COMPUTER GUIDANCE CORPORATION

Independent Service Auditors' Trust Services Report

Report on Suitability of Control Design and Operating Effectiveness For Security, Availability & Confidentiality Trust Principle(s) Criteria

For Period:
October 1, 2017 through September 30, 2018

CliftonLarsonAllen

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

TABLE OF CONTENTS

CliftonLarsonAllen LLP
20 East Thomas Road, Suite 2300
Phoenix, AZ 85012-3111
602-266-2248 | fax 602-266-2907
CLAconnect.com

I. Independent Service Auditors' Report

Executive Management
Computer Guidance Corporation
Scottsdale, Arizona

Scope

We have examined Computer Guidance Corporation's accompanying description of its eCMS Hosting Services system titled "Description of Computer Guidance Corporation's eCMS Hosting Services system" throughout the period October 1, 2017 to September 30, 2018 (description) based on the criteria for a description of a service organization's system in DC section 200A, *Description Criteria for a description of a Service Organization's System in a SOC 2 Report (2015 description criteria) (AICPA, Description Criteria)* (description criteria) and the suitability of design and operating effectiveness controls stated in the description throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that Computer Guidance Corporation'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 100A*, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2016) (AICPA, *Trust Services Criteria and Privacy)* (applicable trust services criteria).

As indicated in the description, Computer Guidance Corporation uses a subservice organization for colocation data center services. The description includes only the applicable trust services criteria, and related controls of Computer Guidance Corporation and excludes the related controls of the subservice organization. The description also indicates that certain applicable trust services criteria can be met only if complementary subservice organization controls assumed in the design of Computer Guidance Corporation's controls are suitably designed and operating effectively, along with the related controls at Computer Guidance Corporation. 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 applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of Computer Guidance Corporation'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 of such complementary user entity controls.

Service Organization's Responsibilities

Computer Guidance Corporation 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 Computer Guidance Corporation's service commitments and system requirements were achieved. Computer Guidance Corporation has provided the accompanying assertion titled "Management of Computer Guidance Corporation's Assertion Regarding Its eCMS Hosting Services system throughout the period October 1, 2017 to September 30, 2018" (assertion) about the description and the suitability of the design of controls stated therein. Computer Guidance Corporation 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 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 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
- performing procedures to obtain evidence about whether description 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 requirement based the applicable trust criteria
- testing the operating effectiveness of controls stated in the description to reasonable assurance that the service organization achieved its service commitment and system requirements based on the applicable trust services criteria
- evaluating the overall presentation of the description

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

Inherent Limitations

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

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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 we tested and the nature, timing, and results of those tests are listed in section IV.

Computer Guidance Corporation's description of its eCMS Hosting Service system discusses its changes to confidentiality procedures, which includes the controls implemented and operated to approve and communicate changes to confidentiality practices. However, during the period October 1, 2017 through September 30, 2018, Computer Guidance Corporation did not change its confidentiality procedures. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criteria C-1.6, *Changes to confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are included in the system*.

Computer Guidance Corporation's description of its eCMS Hosting Service system discusses its data destruction procedures, which includes the controls implemented and operated to ensure disk drives from servers and/or workstations that contain confidential information are destroyed prior to disposal. However, during the period October 1, 2017 through September 30, 2018, Computer Guidance Corporation did not dispose of any disk drives from servers or workstations that would warrant the operation of the this control. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using confidentiality criteria C-1.8, *The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.*

Opinion

In our opinion, in all material respects,—

a. the description presents Computer Guidance Corporation's eCMS Hosting Service system that was designed and implemented throughout the period October 01, 2017 to September 30, 2018, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period October 01, 2017 to September 30, 2018, to provide reasonable assurance that Computer Guidance Corporation's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the user entities applied the complementary controls assumed in the design of Computer Guidance Corporation's controls.

c. the controls stated in the description operated effectively throughout the period October 01, 2017 to September 30, 2018, to provide reasonable assurance that Computer Guidance Corporation's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Computer Guidance Corporation'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 Computer Guidance Corporation, user entities of Computer Guidance Corporation's eCMS Hosting Service system during some or all of the period October 01, 2017 to September 30, 2018, business partners of Computer Guidance Corporation; 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 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

Phoenix, AZ

II. Computer Guidance Corporation's Management Assertion

Management of Computer Guidance Corporation (CGC) Assertion Regarding Its eCMS Hosting Services System throughout the period October 1, 2017 to September 30, 2018.

