a specific customer support requirement, and access is logged with the incident tracking and credential request system.

Connection to the eCMS Hosting Partners' environment is either accomplished through a gateway-to-gateway IP Sec VPN connection between the CGC and SaaS networks, or is facilitated by a company-provided device with an IPsec VPN client installed on the device. Access to the SaaS environment servers must be from a company authorized device, utilizing named user accounts. Generic, guest, and/or group log-in credentials are not permitted.

CGC Customer Logical Access to eCMS Hosting Partners' Environment

Customers can either connect to the eCMS Hosting Partner Environment using a web browser via a point-to-point IPsec VPN connection, or the public internet by way of an HTTPS web access portal. Provisioning is initiated by CGC; and is initiated, setup, and maintained by the Hosting Partner. The Hosting Partner owns and manages the firewall hardware at the data center end-point, which facilitates client logical access. The client owns and manages the configuration and hardware at the client end-point. Client access to the CGC internal corporate network is not permitted, and is prevented by firewall policies between the networks.

Software

The programs and operating software of a system (systems, applications, and utilities)

Operating System(s) Software

Overview

An inventory of all licensed software that supports the SaaS hosting environment is maintained by CGC and includes operating system software version, applications, and utilities that are covered by a software maintenance/support agreement for bug fixes, patches, and new releases; as well as access to vendor support.

Servers

The following operating system(s) software has been installed on servers in support of production and nonproduction operations:

- Microsoft Windows Server
- IBM i (for iSeries)

User Computing Device(s)

Microsoft Windows operating system software for personal computers has been installed on all workstations in support of development, testing, and production operations.

Security Software

Security software has been installed on Windows servers and workstations utilized by CGC employees, as well as on Windows servers in the SaaS environment, to protect data and the underlying infrastructure from unauthorized access and activity within development, operational, and production environments.

Security software includes, but is not limited to, the following:

- Anti-virus software – licensed/managed by CGC
- Intrusion Detection – managed and maintained by Hosting Partner for SaaS networks
- Intrusion Prevention – managed and maintained by Hosting Partner for SaaS networks
- Event Monitoring – managed and maintained by CGC
- Event Alerting – managed and maintained by CGC

Anti-virus definition files are updated on a daily basis.

System Utilities – All CGC

Utilities to support production systems include but are not limited to the following:

- System performance and availability monitoring software
- Backup software (on/off site)
- User authentication and identification for logical access

Business Software

Enterprise Resource Planning, Business Intelligence, and Analytics

eCMS is a comprehensive suite of software applications that helps any size and type of commercial construction contractor manage all aspects of their financials and operations. Therefore, eCMS construction management software suite has been designed to address all elements of business processes for the construction industry. From cost accounting, payroll, and financial reporting, to project-wide communication and content management, eCMS manages projects from start to finish. eCMS Cloud Construction ERP SaaS delivers this integrated financial and project data on-demand for customers.

These enterprise applications consist of internally-hosted, proprietary, and nonproprietary (Cognos Analytics), software which are supported by the Software Delivery Services team at CGC. Additional specialization in support service comes through individual business analysts with advanced training such that they can support deeply technical operational aspects of the software. Support and maintenance of associated equipment is provided by the ICS team that maintains administrative control over network infrastructure; including hardware and firmware/operating systems.

Data

The information used and supported by a system (transaction streams, files, databases, and tables)

Client Data Administration

Client Data

Client data stored within the eCMS application is the responsibility of each client-user organization. CGC personnel do not have administrative authorization to input data into any client instance of the eCMS application. If any data modification is deemed necessary to correct a problem reported by a client user organization, such changes are logged, tracked, and monitored as part of a formal incident management system; and, incident details are available for review by CGC management and/or client management.

Data Segregation

Access to client data within the application is logically controlled by each client being assigned a distinct, secure, server and database instance. A unique uniform resource locator (URL) and/or internet protocol (IP) address are used to link client-users to a specific server instance with its own access control list and database. This structure prohibits the client-users from accessing or viewing any other client's data and/or resources.

Furthermore, security groups are used to limit access to menus, forms, and reports as defined by the client's designated application administrator. As such, eCMS is a single-tenant hosted solution with layered logical controls in place to ensure the confidentiality of data.

Client Data Storage

CGC replicates client databases asynchronously between the two data centers in real-time mode between iSeries servers in support of the availability of data for clients in the SaaS environment. In addition, disk-to-disk backups are performed on a daily, weekly, and monthly basis at each data center. The weekly, and monthly backups are replicated between the two data centers to maintain off-site copies of data backups.

Backups are tested annually to determine the recoverability of data for disaster recovery purposes. In all instances, CGC is responsible for monitoring the success/failure of the data backup processes.

Client Data Retention

Client-user organizations are responsible for determining data retention periods within the eCMS application.

Operational Data Administration

Overview

In support of business operations related to hosting the eCMS application, the following files and logs are available from the iSeries systems, and are maintained to support business operations and monitoring activities:

- Operating system(s) and security events logs
- eCMS Application logs

Data File(s)

All client data files containing employee, financial, or other confidential information are stored within a secure database or a structured file system on a CGC server located in the SaaS environment network for backup purposes. Access to this data is limited to individuals that have been assigned to the appropriate security groups, as authorized by management.

Data Storage

All client data contained/stored within the eCMS database resides on either a storage area network (SAN) or on the direct attached storage of the IBM iSeries server; both of which are owned by CGC and managed by the ICS team.

Database(s)

Overview

The eCMS application and supporting tools, as developed and hosted by CGC, are dependent on a DB2 database, hosted on each client's iSeries server instance, exclusively. Database design, implementation, and maintenance is controlled internally by CGC. Clients do not have the ability to make changes to the database structure; although, they may access the data for reporting purposes.

Database Instances

CGC has established separate database instances for quality assurance, user acceptance testing, and production processing, on one or more separate servers within the CGC corporate network. Client servers are used for production purposes only. All database changes are tested before they are promoted to the CGC "production level," which is defined as the level at which it is authorized for deployment.

Database Access

Overall responsibility for ensuring logical access, including database access, is restricted to authorized individuals within the client organization is the responsibility of the client organization.

Access to client data within the application is controlled by the (iSeries) operating system access control list, which is unique to each client as each client has a dedicated server instance; and, such access requires the entry of a unique username and password.

Individuals within CGC that have the responsibility for system and database administration utilize a dedicated CGC account that is enabled via a technical service request with a limited windows for access, and the account is disabled automatically every night; except in the rare circumstance where the operating system administrator account must be used to effect repairs.

Database Auditing & Logging

Database journaling, auditing, and logging are enabled; including access logging for administrator accounts. Activity logs are available for inspection and review to support research and audit activities.

People

The personnel involved in the operation and use of a system (developers, operators, users, and managers)

CGC Employees

CGC's Management has established an overall framework for planning, directing, managing, and controlling operations specific to hosting services and promotes operational independence from other functions within the organization. Operations specific to hosting services are under the direction of the President; and, ultimately, the parent company, JDM Technology Group (JDM).

Management Team

The organization structure and reporting hierarchy of CGC has been established to support its strategic objectives and enforce appropriate segregation of duties. Key management roles relating to hosting services include:

Business Function	Responsibility	Reporting Relationship
President	Responsible for Sales & Operations; including Software Development, Professional & Technical Services, and Application Support. Exercises ultimate oversight of Information Security obligations and policies.	JDM
Controller	Responsible for Accounting, Human Resources, and Company Administration	President
Director – Application Development	Responsible for the software developed by Computer Guidance as part of our ERP solution	President
Manager – Professional Services	Responsible for oversight of CGC's consulting services, client training, and implementation program for customers	President
Director of Business Intelligence & Emerging Technologies	Responsible for analytical reporting and new technology evaluations / roadmaps	President
Director, Infrastructure & Cloud Services	Responsible for the company network, network security, technical and computer support services	President
Manager – Application Support	Responsible for customer support, software application support, and the help desk	President
Manager – Software Delivery	Responsible for the quality of software delivered to clients.	President

CGC has a formal management information and reporting system that enables management to monitor key control and performance measurements. The organization emphasizes integrity and ethical values of all CGC personnel; as well as the importance of maintaining sound internal controls.

Computer Guidance is a wholly owned subsidiary of JDM Technology Group, a private company. JDM allows each company to operate as an autonomous business units, aligning business processes, staff expertise and oversight activities to match the business units individual needs. JDM has not established a board of directors based oversight group.

Services Management

The in-house service desk function is staffed 5 AM to 5 PM Arizona time, Monday through Friday, to receive customer and employee issues related to the SaaS environment. Outside of these hours, customers can send an email to: afterhourssupport@computerguidance.com which is displayed on the CGC website. This email is routed to all managers and key technical staff for review, response, and/or entry into the incident system.

Incident tickets are initiated when a hosting services customer creates an 'incident' using the online portal or CGC staff deem an issue is of significance to be deemed an incident. Service desk staff review the reported information, prioritize the incident, and assign the incident to the appropriate department/personnel.

Customers can check the status of incidents directly; and customers are updated via email as the incident is completed. Incidents that are classified as "support mode" are defined as those which cannot be resolved within a specific time period, as established by management. Such Support Mode Incidents are escalated to the Application Support team or the ICS team, as applicable. For purposes of confidentiality, each ticket is not only assigned a unique number, but also linked to a customer account. These may only be viewed CGC and by the customer.

Either the service desk staff or development team are responsible for updating the status and documenting the resolution of incident tickets. Customers are able to review the status and/or resolution, at any time. If an RPG code change or update is required, a separate incident will be created in the Change Management System (Aldon) and linked to the original incident.

Contracted Personnel

Except for its agreements with the hosted data centers, as described elsewhere in this document, CGC does not currently contract with independent personnel or companies to support the SaaS infrastructure, software, hardware, or environment.

Vendor Personnel

CGC does not directly engage vendor personnel to support the hosting services environment. However, as part of the contract with the subservice organization, Tech Data, the Hosting Partner may provide individuals to assist with physically moving equipment located at the data center.

Procedures

The automated and manual procedures involved in the operation of a system

Systems Security

Management has established and communicated appropriate policies, procedures, systems, and processes related to information systems security to employees, clients, and external business partners which restrict logical access to CGC systems that include the eCMS SaaS environment. Procedures are reviewed annually by the ICS team, with changes presented to senior management for approval, when appropriate. These policies and procedures cover the following key elements of systems security:

- Business Impact / Risk Assessments, which drive proposed security approaches;
- Selection, documentation, and implementation of security controls related to:
  - Network and security devices;
  - Servers and workstations;
  - Source code, application servers, and databases;
  - Facilities and physical access;
- Systems security configuration, patching, and monitoring;
- Managing systems user account access; and,
- Security protocols.

Systems Availability

Management has developed and communicated relevant procedures over system availability to employees, clients, and external business partners to ensure CGC systems are available when needed; especially including the eCMS application. Relevant procedures are reviewed continuously by the ICS team, at a minimum frequency of once per month. Significant risks are communicated to all employees, clients, and business partners. These procedures cover the following key elements of systems availability:

- Technical infrastructure documentation;
- Any Impact Assessments that result from the unavailability of systems;
- Technical infrastructure patch management and change control;
- Server performance, disk capacity, systems maintenance; and,
- Data storage, backup, recovery, and business continuity.

Data Confidentiality

Management has developed and communicated relevant procedures governing the confidentiality of data to employees, clients, and external business partners in order to protect data in a manner consistent with CGC policies, contracts, and other relevant legal obligations. Procedures are reviewed annually by CGC management with changes submitted for review, and approval, by the President. These procedures cover the following key elements of data confidentiality:

- Contractual agreements with clients and/or vendors;
- Nondisclosure and confidentiality agreements;
- User account administration;
- Data encryption (for data in transit over the pubic internet).

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

Control Environment

Management Philosophy

CGC has established a business environment and culture that reflects the philosophy of our Executive Management. That philosophy prioritizes the critical importance of effective controls that are specific to the availability and security of the systems that support hosting services, as well as the protection of confidential data that is either in electronic format or on printed materials.

Security Management

Management's philosophy is further emphasized by the President, who has overall responsibility for information security within CGC. The President is responsible for reviewing and approving CGC's policies over security and availability of systems including the protection of confidential data. These policy statements are made available to employees on a CGC internal network site, with department managers being responsible for implementing the appropriate administrative, technical, and physical controls to meet (or exceed) the applicable criteria for the selected Trust Service Principles. The procedures and control expectations are communicated to employees as principles which form the basis for conducting business operations and protecting the overarching system.

Policy Statements, Standards, and Procedures

Organizational values, behavioral standards, and operational guidelines are communicated to personnel by management through various methods, including by way of the Security Policy and Employee Handbook, for topics including, but not limited to:

- General conduct;
- Physical security;
- Data security;
- Email and internet usage;
- Use of company technology assets.

In addition, structured procedures have been established for directing and controlling operations, including the Hosting Partner environment.

Personnel Administration

Overview

Management of CGC has a strong commitment to recruit, develop, and retain competent personnel to execute the business plan, and to achieve our business and control objectives; including employee roles that are responsible for the SaaS environment eCMS application. Most staff positions are filled through general solicitation or employee referrals. Management positions are commonly filled through internal hiring procedures which recognize growth in employee experience, skills and competence. The system also utilizes referrals, which help to establish the presence and quality of leadership traits. Hiring practices are designed to ensure that new employees are qualified to meet their job responsibilities and that they can competently, confidently, and diligently contribute to the successful operation of their respective teams and the company overall.

Position Description

Position descriptions are established and maintained for all positions within CGC that are responsible for the eCMS application in a hosted environment. Each position description identifies key areas of accountability and reporting structure, along with education, experience, and skill requirements. Position descriptions are developed and maintained by the Controller, with assistance from the ICS team, and are used as a basis for establishing access permissions relating to facilities and the Hosted Partner environment.

Candidate Screening

Prospective employees that are extended offers of employment with CGC are required to sign a Computer Guidance Pre-Hire Agreement that includes verbiage related to data security and a noncompetition agreement. Candidates are also subject to a background check at the discretion of CGC management.

New Hire Process

Employee Handbook & Acknowledgements

The Employee Handbook is discussed and reviewed with employees as part of the new hire orientation process. The Handbook is available via the company intranet site to all employees.

User Account Request(s)

The Controller is responsible for notifying the ICS team when a user account needs to be established for a new employee. The Technical Service Manager determines if the individual is authorized to access the hosted environment based on business need.

New Employee Training

New hire training commences upon the completion of the orientation process that is facilitated by the CGC Expo, which is an event that is scheduled and sponsored by the Controller as needed, based on hiring activity. In addition to initial training, staff are provided with ongoing training and guidance by their respective department managers and also by training by department personnel, commonly addressing specific requirements of new or recently changed customers, software, hardware, and/or applications requirements.

Employee Separation

The Controller has established an employee separation form that includes a checklist to determine compliance with company policies related to both voluntary resignations and involuntary terminations. The Controller completes the checklist segment of the form as part of the employee separation process. Notification of the employee separation is immediately sent to ICS team via electronic mail.

The ICS team is responsible for disabling/deleting user accounts, user data, and disabling physical access. The Controller is responsible for retrieving any company-owned assets, including technological assets, and/or physical access devices.

Physical Security and Environmental Controls

Physical Security – CGC Headquarters

Systems, tools, and activities employed by CGC have been implemented to provide reasonable assurance that physical access to facilities is limited to appropriate and authorized personnel, as follows:

Physical Security Administration

The building management is responsible for the administration of physical access controls at the office space in Scottsdale, AZ.

Door Access Readers

The building management has installed access readers for employee entrances. Access is administered by building management, the Controller, and the ICS Director.

Lost, stolen, or unreturned access cards result in building management being notified and any affected access cards are disabled. Upon employee separation, access cards are returned, disabled, and placed in a repository for future use.

Key Control and Locked Doors

CGC employees are not issued any keys to the office space. All access is controlled through proximity cards, which are managed by the building management. The doors to the CGC offices operates on a timer that prevents any access outside business hours.

Video Surveillance

A video camera monitors the lobby, including the lobby door. There is an additional Security camera in the elevator. A security guard patrols the site.

eCMS SaaS Hosting Partner data center physical security controls

Physical security controls within Hosting Partner data centers are the responsibility of the Hosting Partner.

Environmental Controls

CGC Headquarters

Smoke & Fire

Smoke detectors are installed and monitored by building management staff. These detectors are tested annually by the building management. The building's fire suppression system consists of sprinklers, which are maintained by building management.

HVAC, Water, Electricity, and Telecommunications

Environmental Control over heating, ventilation, air conditioning, is the responsibility of building management.

Ensuring the availability of utilities to the premises, such as water, electricity, and telecommunications is the responsibility of building management. Any issue encountered by CGC with regard to the availability or functionality of these services and/or conditions is reported to building management upon detection by staff.

eCMS SaaS Hosting Partner data center environmental controls

Environmental controls within Hosting Partner data centers are the responsibility of the Hosting Partner.

<u>Change Management</u>

eCMS Application and Database Change Management

Overview

Any eCMS application and/or database changes or updates within the SaaS (Hosting Partner) environment require approval from the Manager of Software Delivery prior to promoting the change into the SaaS production environment. Changes are recorded, and tracked, within the CGC Customer Service Program (CSP) incident and ticketing system; and, in the case of application changes, the code management system in Aldon. Changes to applications and databases in the SaaS production environment are only performed by authorized software delivery personnel and are tracked by the Manager of Software Delivery.

Incident(s) / Change Request(s)

Incident tickets or change requests that are submitted by client-user organizations or authorized CGC staff related to the eCMS application are reviewed by a CGC business analyst to determine whether any change has an appropriate business justification, and whether such change requires a programming change to source code. If a programming change is necessary, then the incident in CSP is given a Task ID Number, and is assigned to a developer for tracking purposes by the Director of Application Development.

Program Change(s)

In addition to developer assignment, the Task ID is required within the code management system and is required for the developer to make changes to source code. The assigned developer is responsible for checking out the necessary program objects associated with the specified Task ID. Programs are modified, and tested, as appropriate for the change.