We have prepared the description of Computer Guidance Corporation's system entitled, "System Description of eCMS Hosting Services System," throughout the period October 1, 2017 to September 30, 2018 (description) based on the criteria description of a service organization's system in DC section 200A, *Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (2015 description criteria) (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of the controls stated in the description throughout the period October 1, 2017 to September 30, 2018, to provide reasonable assurance that Computer Guidance Corporation'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 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, Trust Services Principles and 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 Computer Guidance Corporation to meet the applicable trust services criteria. The description presents Computer Guidance Corporation's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Computer Guidance Corporation's controls.

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

a) the description fairly presents the eCMS Hosting System throughout the period October 1, 2017 to September 30, 2018, based on the following description criteria:
   i. The description contains the following information:
      (1) The types of services provided.
      (2) The components of the system used to provide the services, which are as follows:
         - *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

- *Software*. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- *People*. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- *Procedures*. The automated and manual procedures.
- *Data*. Transaction streams, files, databases, tables, and output used or processed by the system.

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

(4) How the system captures and addresses significant events and conditions.

(5) The process used to prepare and deliver reports and other information to user entities or other parties.

(6) For information provided to, or received from, subservice organizations and other parties, (*a*) how the information is provided or received and the role of the subservice organizations and other parties and (*b*) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, (*a*) complementary user entity controls contemplated in the design of the service organization's system.

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

(9) Any applicable trust services criteria that are not addressed by a control at the service organization and the reasons therefore.

(10) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(11) Relevant details of changes to the service organization's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a

broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b) the controls stated in the description were suitably designed throughout the period October 1, 2017 to September 30, 2018, to meet the applicable trust services criteria.

c) the controls stated in the description operated effectively throughout the period October 1, 2017 to September 30, 2018, to meet the applicable trust services criteria, and if user entities applied the complementary controls assumed in the design of Computer Guidance Corporation's controls throughout that period, except for controls related to confidentiality process changes and data or device disposal that did not operate during the period, as evaluated using trust services criteria C-1.6 and C-1.8.

By:

Michael Bihlmeier

Michael Bihlmeier
President

Computer Guidance Corporation
March 11, 2019

III. System 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:

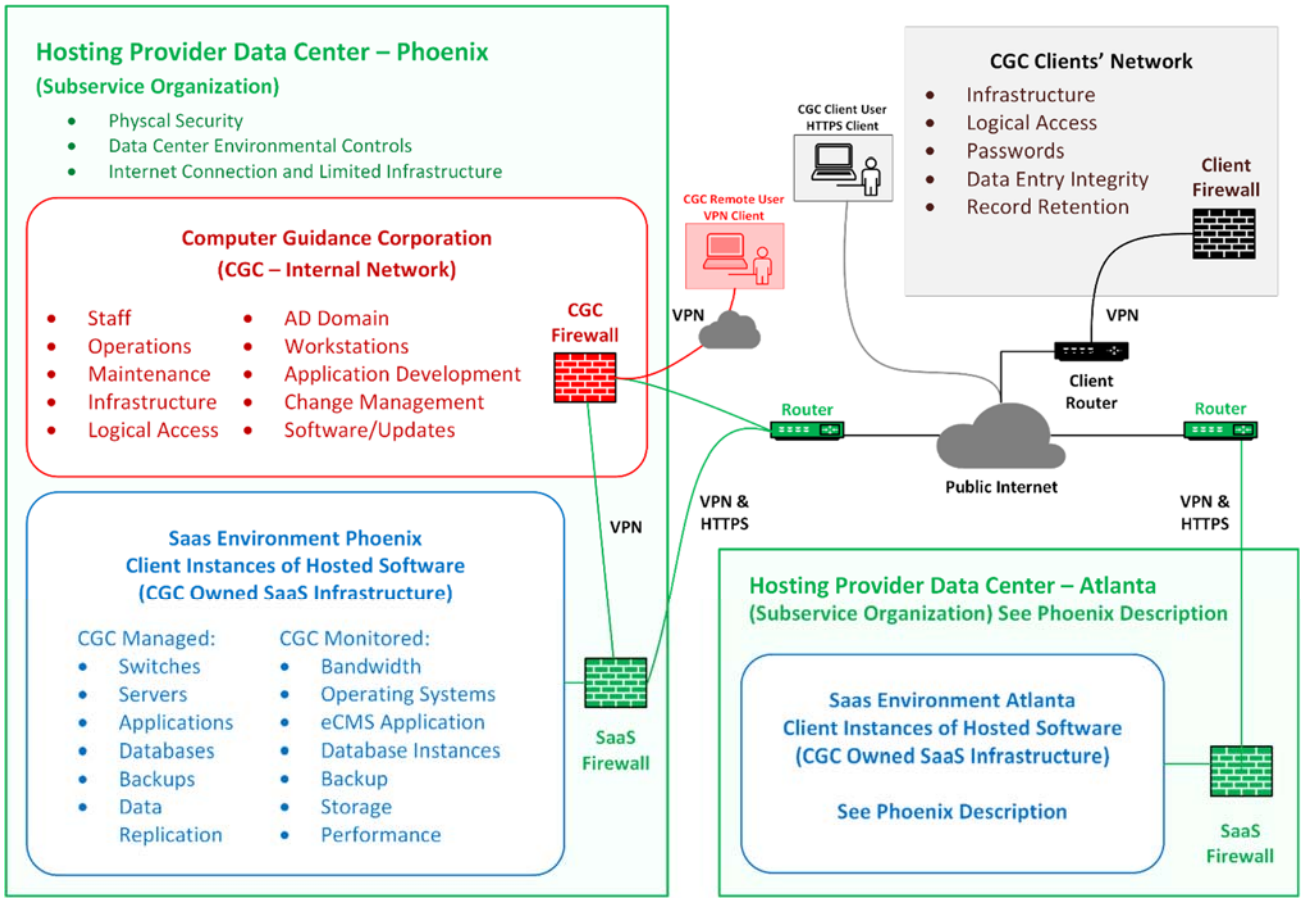
Operations related to the delivery of CGC's products and/or services are supported by the following functional business areas:

- 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 non-production 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 non-proprietary (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.

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;
- Non-disclosure 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 non-competition 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.

Change Management

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.

Non-Scheduled (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.

Technical Infrastructure Monitoring

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 non-disclosure 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 controls described within this section are the responsibility of client-user organizations, and should be actively in operation to properly complement the controls of CGC. Each client user organization must evaluate its own control environment to determine if the following controls are in-place and operating effectively. Accordingly, this list does not purport to be (and most likely is not) a complete listing of the controls that provide a basis for the assertions underlying the financial statements of clients.

With these limitations in mind, the following user control considerations have been presented to assist the user organization in addressing certain control issues that are considered to be an integral part of the entire control environment under which their data is processed. User organizations are responsible for the development, implementation, documentation, review, and modification of appropriate internal controls and procedures to confirm that data processed by CGC is done completely, accurately, and in a timely manner. Controls which user organizations are responsible for include, but are not limited to the following:

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.
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-5.5	Physical Security	• Physical Security to Hosting Facility
CC-2.5	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. Independent Service Auditors' Tests of Controls and Results

Overview

The identified control activities are solely the responsibility of the management of Computer Guidance Corporation (CGC). The control activities listed in the first column "*Control Activity Specified by Computer Guidance, Inc.*" have been identified by CGC 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.

Control Activity Test(s)

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 meet the selected Trust Services Criteria during the period from October 01, 2017 to September 30, 2018. Our tests of operating effectiveness of controls were designed to cover the period from October 01, 2017 to September 30, 2018, for each of the controls listed in the matrix in Section 4, which are designed to meet the selected Trust Services Criteria. 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 selected Trust Service(s) Criteria.

Tests performed of the operating effectiveness of controls detailed in the matrix contained in Section 4 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.

Service Organization Controls (SOC) 2 Trust Services Criteria

Although the Trust Services Criteria and related controls are presented in section 4, they are an integral part of the CGC System description. The following pages contain criteria for each category of the selected Trust Services Criteria as defined by the American Institute of Certified Public Account (AICPA) with a description of the controls that CGC has implemented to meet the defined criteria.