Testing Environments

CGC maintains four unique environments for the development and support of the eCMS application; including (i) development, (ii) quality assurance (QA), (iii) install testing (packaging of compiled code), and (iv) application support (which utilizes the final production version). All environments are maintained within the CGC internal corporate network and code management is automated using Aldon.

Once user and/or developer testing is complete, the developer promotes the changed programs to the Integration environment. The QA team performed testing of all code changes prior to moving code changes to the next phase. After completion of the QA testing, a promotion request is completed to move source code changes to the install/packaging team in order to compile source code, and dependencies, into packages for install into production environments. Finally, the validated packages are moved to CGC's internal production environment which is used by the application support team.

The program development and change process is tracked and monitored by the Manager of Software Delivery.

eCMS SaaS Environment Changes

Planned Changes

All planned changes within the SaaS environment are initiated by the Software Delivery team, after approval by customers, and require final approval by the Manager of Software Delivery.

Nonscheduled (Emergency) Changes

Emergency changes within the SaaS environment follow the same process as planned changes.

Infrastructure Change Management

All infrastructure changes are initiated, authorized, and tracked in the incident management system. Implementation of infrastructure changes is based on assignment of the incident to an individual or team based on the requirements of the incident. Management monitors all new and open incidents. Additionally, closed incidents not approved by customer can be reopened by the customer.

CGC Internal Corporate Network

Planned and emergency changes to the CGC internal corporate network are performed by the ICS team.

eCMS SaaS Hosting Partner Network

Planned and emergency changes to the eCMS SaaS Hosting Partner network are the responsibility of the Hosting Partner.

Servers

All changes to servers within the SaaS Hosting Partner environment require approval from the Director of ICS, or an authorized ICS team member, prior to moving a change into the production environment. Changes to servers in the SaaS Hosting Partner environment are the responsibility of the ICS team.

<u>Technical Infrastructure Monitoring</u>

Network Availability and Security-Related Events

All servers, switches, and routers are monitored by a centralized event monitoring solution - Nagios. This tool aggregates information from all applicable devices and allows for real time monitoring via customizable dashboard; as well as supporting e-mail alerts based on rule sets, and the creation of monitoring reports. The monitoring tool also maintains a log of historical events.

Server Capacity and Performance

The ICS team utilizes Nagios to monitor server capacity and performance as part of strategic and tactical capacity, as well as performance planning activities. Immediate issues are addressed by creating an incident in the CSP system. Long term risks are addressed by management as part of future planning.

Capacity and performance monitoring is configured for the following:

- Server, database, and application availability;
- Services status;
- Disk space: total, used, and available;
- CPU performance and usage;
- Application response time

Specific server events will generate e-mail alerts which are send to ICS and customer service team members.

Data Backup and Recovery

Overview

CGC replicates client databases asynchronously between the two data centers in real-time mode between iSeries servers in support availability of data for clients in the SaaS environment. Database backups are performed using IBM tools and are backup up (disk-to-disk) to a storage server in the SaaS network.

Schedule

Disk-to-disk backups are performed on a daily, weekly, and monthly basis at each data center. The, weekly, and monthly backups are replicated between the two data centers, daily or weekly, to maintain off-site copies of data backups. Backup tapes were no longer taken to an off-site location.

Backup Validation

Backups are tested annually to determine the recoverability of data for disaster recovery purposes. In all instances, CGC is responsible for monitoring the success/failure of the data backup processes.

System(s) Account Management

Overview

Access to all networks, and primary software applications, is role-based as established by management; users have unique login credentials tied to role security. Operationally, key production systems are supported by business analysts with advanced knowledge and training on the eCMS software and complementary applications. Networks are secured at the perimeter by firewalls with intrusion prevention and detection.

Logical Access – CGC Network Authentication

Authentication

User Name

Access to the CGC network requires the user to enter a unique username and strong password.

Password Controls

Password controls are technically enforced for length, change frequency, and history. User accounts are locked after a specified number of unsuccessful login attempts and remain locked for a predetermined period of time or until reset by ICS staff.

Account Password Reset Procedures

Requests to reset user account passwords can only be submitted to, and performed by, the ICS team. Password resets are performed by ICS staff and require the user to change the password at their next login.

User Account Administration

CGC user permissions are based on the defined responsibilities of the employee role and managed by security group membership in Active Directory. CGC has established structured procedures for adding, changing, and deleting user accounts. In addition, an employee register is maintained that identifies systems and applications each CGC user is authorized to access.

New Hires

The Controller is responsible for completing a *New User Request Form* that identifies employee access and authorization to network resources and the SaaS environment. The completed form is then forwarded to the ICS team via email for setup. The user account is not activated prior to the employee's first day of employment. User accounts for new employees are assigned with a unique initial password that must be changed by the employee at their first login.

Terminations

The Controller is responsible for completing the *Employee Separation / Termination Form* that identifies any/all employees that are leaving the organization, whether voluntarily or involuntarily. Notification of termination is forwarded to the ICS team via email for user account processing. This process includes disabling and/or deleting user accounts that access the network or hosted systems environment. Situations that require immediate dismissal of staff may be communicated verbally to the ICS Director; and, followed by appropriate written documentation.

Periodic Validation

As a secondary level of control, a validation process is performed on a semi-annual basis by the ICS Director to determine whether (and to ensure that) all user accounts for terminated employees have been disabled or deleted.

Logical Access – SaaS environment

Overview

Access to the SaaS environment by CGC staff is controlled by a firewall which only allows access by way of an IPsec VPN, using Active Directory authentication. Once a CGC employee has access through the firewall, additional user-specific, role restricted credentials are needed to access any of the servers in the SaaS environment. The ICS Director is responsible for monitoring the CGC firewall, and the server operating system accounts in the SaaS environment.

Client eCMS Application Authentication

Access to the eCMS applications in the SaaS environment requires a named user account and password to access the client-specific server.

Client eCMS Account Administration

Server and eCMS account administration is the responsibility of the customer within their SaaS environment. Initial client-user accounts for the SaaS environment are originally setup based on individual client specifications. Each client is provided a user account that has appropriate privileges which authorize that user to create, modify, and/or delete additional user accounts, on an ongoing basis. In addition, at least one CGC user account ("cgcowner") is created on the client system for support purposes, as authorized and described in the customer agreement. Application password complexity rules are defined by the client.

Risk Assessment Process

Risk assessment is the process of identifying and analyzing relevant risks which would prevent CGC from achieving its operational, financial, and compliance objectives. CGC performs risk assessments on an ongoing basis to assess and manage any risk(s) that could affect the organization's ability to provide reliable services to its clients, with an emphasis on data security and data integrity. For any significant risks identified, management is responsible for implementing appropriate measures to monitor, remediate and/or manage these risks (e.g., implementing/revising control procedures, conducting specific audit projects, designing and delivering issue-specific training).

In support of business operations, CGC carries the following insurance which transfer some or all the risk of unplanned events to a third-party insurer; including, but not necessarily limited to: Professional Liability, General Liability, Workers Compensation, Directors and Officers Insurance, Umbrella Liability, Crime and Fidelity, and Casualty.

Information and Communication Systems

Internal (Employees)

Pertinent information must be identified, captured, and communicated in a form, manner, and timeframe that enables employees to carry out their assigned responsibilities effectively and efficiently. This information is usually distributed to the employees in the form of policy statements, meetings, training sessions, intranet postings, emails, and paper documents.

External (Customers)

CGC provides several options for incoming and outgoing client communication including:

- U.S. Mail
- Electronic Mail (E-mail)
- Telephone / Facsimile
- Self-service web portal

The self-service web portal, telephone, and email comprise a majority of the communications. Clients are directed to use the customer support website to report incidents, usually by using the self-service web portal. It is the responsibility of the Service Desk to direct the issue to the appropriate resource for resolution.

Monitoring of Controls

Monitoring is the process that assesses the adequacy of internal control design and compliance with the design over a period of time to determine effectiveness. CGC management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. To assist in this monitoring, CGC has developed comprehensive and summary reports that facilitate the monitoring of its services and related controls. Results of internal control monitoring may require management to makes adjustments to controls to determine availability and security of systems.

Subservice Organizations (External Business Partners)

Overview

CGC has a contract with Tech Data Corporation (NASDAQ: TECD) to provide data center services to host both the internal corporate network and the SaaS eCMS environment on network equipment and servers owned and managed by CGC.

Tech Data Corporation is a Fortune 500 global distributor of technology products, services, and solutions, headquartered in Clearwater, Florida.

Responsibility

CGC has established and implemented policies that govern the administration of external business partners, as outlined in the Operations Policy and Procedure manual related to vendors. The Controller is responsible for maintaining a list of vendors used by CGC; with each record including the company name(s), contact(s), service(s), and specific contract terms and information. Responsibility for each individual vendor relationship is assigned to one or more individuals within CGC, based on the vendor type.

Contractual Agreement(s)

Services obtained from third-party business partners, such as those related to hosting services, are supported by one or more written agreement that outlines the specific responsibilities of each partner; including the nondisclosure of confidential information.

Exclusions

Controls that are the responsibility of Tech Data Managed Technologies, and its subservice organizations, have been excluded from the scope of this engagement. Tech Data Managed Technologies and its subservice organization have their own assurance reports available for review.

Complementary User-Entity Controls

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

Criteria		Customer User Entity Control(s)
All	Data Integrity	User entities are responsible for maintaining integrity of data entered into CGC's software solutions.
		User entities are responsible for performing automated nightly functions including (but not limited to): • Nightly job processing • Creating Data Files for Transmission • Building daily work queues • Monitoring automated jobs for errors and completeness.
		User entities are responsible for reviewing and verifying any activity performed by CGC users by viewing their QHST, Job Accounting Journal, System Messages, and eCMS logs.

Criteria		Customer User Entity Control(s)
CC-5.1	Logical Access	User entities are responsible for user account administration to the SaaS environment within their organization. This includes controlling access and access permissions to objects and menu security within their organization.
		User entities are responsible for establishing, monitoring, and enforcing password complexity requirements for all organization-issued accounts.
		User entities are responsible for maintaining the CGC provided User Account that is created as part of the initial installation/implementation.
		By Default, the account is disabled; and it is only enabled through the 'CGCOWNER' request process. It is automatically disabled each evening.
		User entities are responsible for securing and maintaining firewall and VPN configurations at each user entity's end-point
C-1.8	Data Disposal	User entities are responsible for purging their organization's data.

Complementary Subservice-Entity Controls

CGC has established relationships with the following subservice organization(s) in support of service(s) delivery. The following illustrates the vendor that is providing the service and a description of the control(s) that are the responsibility of the subservice organization by control objective.

Criteria		Control(s) Responsibility
Tech Data – Hosting Data Center		
CC-6.4	Physical Security	• Physical Security to Hosting Facility
CC-7.3	System Anomalies	• Communicate CGC if an actual or potential network security breach is detected or identified
A-1.2	Data Center Environmental Controls	• Data Center Environmental Controls o Electrical Generator / UPS o Temperature Control o Humidity Control o Public Internet Connectivity

As previously stated, processes and controls that are the responsibility of subservice organizations are excluded from this report.

IV. Trust Services Category, Criteria, Related Controls, and CliftonLarsonAllen LLC's Test(s) of Controls and Test(s) Results

Overview

The identified control activities are solely the responsibility of the management of Computer Guidance Corporation. The control activities listed in the first column "*Control Activity Specified by CGC"* have been identified by Computer Guidance Corporation and are based on the accompanying description of relevant controls provided by the organization.

CliftonLarsonAllen assessed control descriptions for accuracy and suitability of design to meet the selected trust services criteria and performed tests of controls to determine compliance with design for effectiveness.

Applicable Trust Services Criteria Relevant to Security

The trust services criteria relevant to security (CC series) address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of

i. *information* during its collection or creation, use, processing, transmission, and storage and
ii. *systems* that use electronic information to process, transmit or transfer, and store information to enable the achievement of CGC's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Applicable Trust Services Criteria Relevant to Availability

The trust services criteria relevant to availability (A series) address the available for operations and use of information and systems to meet the entity's objectives.

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

Applicable Trust Services Criteria Relevant to Confidentiality

The trust services criteria relevant to confidentiality (C series) address the need for information designated as confidential be protected to meet the entity's objectives.

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

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

Tests of Control(s) Operating Effectiveness

Our tests of operating effectiveness of controls included such tests as we considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from October 1, 2018 to December 31, 2019. Our tests of operating effectiveness of controls were designed to cover the period from October 1, 2018 to December 31, 2019, for each of the controls listed in section III, which are designed to achieve the specified control objectives. In selecting particular tests of the operating effectiveness of controls, we considered (a) the nature of the controls being tested, (b) the types and competence of available evidential matter, and (c) the control objectives to be achieved.

Tests performed of the operating effectiveness of controls detailed in section III are described below:

Test Type	Description
Inquiry	Made inquiries of appropriate CGC personnel to obtain information or corroborating evidence of the control.
Observation	Observed that a specific control exists, is appropriate and operating as intended.
Inspection	Inspected documents and reports indicating performance of the control. This includes, among other things: • Inspection of reconciliations and management reports. • Examining documents or records of performance such as the existence of initials or signatures.
Re-Performance	Re-performed the control or processing application of the control to ensure the accuracy of their operation.

CONTROL ENVIRONMENT– Common Criteria Related to Control Environment
Number **CC-1.1**
The entity demonstrates a commitment to integrity and ethical values.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-1.1.1	Organizational values and behavioral standards are communicated to all personnel through various policy statements. Specific policy statements are identified below: • Employee Handbook • Information Security Policy • Internet Web and Email Policy	Inspected the IT Security Policies, Internet Web and Email Policy, and Employee Handbook to determine that policy statements outlined the organizational values and behavioral standards.	No Exceptions Noted
CC-1.1.2	All new employees are required review and sign policy, acknowledging their acceptance of the policies. This is performed via the employee new hire onboarding.	Inspected signed acknowledgements for the new hires during the period to determine that an employment agreement, acknowledgment of the IT Security Policy, and acknowledgement of the Employee Handbook were signed.	No Exceptions Noted
CC-1.1.3	Professional Services Agreements are used when contractors are engaged to perform services for CGC. The agreements include non-disclosure verbiage	Inspected the Professional Services Agreement to determine the agreement was designed when contractors were engaged and that agreement included nondisclosure verbiage. Inquired of management to determine whether any contractors were engaged during the period and required the use of the Professional Services Agreement.	No Exceptions Noted Control activity did not occur during the reporting period. As a result, no testing performed.

CONTROL ENVIRONMENT– Common Criteria Related to Control Environment
Number **CC-1.2**
The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
N/A	Not relevant to Computer Guidance Corporation due to size of the organization and the organization structure.	N/A	N/A

CONTROL ENVIRONMENT– Common Criteria Related to Control Environment
Number **CC-1.3**
Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-1.3.1	The organizational structure of CGC is documented and provides the overall framework for planning, directing, and controlling operations for hosting services.	Inspected the Organization Chart to determine that the chart was documented and provided the overall framework for planning, directing, and controlling operations for hosting services.	No Exceptions Noted
CC-1.3.2	CGC has defined and documented employee responsibilities, via formal Job Descriptions. Segregation of duties are detailed in the organizational chart and job descriptions	Inspected job descriptions for the new hires during the period to determine that content provided a level of detail to establish responsibilities. Inspected the Organization Chart to determine that the chart provided details regarding segregation of duties.	No Exceptions Noted
CC-1.3.3	Professional Services Agreements are used when contractors are engaged to perform services for CGC. The agreements include non-disclosure verbiage	Inspected the Professional Services Agreement to determine the agreement was designed when contractors were engaged and that agreement included nondisclosure verbiage. Inquired of management to determine whether any contractors were engaged during the period and required the use of the Professional Services Agreement.	No Exceptions Noted Control activity did not occur during the reporting period. As a result, no testing performed.

CONTROL ENVIRONMENT– Common Criteria Related to Control Environment
Number **CC-1.4**
The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-1.4.1	HR performs hiring procedures that include a comprehensive screening for candidates for key positions and consideration of whether the candidate's credentials are in alignment with the position.	Inspected new hire documentation for the new hires during the period to determine that candidate was screened using tools designed to determine aptitude and fitness.	No Exceptions Noted
CC-1.4.2	Criminal background checks are performed by HR after an offer of employment has been extended. The hiring of individuals is contingent upon the successful completion of a background check.	Inspected background check documentation for the new hires during the period to determine that a background check was performed.	No Exceptions Noted
CC-1.4.3	CGC provides the following benefits to its employees: • Life Insurance (Company paid for up to 1x your annual salary) • Short Term Disability (Company paid) • Long Term Disability (Company Paid) • 401k Match (3% on up to 6%) • Health Insurance (PPO's and HDHP) (partial co paid depending on tenure/manager; managers and 10+ get HDHP at no cost to EE) • H.S.A for the HDHP plan (Company contributes depending on how enrolled) • Dental Insurance (partial co paid depending on tenure/manager) • Vision Insurance (100% EE paid) • Work from home to provide work/home balance • F.S.A • PTO o 0-5 years are 15 days/year; 5 sick and 2 optional holidays o 5-10 years get 20 days/year; 5 sick and 2 optional holidays o 10+ years get 25 days/year; 5 sick and 2 optional holidays	Inspected the CGC Employee Handbook for descriptions of benefits provided to employees to determine that CGC provided the items listed.	No Exceptions Noted

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-1.4.4	Professional Services Agreements are used when contractors are engaged to perform services for CGC. The agreements include non-disclosure verbiage	Inspected the Professional Services Agreement to determine the agreement was designed when contractors were engaged and that agreement included nondisclosure verbiage.	No Exceptions Noted
		Inquired of management to determine whether any contractors were engaged during the period and required the use of the Professional Services Agreement.	Control activity did not occur during the reporting period. As a result, no testing performed.
CC-1.4.5	CGC utilizes the intranet as a communications tool that is accessible by internal users. Specific information includes but is not limited to the following: • Company policies • Comprehensive training materials • Organizational structure documentation	Inspected a screenshot of CGC's intranet to determine that documents were available to internal users including: • Company policies • Comprehensive training materials • Organizational structure documentation	No Exceptions Noted
CC-1.4.6	CGC produces a quarterly employee newsletter to communicate ongoing, company wide communications	Inspected quarterly newsletters for a selection of quarters during the reporting period to determine that communication to employees was sent.	No Exceptions Noted

CONTROL ENVIRONMENT– Common Criteria Related to Control Environment
Number **CC-1.5**
The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-1.5.1	The organization provides weekly status reports from the departments to the President where the departments document performance, standards and procedural activities for the last week.	Inspected the weekly status reports to the President for a selection of weeks during the reporting period to determine that the departments reported on performance, standards and procedural activities for the last week.	No Exceptions Noted

COMMUNICATION AND INFORMATION– Common Criteria Related to Communication and Information
Number **CC-2.1**
The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-2.1.1	The organization provides weekly status reports from the departments to the President where the departments document performance, standards and procedural activities for the last week.	Inspected the weekly status reports to the President for a selection of weeks during the reporting period to determine that the departments reported on performance, standards and procedural activities for the last week.	No Exceptions Noted
CC-2.1.2	Summary and weekly dashboards are directly imported from the ticket tracking system via established queries.	Inspected the weekly summary and dashboards reports for a selection of weeks during the reporting period to determine that results were imported based on established queries.	No Exceptions Noted
CC-2.1.3	CGC collects performance, event and availability data in real time for all productions systems using the following: * Windows Hyper-V PerfMon * Nagios Logs * Syslog Logs	Inspected system logging screenshots for the monitoring tools utilized by CGC to determine that activity was logged and available for review.	No Exceptions Noted
CC-2.1.4	CGC uses a tool to capture real time data about disk space utilization and has established criteria to alert of the criteria being reached.	Inspected a screenshot of the monitoring system dashboard to determine that there was real time data available when performance thresholds had been exceeded. Inspected alert messages from the monitoring system to determine that alerts were produced after a threshold was exceeded.	No Exceptions Noted
CC-2.1.5	CGC uses vendor tools (Nagios and Backup) to automated alert CGC about established criteria and events	Inspected alert messages from the Nagios monitoring system to determine that alerts were produced after a threshold was exceeded. Inspected alert messages from the Backup system to determine that alerts were produced to alert CGC regarding established criteria and events.	No Exceptions Noted

COMMUNICATION AND INFORMATION– Common Criteria Related to Communication and Information
Number **CC-2.2**
The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-2.2.1	CGC utilizes the intranet as a communications tool that is accessible by internal users. Specific information includes but is not limited to the following: • Company policies • Comprehensive training materials • Organizational structure documentation	Inspected a screenshot of CGC's intranet to determine that documents were available to internal users including: • Company policies • Comprehensive training materials • Organizational structure documentation	No Exceptions Noted
CC-2.2.2	CGC produces a quarterly employee newsletter to communicate ongoing, companywide communications.	Inspected quarterly newsletters for a selection of quarters during the reporting period to determine that communication to employees was sent.	No Exceptions Noted
CC-2.2.3	CGC has defined and documented employee responsibilities, via formal Job Descriptions. Segregation of duties are detailed in the organizational chart and job descriptions	Inspected job descriptions for the new hires during the period to determine that content provided a level of detail to establish responsibilities. Inspected the Organization Chart to determine that the chart provided details regarding segregation of duties.	No Exceptions Noted
CC-2.2.4	CGC emails a monthly security awareness newsletter to improve security knowledge and awareness among the CGC's employees.	Inspected monthly security awareness newsletters for a selection of months during the reporting period to determine that GCG emails CGC's employees about security knowledge and awareness.	No Exceptions Noted
CC-2.2.5	CGC has established contractual and service-level agreements with customers that describe services and boundaries of the system.	Inspected the contracts and service-level agreements for a selection of new clients during the period that are using the eCMS Hosted Environment to determine that verbiage within the agreement included a description of services and the boundaries of the system.	No Exceptions Noted

COMMUNICATION AND INFORMATION– Common Criteria Related to Communication and Information

Number
CC-2.3

The entity communicates with external parties regarding matters affecting the functioning of internal control.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-2.3.1	CGC has established contractual and service-level agreements with customers that describe services and boundaries of the system.	Inspected the contracts and service-level agreements for a selection of new clients during the period that are using the eCMS Hosted Environment to determine that verbiage within the agreement included a description of services and the boundaries of the system.	No Exceptions Noted
CC-2.3.2	CGC notifies the client of significant changes that directly impact the security, availability, and confidentiality commitments as required per client agreements. CGC communicates updates and changes to external users via email.	Inspected copies of ad hoc emails provided to clients to determine that CGC does communicate significant changes that impact security, availability and confidentiality.	No Exceptions Noted
CC-2.3.3	CGC Marketing provides weekly tips and tricks to external parties about the services provided.	Inspected weekly CGC Marketing Tips and Tricks for a selection of weeks during the reporting period to determine that external parties were provided with them.	No Exceptions Noted
CC-2.3.4	GCG Marketing provides quarterly newsletters to external parties about changes and updates related to the services provided.	Inspected quarterly newsletters for a selection of quarters during the reporting period to determine that communication to external parties was sent.	No Exceptions Noted

RISK ASSESSMENT– Common Criteria Related to Risk Assessment
Number **CC-3.1**
The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-3.1.1	CGC management performs a risk assessment annually. The risk assessment is based on the objectives established by management.	Inspected the annual risk assessment to determine that the risk assessment was performed. Inspected the risk assessment to determine the risk assessment was based on the objectives established by management.	No Exceptions Noted
CC-3.1.2	Managers document and communicate operational metric data for analysis to all level of the organization on a weekly basis.	Inspected weekly reports for a selection of weeks in the period to determine that metrics were documented and communicated throughout the organization. Inspected the outlook calendar for the CIO to determine that management had regularly scheduled weekly meetings to review the eCMS environment and address any known risks or threats.	No Exceptions Noted

RISK ASSESSMENT– Common Criteria Related to Risk Assessment

Number
CC-3.2

The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-3.2.1	Managers document and communicate operational metric data for analysis to all level of the organization on a weekly basis.	Inspected weekly reports for a selection of weeks in the period to determine that metrics were documented and communicated throughout the organization. Inspected the outlook calendar for the CIO to determine that management had regularly scheduled weekly meetings to review the eCMS environment and address any known risks or threats.	No Exceptions Noted
CC-3.2.2	Management assess and responds to security risks and potential fraud on an ongoing basis through regular meetings, reviewing and acting upon security event logs and conducting the annual risk assessment.	Inspected weekly reports for a selection of weeks in the period to determine that management was reviewing and acting upon security event logs and potential fraud. Inspected the outlook calendar for the CIO to determine that management had regularly scheduled weekly meetings to review the eCMS environment and address any known risks or threats. Inspected the annual risk assessment to determine that management was assessing and responding to security risks.	No Exceptions Noted

RISK ASSESSMENT– Common Criteria Related to Risk Assessment
Number **CC-3.3**
The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-3.3.1	CGC employees are instructed that any breach or suspected breach of the security of the CGC Internal Corporate Environment that impacts data in electronic format should contact CGC management to determine next steps. Handling of the incident is outlined in the CGC IT Security Policy and Protocols.	Inspected the IT Security Policy and Security Protocol Documents to determine that they described procedures on how to notify appropriate individuals of actual or suspected breaches. Inquired management to determine that no breach or suspected breach occurred during the reporting period.	No Exceptions Noted
CC-3.3.2	ICS staff is responsible for monitoring and managing system alerts that may impact system security and respond appropriately to minimize any negative impact.	Inspected the monitoring system and alerts to determine that ICS staff was responsible for monitoring and managing system alerts.	No Exceptions Noted
CC-3.3.3	CGC management is responsible for notifying clients and/or external business partners of confirmed security breaches based on agreed upon terms and conditions	Inspected the agreements for a sample of new clients in the reporting period to determine that CGC management was responsible for notifying clients of confirmed security breaches. Inspected the IT Security Protocol to determine that management was responsible for notifying clients and/or external business partners for all confirmed security breaches. Inquired management to determine that no breach or suspected breach occurred during the reporting period.	No Exceptions Noted
CC-3.3.4	CGC has an established Security Awareness program that includes monthly Security Awareness Newsletters. CGC has also defined policies to mitigate this risk.	Inspected Security Awareness Newsletters for a selection of months to determine that the Security Awareness program included the newsletters. Inspected CGC IT Security Policy, Internet Web Policy and Email Policy to determine that policies addressed Security Awareness.	No Exceptions Noted

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-3.3.5	CGC has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.	Inspected the CGC Employee Handbook to determine that policies regarding unauthorized use of company equipment and systems was addressed. Inspected the facility access list and the active directory listing for a selection of terminated employees during the period to determine that access to the facility and CGC systems was disabled or deleted to protect against unauthorized acquisition, use or disposal of assets.	Exception Noted - The facility access was not disabled or deleted for one of the three employees who terminated employment during the period.

RISK ASSESSMENT– Common Criteria Related to Risk Assessment

Number
CC-3.4

The entity identifies and assesses changes that could significantly impact the system of internal control.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-3.4.1	CGC, through its ongoing an annual risk assessment process, evaluates changes in: a. the regulatory, economic, and physical environment in which CGC operates. b. the business environment, including industry, competitors, regulatory environment, and consumers. c. the potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. d. CGC's systems and changes in the technology environment. e. vendor and business partner relationships.	Inspected the annual risk assessment to determine that the risk assessment was performed and evaluated changes in: a. the regulatory, economic, and physical environment in which CGC operates. b. the business environment, including industry, competitors, regulatory environment, and consumers. c. the potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. d. CGC's systems and changes in the technology environment. e. vendor and business partner relationships.	No Exceptions Noted

MONITORING ACTIVITIES– Common Criteria Related to Monitoring Activities
Number **CC-4.1**
The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-4.1.1	CGC Manager formally review their workload on a weekly basis and analysis is communicated to Senior management and the management team.	Inspected weekly reports for a selection of weeks in the period to determine that workload analysis was communicated.	No Exceptions Noted

MONITORING ACTIVITIES– Common Criteria Related to Monitoring Activities
Number **CC-4.2**
The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-4.2.1	CGC Manager review their incidents on a weekly basis and analysis is communicated to Senior Management for corrective action.	Inspected weekly reports for a selection of weeks in the period to determine that incidents analysis were communicated to senior management for corrective action.	No Exceptions Noted
CC-4.2.2	Management tracks the status of all deficiencies that have been rated as a serious threat to the organization until satisfactorily resolved.	Inspected weekly reports for a selection of weeks in the period to determine that management tracked the status of deficiencies that were rated as serious threats until satisfactorily resolved. Inquired management to determine whether a breach or suspected breach rated as serious threat occurred during the reporting period.	No Exceptions Noted

CONTROL ACTIVITIES– Common Criteria Related to Control Activities

Number
CC-5.1

The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-5.1.1	As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.	Inspected the annual risk assessment to determine that management linked the identified risks to control. Inquired of management to determine whether new controls were identified and implemented.	No Exceptions Noted
CC-5.1.2	CGC employs procedures, system monitoring, communications, documentation and management review to mitigate risk. System monitoring is performed in real-time, communications are performed as needed and documentation is reviewed on an annual basis.	Inspected the IT Security Protocols to determine that management performs reviews and implements controls to mitigate risks. Inspected a screenshot of the monitoring system dashboard to determine that there was real time data available when performance thresholds had been exceeded. Inspected alert messages from the monitoring system to determine that alerts were produced after a threshold was exceeded. Inspected the annual risk assessment to determine that risks noted throughout the year were reviewed on an annual basis.	No Exceptions Noted
CC-5.1.3	CGC segregates responsibilities under lead groups. * Development * Technical Services * Software Delivery / Quality Assurance * Application Support These groups were established on functional, security and general business demands.	Inspected the descriptions of the lead groups to determine that the groups were established based on functional, security, and general business demands.	No Exceptions Noted

CONTROL ACTIVITIES– Common Criteria Related to Control Activities
Number **CC-5.2**
The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-5.2.1	Management developed a list of control activities to manage the security access management risks identified during the annual risk assessment process.	Inspected the wiki list of control activities to determine that controls were used to manage the security access management risks.	No Exceptions Noted
CC-5.2.2	CGC employs procedures, system monitoring, communications, documentation and management review to mitigate risk.	Inspected the IT Security Protocols to determine that management performs reviews and implements controls to mitigate risks. Inspected a screenshot of the monitoring system dashboard to determine that there was real time data available when performance thresholds had been exceeded. Inspected alert messages from the monitoring system to determine that alerts were produced after a threshold was exceeded. Inspected the annual risk assessment to determine that risks noted throughout the year were reviewed on an annual basis.	No Exceptions Noted

CONTROL ACTIVITIES– Common Criteria Related to Control Activities
Number **CC-5.3**
The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-5.3.1	CGC has defined and documented employee responsibilities, via formal Job Descriptions. Segregation of duties are detailed in the organizational chart and job descriptions.	Inspected job descriptions for the new hires during the period to determine that content provided a level of detail to establish responsibilities. Inspected the Organization Chart to determine that the chart provided details regarding segregation of duties.	No Exceptions Noted
CC-5.3.2	CGC has established its business processes and documented them in policies communicated to the employees.	Inspected the IT Security Policy, Information Security Policy, Web Usage Policy and the Corporate Software Support Guidelines to determine that business process were documented. Inspected signed acknowledgements for the new hires during the period to determine that an employment agreement, acknowledgment of the IT Security Policy, and acknowledgement of the Employee Handbook were signed.	No Exceptions Noted

LOGICAL AND PHYSICAL ACCESS CONTROLS– Common Criteria Related to Logical and Physical Access
Number **CC-6.1**
The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-6.1.1	Policy statements are reviewed on an annual basis by the Director of ICS.	Inspected the IT Security Policy, Information Security Policy and the Web Usage Policy to determine that the statements were reviewed on an annual basis by the Director of ICS.	No Exceptions Noted
CC-6.1.2	CGC maintains documentation on IT related assets.	Inspected the IT related assets listing to determine that CGC provided adequate descriptions of the assets and maintained the listing.	No Exceptions Noted
CC-6.1.3	CGC uses Microsoft's Active Directory to maintain security settings for employees. Groups are defined by functional areas an assigned to the appropriate staff members.	Inspected Active Directory configuration to determine that security settings for employees were maintained Inspected the Active Directory configuration to determine that groups were defined by functional areas.	No Exceptions Noted
CC-6.1.4	CGC maintains separate network segments for CGC internal and SAAS Customer networks.	Inspected system generated documentation to determine that separate environment existed.	No Exceptions Noted
CC-6.1.5	CGC internal data is organized by functional area and access to restricted information is provided on an as-needed basis.	Inspected system documentation to determine that internal data was organized. Inspected access listing to determine that restricted information was granted based on an as-needed basis.	No Exceptions Noted

LOGICAL AND PHYSICAL ACCESS CONTROLS– Common Criteria Related to Logical and Physical Access

Number
CC-6.2

Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-6.2.1	Controller is responsible for completing a New User Request Form (e-mail) that identifies CGC employee access and authorization to network resources and the hosting partner systems environment. The email is then forwarded to ICS via email for setup.	Inspected New User Request e-mail from the Controller for all new hires during the period to determine that approval was obtained from CGC management to grant access.	No Exceptions Noted
CC-6.2.2	Only authorized staff within ICS have been assigned privileges to create user accounts and related permissions.	Inspected Active Directory Domain Administrators to determine that access was assigned to ICS personnel	No Exceptions Noted
CC-6.2.3	The Controller notifies ICS of all termination events for the disabling of user accounts. User account passwords are immediately changed and are subsequently disabled after email forwarding has been established,	Inspected termination email notification from the Controller for the terminated employees during the period to determine that notification was sent to ICS. Inspected the active directory listing for the terminated users during the period to determine that user accounts were disabled or deleted upon notification.	No Exceptions Noted
CC-6.2.4	Annually, a list of active employees from the Controller is compared to Active Directory and application user accounts to identify any discrepancies.	Inspected access review documentation for the annual reviews in the period to determine that access reviews were completed and documented.	No Exceptions Noted

Proprietary and Confidential
Do NOT reproduce, duplicate, or disclose without express written consent.

LOGICAL AND PHYSICAL ACCESS CONTROLS– Common Criteria Related to Logical and Physical Access
Number **CC-6.3**
The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-6.3.1	Controller is responsible for completing a New User Request Form (e-mail) that identifies CGC employee access and authorization to network resources and the hosting partner systems environment. The email is then forwarded to ICS via email for setup.	Inspected New User Request e-mail from the Controller for all new hires during the period to determine that approval was obtained from CGC management to grant access.	No Exceptions Noted
CC-6.3.2	The Controller notifies ICS of all termination events for the disabling of user accounts. User account passwords are immediately changed and are subsequently disabled after email forwarding has been established,	Inspected termination email notification from the Controller for the terminated employees during the period to determine that notification was sent to ICS. Inspected the active directory listing for the terminated users during the period to determine that user accounts were disabled or deleted upon notification.	No Exceptions Noted
CC-6.3.3	The user-access model is based on the principle of least-privileged access. CGC employee user permission are based on the defined responsibilities of the role assigned to the employee.	Inspected New User Request e-mail from the Controller for a sample of hires to determine that access was requested and approved. Inspected Active users and groups to determine that unique user account existed. Inspected Active Directory Domain Administrators to determine that access was assigned to Technical Services personnel.	No Exceptions Noted
CC-6.3.4	CGC segregates responsibilities under lead groups. * Development * Technical Services * Software Delivery / Quality Assurance * Application Support These groups were established on functional, security and general business demands.	Inspected the descriptions of the lead groups to determine that the groups were established based on functional, security, and general business demands.	No Exceptions Noted

LOGICAL AND PHYSICAL ACCESS CONTROLS– Common Criteria Related to Logical and Physical Access
Number **CC-6.4**
The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-6.4.1	CGC office space is controlled by electronic security cards and are locked during nonbusiness hours.	Observed the facility to determine that all doors to access the CGC office space locked on a programmed schedule. Inspected the door card schedule for the office space used by CGC to determine the doors were scheduled to lock during nonbusiness hours.	No Exceptions Noted
CC-6.4.2	Employees who need access to the CGC office space are issued electronic key cards.	Inspected CGC Asset Forms for all new hires during the period to determine that access cards issued to new hires were documented.	No Exceptions Noted
CC-6.4.3	CGC preforms annual comparisons of it door access list and employee list to verify they match.	Inspected access review documentation for the annual reviews in the period to determine that access comparisons were completed and documented.	No Exceptions Noted

Proprietary and Confidential
Do NOT reproduce, duplicate, or disclose without express written consent.

LOGICAL AND PHYSICAL ACCESS CONTROLS– Common Criteria Related to Logical and Physical Access

Number
CC-6.5

The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-6.5.1	Formal data retention and disposal procedures are in place to guide the secure disposal of the company's and customers' data.	Inspected the IT Security Policy that included formal data retention and disposal procedures to determine that the procedures provided guidelines to dispose of data.	No Exceptions Noted
CC-6.5.2	When disposing of any IT equipment that may contain customer data, the device must be scrubbed of all customer data. Tapes, CD, hard drives and computer must be destroyed through a certified eRecyling service.	Inquired of CGC management to determine that devices contained client data were destroyed prior to disposal. Inquired of management to determine whether any devices containing client data were destroyed during the reporting period.	Control activity did not occur during the reporting period. As a result, no testing performed.

LOGICAL AND PHYSICAL ACCESS CONTROLS– Common Criteria Related to Logical and Physical Access
Number **CC-6.6**
The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-6.6.1	CGC uses Microsoft's Active Directory to maintain security settings for employees. Groups are defined by functional areas an assigned to the appropriate staff members.	Inspected Active Directory configuration to determine that security settings for employees were maintained Inspected the Active Directory configuration to determine that groups were defined by functional areas.	No Exceptions Noted
CC-6.6.2	All access to CGC systems is performed over security VPN or SSL based encrypted communications.	Inspected firewall definitions to determine that VPN access is limited to Active Directory users and that routes exist between the CGC corporate network and the SaaS networks.	No Exceptions Noted
CC-6.6.3	A Wi-Fi access point is available to employees for connection to CGC’s internal network (Intranet). All employees are required to enter a valid Wi-Fi security code to connect to the Intranet.	Inspected Wi-Fi configuration to determine that Wi-Fi access for employees required a security code to gain access to the Wi-Fi.	No Exceptions Noted
CC-6.6.4	Wi-Fi access point is provided to visitors for only Internet connectivity. The guest network is on a separate VLAN and requires a password provided by IT Services	Inspected Wi-Fi configuration to determine that Wi-Fi access for visitors did not connect to the CGC network and only had internet access.	No Exceptions Noted
CC-6.6.5	CGC uses firewalls to restrict and limit traffic between public networks and the internal networks.	Inspected network diagram to determine that the network had been adequately mapped and indicated the placement of firewalls. Inspected the firewall configuration to determine that traffic was restricted and limited.	No Exceptions Noted

LOGICAL AND PHYSICAL ACCESS CONTROLS– Common Criteria Related to Logical and Physical Access
Number **CC-6.7**
The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-6.7.1	CGC employees that have a business need to connect onsite are required to establish the connection with a company-provided device loaded with appropriate VPN certificates	Inspected the Cisco AnyConnect configuration to determine that the VPN was integrated with active directory and included an IP Sec tunnel for onsite connections. Inspected the Client VPN configuration to determine that an IP Sec tunnel with a valid certificate was required to establish a connection.	No Exceptions Noted
CC-6.7.2	All access to CGC systems is performed over security VPN or SSL based encrypted communications.	Inspected firewall definitions to determine that VPN access is limited to Active Directory users and that routes exist between the CGC corporate network and the SaaS networks.	No Exceptions Noted

LOGICAL AND PHYSICAL ACCESS CONTROLS– Common Criteria Related to Logical and Physical Access
Number **CC-6.8**
The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-6.8.1	Antivirus software is installed and maintained on workstations, laptops, and Windows servers.	Inspected the configuration of anti-virus software console to determine that software was installed on workstations, laptops, and Windows servers.	No Exceptions Noted
CC-6.8.2	Anti-virus pattern files update upon user login to the corporate internal network and throughout the business day as updated pattern files become available.	Inspected anti-virus configurations to determine that pattern files were updated and pushed to network devices.	No Exceptions Noted
CC-6.8.3	The ability to install applications on servers is restricted to personnel with access to the servers as granted by ICS.	Inspected the groups established by CGC that had been authorized to install applications on servers to determine access was restricted to ICS or the asset owner.	No Exceptions Noted
CC-6.8.4	CGC has established it change management procedures and documented them in policies communicated to the employees.	Inspected the Software Support Guidelines and the Configuration Management Plan to determine that change management procedures were documented and were available to the employees.	No Exceptions Noted

SYSTEM OPERATIONS – Common Criteria Related to System Operations

Number
CC-7.1

To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-7.1.1	Defined entity standards exist for infrastructure and software hardening and configuration that include requirements for implementation of access control software, entity configuration standards, and standardized access control lists that define which privileges are attributable to each user or system account.	Inspected the Windows Server Security Procedure to determine that the entity's standards were documented including requirements for implementation of access control software, entity configuration standards, and standardized access control lists that defined which privileges were attributable for each user or system account. Inspected the configuration standard template to determine that the Windows Servers operating systems were hardened beyond the default configuration and that only necessary ports and services were enabled.	No Exceptions Noted
CC-7.1.2	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests.	Inspected the weekly status reports for a selection of weeks during the reporting period to determine that the departments reported on performance, security threats and vulnerabilities, resource utilization and to detect unusual system activity or service requests for the last week.	No Exceptions Noted
CC-7.1.3	ICS staff is notified of events that impact the security or availability of systems or the confidentiality of data.	Inspected an example alert from the A/V software to determine that the ICS staff was notified of events that impact the security or availability of systems or the confidentiality of data. Inspected a screenshot of the monitoring system dashboard to determine that there was real time data available when performance thresholds had been exceeded. Inspected alert messages from the monitoring system to determine that alerts were produced after a threshold was exceeded.	No Exceptions Noted

SYSTEM OPERATIONS – Common Criteria Related to System Operations

Number
CC-7.2

The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-7.2.1	CGC uses firewalls to restrict and limit traffic between public networks and the internal networks.	Inspected network diagram to determine that the network had been adequately mapped and indicated the placement of firewalls. Inspected the firewall configuration to determine that traffic was restricted and limited.	No Exceptions Noted
CC-7.2.2	CGC utilizes firewalls and software related filters to prevent unauthorized access to CGC systems.	Inspected network diagram to determine that the network had been adequately mapped and indicated the placement of firewalls. Inspected the firewall and software related filters configuration to determine that access was prevented from unauthorized access.	No Exceptions Noted
CC-7.2.3	All servers, switches, and routers are monitored by a centralized event logging and alerting tool. Monitoring tools are configured to generate automated alerts when pre-determine thresholds are exceeded. Notifications are sent to the ICS team.	Inspected system logging screenshots for the monitoring tools utilized by CGC to determine that all servers, switched and routers are monitored by a centralized event logging and alerting tool. Inspected alert messages from the monitoring system to determine that alerts were produced after a threshold was exceeded.	No Exceptions Noted

SYSTEM OPERATIONS – Common Criteria Related to System Operations
Number **CC-7.3**
The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-7.3.1	Operations and security personnel follow defined protocols for resolving and escalating reported events as they relate to security and availability of systems and the confidentiality of data.	Inspected Security Protocols Document to determine that a process was required for the identification and mitigation of security breaches and other incidents. Inquired of management to determine there were no security incidents during the reporting period.	No Exceptions Noted
CC-7.3.2	CGC employees follow defined protocols for evaluating and escalating reported events. Security related events are assigned to the ICS group for evaluation.	Inspected Security Policy Statement and Security Protocol document to determine a process was defined for managing and resolving complaints and requests relating to security issues. Inquired of management to determine whether there were any security incidents in the reporting period.	No Exceptions Noted
CC-7.3.3	Director of ICS generates a weekly report to give ticket metrics to the President of CGC.	Inspected weekly reports for a selection of weeks during the period to determine that ticket metrics were generated and sent to the President of CGC.	No Exceptions Noted

SYSTEM OPERATIONS – Common Criteria Related to System Operations
Number **CC-7.4**
The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-7.4.1	CGC segregates responsibilities under lead groups. * Development * Technical Services * Software Delivery / Quality Assurance * Application Support These groups were established on functional, security and general business demands.	Inspected the descriptions of the lead groups to determine that the groups were established based on functional, security, and general business demands.	No Exceptions Noted
CC-7.4.2	CGC employees follow defined protocols for evaluating and escalating reported events. Security related events are assigned to the ICS group for evaluation.	Inspected Security Policy Statement and Security Protocol document to determine a process was defined for managing and resolving complaints and requests relating to security issues. Inquired of management to determine whether there were any security incidents in the reporting period.	No Exceptions Noted
CC-7.4.3	Operations and security personnel follow defined protocols for resolving and escalating reported events as they relate to security and availability of systems and the confidentiality of data.	Inspected Security Protocols Document to determine that a process was required for the identification and mitigation of security breaches and other incidents. Inquired of management to determine there were no security incidents during the reporting period.	No Exceptions Noted
CC-7.4.4	Director of ICS generates a weekly report to give ticket metrics to the President of CGC.	Inspected weekly reports for a selection of weeks during the period to determine that ticket metrics were generated and sent to the President of CGC.	No Exceptions Noted
CC-7.4.5	Disk-to-disk backups are performed on a daily, weekly, and monthly basis at each data center. The weekly and monthly backups are replicated between the two data centers, daily or weekly, to maintain off-site copies of data backups.	Inspected iSeries job scheduler and auto-generated emails to determine that database backups executed nightly and were sent via FTP to the backup server.	No Exceptions Noted

SYSTEM OPERATIONS – Common Criteria Related to System Operations
Number **CC-7.5**
The entity identifies, develops, and implements activities to recover from identified security incidents.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-7.5.1	Incident tickets are initiated when an eCMS client user organization reports an issue to the CGC Service Desk either via the web portal, telephone or by email.	Inquired of management to determine whether there were any security incidents in the reporting period.	Control activity did not occur during the reporting period. As a result, no testing performed.
CC-7.5.2	Director of ICS generates a weekly report to give ticket metrics to the President of CGC.	Inspected weekly reports for a selection of weeks during the period to determine that ticket metrics were generated and sent to the President of CGC.	No Exceptions Noted
CC-7.5.3	If no restoration has been completed in a 12 month period, a test of the recovery process is conducted by management.	Inspected documentation to determine data backups had been effectively been restored.	No Exceptions Noted
CC-7.5.4	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	Inspected documentation to determine that data backup tapes from the eCMS application were restored on a periodic basis for recovery purposes. Inspected documentation to determine that the business continuity plan and disaster recovery plans were tested annually.	No Exceptions Noted
CC-7.5.5	Test results were reviewed, and the contingency plan is updated as necessary to ensure timely recovery of systems.	Inspected documentation to determine that the business continuity plan and disaster recovery plans were tested annually.	No Exceptions Noted

CHANGE MANAGEMENT – Common Criteria Related to Change Management
Number **CC-8.1**
The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-8.1.1	CGC Configuration Management Plan outlines tasks associated with scheduled changes including authorization, testing, and approval before deploying to the production environment.	Inspected the Configuration Management Plan to determine that it outlined tasks associated with schedule changes, including authorization, testing, and approval before deploying the change to the production environment. Inspected change tickets for a selection of eCMS Incident Tickets from a list of changes during the reporting period to determine that changes were tracked in the management system and that they contained evidence of authorization, testing and approval before being deployed into the production environment.	No Exceptions Noted
CC-8.1.2	All infrastructure changes are initiated, authorized, and tracked in the management system.	Inspected change tickets for a selection of eCMS Incident Tickets from a list of changes during the reporting period to determine that changes were tracked in the management system and that they contained evidence of authorization, testing and approval before being deployed into the production environment.	No Exceptions Noted
CC-8.1.3	All software development changes are initiated, authorized, and tracked in the management system.	Inspected change tickets for a selection of eCMS Incident Tickets from a list of changes during the reporting period to determine that changes were tracked in the management system and that they contained evidence of authorization, testing and approval before being deployed into the production environment.	No Exceptions Noted
CC-8.1.4	CGC has established an environment separate from production for design and testing purposes for critical infrastructure	Inspected system generated documentation to determine that separate environments had been established for design and testing purposes outside of the production environment.	No Exceptions Noted
CC-8.1.5	Access to SaaS Hosted Environment is limited to CGC support staff only.	Inspected system-generated documentation to determine that only Technical Services personnel had access to the production environment.	No Exceptions Noted

RISK MITIGATION – Common Criteria Related to Risk Mitigation
Number **CC-9.1**
The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-9.1.1	CGC employs procedures, system monitoring, communications, documentation and management review to mitigate risk. System monitoring is performed in real-time, communications are performed as needed and documentation is reviewed on an annual basis.	Inspected the IT Security Protocols to determine that management performs reviews and implements controls to mitigate risks. Inspected a screenshot of the monitoring system dashboard to determine that there was real time data available when performance thresholds had been exceeded. Inspected alert messages from the monitoring system to determine that alerts were produced after a threshold was exceeded. Inspected the annual risk assessment to determine that risks noted throughout the year were reviewed on an annual basis.	No Exceptions Noted
CC-9.1.2	CGC management performs a risk assessment annually. The risk assessment is based on the objectives established by management.	Inspected the annual risk assessment to determine that the risk assessment was performed. Inspected the risk assessment to determine the risk assessment was based on the objectives established by management.	No Exceptions Noted

RISK MITIGATION – Common Criteria Related to Risk Mitigation
Number **CC-9.2**
The entity assesses and manages risks associated with vendors and business partners.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
CC-9.2.1	CGC has contractual agreements with external vendors that provide colocation services that outline the responsibilities of the vendor.	Inspected the agreement between Tech Data and CGC to determine that the contract identified roles and responsibilities of Tech Data.	No Exceptions Noted
CC-9.2.2	A vendor risk assessment is performed for all vendors on an annual basis that have access to confidential data or impact the security of the system.	Inspected the annual vendor risk assessment to determine the risk assessment was performed on all vendors that have access to confidential data or impact the security of the systems.	No Exceptions Noted

AVAILABILITY – Additional Criteria for Availability
Number **A1.1**
The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
A1.1.1	Processing capacity is monitored real time on an ongoing basis including: • RAM • CPU • Server Disk Space • Network Bandwidth Defined capacity rule sets that that are exceeded will generate auto alerts to the ICS Team.	Inspected a screenshot of the monitoring system dashboard to determine that there was real time data available when performance thresholds had been exceeded. Inspected alert messages from the monitoring system to determine that alerts were produced after a threshold was exceeded.	No Exceptions Noted

AVAILABILITY – Additional Criteria for Availability
Number **A1.2**
The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
N/A	N/A as the all in-scope data and software is stored at a third party facilities and environmental protections are the responsibility of the respective vendor.	N/A	N/A

AVAILABILITY – Additional Criteria for Availability
Number **A1.3**
The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
A1.3.1	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	Inspected documentation to determine that data backup tapes from the eCMS application were restored on a periodic basis for recovery purposes. Inspected documentation to determine that the business continuity plan and disaster recovery plans were tested annually.	No Exceptions Noted

CONFIDENTIALITY – Additional Criteria for Confidentiality
Number **C1.1**
The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
C1.1.1	CGC has developed policies relevant to security and availability of systems, including the protection of confidential data.	Inspected the IT Security Policy and Security Protocol Documents to determine that policies addressed the security and availability of systems, including the protection of confidential data.	No Exceptions Noted
C1.1.2	CGC internal data is organized by functional area and access to restricted information is provided on an as-needed basis.	Inspected system documentation to determine that internal data was organized. Inspected access listing to determine that restricted information was granted based on an as-needed basis.	No Exceptions Noted

CONFIDENTIALITY – Additional Criteria for Confidentiality

Number
C1.2

The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Control #	Control Activity Specified by CGC	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results Of Test(s)
C1.2.1	CGC has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.	Inspected the CGC Employee Handbook to determine that policies regarding unauthorized use of company equipment and systems was addressed. Inspected the facility access list and the active directory listing for a selection of terminated employees during the period to determine that access to the facility and CGC systems was disabled or deleted to protect against unauthorized acquisition, use or disposal of assets.	Exception Noted - The facility access was not disabled or deleted for one of the three employees who terminated employment during the period.
C1.2.2	When disposing of any IT equipment that may contain customer data, the device must be scrubbed of all customer data. Tapes, CD, hard drives and computer must be destroyed through a certified eRecyling service.	Inquired of CGC management to determine that devices contained client data were destroyed prior to disposal. Inquired of management to determine whether any devices containing client data were destroyed during the reporting period.	Control activity did not occur during the reporting period. As a result, no testing performed.

Proprietary and Confidential
Do NOT reproduce, duplicate, or disclose without express written consent.

V. Other Information Provided by Computer Guidance Corporation That Is Not Covered by the Service Auditor's Report

The information in Section V is presented by the management of Computer Guidance Corporation to provide additional information and is not a part of Computer Guidance Corporation's description of its system made available to user entities during the period October 1, 2018 to December 31, 2019. Information in Section V has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system, and, accordingly, we express no opinion on it.

Findings & Management Response

Controls Specified by Computer Guidance Corporation	Results of Test(s)	Management Response
CC-3.3.5 C-1.2.1 CGC has established measures to protect against unauthorized and willful acquisition, use, or disposal of assets.	The facility access was not disabled or deleted for one of the three employees who terminated employment during the period.	While a single facility access card was not promptly disabled after an employee termination, the access card was confiscated and in the possession of HR immediately after the employee was terminated.