Common Criteria to Security, Availability, and Confidentiality Principles

ORGANIZATION AND MANAGEMENT – Common Criteria Related to Organization and Management	
CC-1.0	**Organization and Management** The criteria relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

Common Criteria – Organization Structure	
CC-1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to security, availability, and confidentiality.

	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CC-1.1.01	**Organization Structure**		
	The organization 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

Common Criteria – System Controls Responsibility			
CC-1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies, and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.		
	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CC-1.2.01	**Policy Development**		
	CGC has developed policies relevant to security and availability of systems, including the protection of confidential data.	Inspected the IT Security Policies to determine that the policies addressed information security, availability, and protection of confidential data	No Exceptions Noted
CC-1.2.02	**Policy Approval**		
	The Director of ICS approves policy statements produced by the Technical Services staff.	Inspected the IT Security Policies to determine that policies were approved by the Director of ICS.	No Exceptions Noted
CC-1.2.03	**Policy Statements**		
	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 Policy statements are made available to the employees via the Employee Handbook and its Intranet site.	Inspected the IT Security Policies and Employee Handbook to determine that policy statements outlined the organizational values and behavioral standards. Inspected the intranet site to determine that the Employee Handbook and other security-related policies were available to employees.	No Exceptions Noted
CC-1.2.04	**Policy Reviews**		
	Policy statements are reviewed on an annual basis by the Director of ICS.	Inspected the IT Security Policies to determine that security policies were reviewed annually.	No Exceptions Noted

CC-1.2.05	**Policy Updates**		
	CGC management is responsible for communicating policy and procedure changes to employees when updates are made.	Inquired of management to determine that policy and procedure changes would have been communicated to employees via email or in team meetings.	Control activity did not occur during the reporting period. As a result, no testing performed.

Common Criteria – Personnel Qualifications & Resources

CC-1.3 The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting security, availability, and confidentiality and provides resources necessary to fulfill their responsibilities.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-1.3.01	**Position Descriptions**		
	Position descriptions are established and maintained for positions within CGC that are responsible for the eCMS Hosted Services, describing key areas of accountability and reporting structure, along with education, experience, and skill requirements.	Inspected job descriptions for the Technical Services Team to determine that content provided a level of detail to establish accountability and reporting structure, along with education, experience, and skill requirements.	No Exceptions Noted
CC-1.3.02	**Candidate Qualifications**		
	Hiring procedures 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
	Criminal background checks are performed 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 hire in the period to determine that a background check was performed.	No Exceptions Noted

Common Criteria – Personnel Qualifications & Resources

CC-1.3 The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting security, availability, and confidentiality and provides resources necessary to fulfill their responsibilities.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
As part of the hiring process, employees are required to sign the following: • Employment Agreement • IT Security Policy Acknowledgement • Employee Handbook Acknowledgement	Inspected signed acknowledgements for a sample of hires in 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.
New employees are trained on security which is outlined in the employment agreement and Employee Handbook.	Inspected new hire training acknowledgements for a sample of hires in the period to determine that an acknowledgment agreement was signed after receiving training.	No Exceptions Noted.
Professional Services Agreements are used when contractors are engaged to perform services for CGC. The agreements include non-disclosure verbiage.	Inquired of management to determine that Professional Services Agreements would have been used if any contractors had been used during the reporting period.	Control activity did not occur during the reporting period. As a result, no testing performed.

Common Criteria – Workplace Conduct Standards

CC-1.4 The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring of the system affecting security, availability, and confidentiality and provides resources necessary to fulfill their responsibilities.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CROSS REFERENCE – Previously Defined Controls		
CC-1.2.03 **Policy Statements**	Refer to CC-1.2.03 **Policy Statements**	No Exceptions Noted
CC-1.3.01 **Position Descriptions**	Refer to CC-1.3.01 **Position Descriptions**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted

COMMUNICATIONS – Common Criteria Related to Communications

CC-2.0 Communication

The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

Common Criteria – System Boundaries

CC-2.1 Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users of the system to permit users to understand their role in the system and the results of system operation.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CROSS REFERENCE – Previously Defined Controls		
CC-1.1.01 **Organization Structure**	Refer to CC-1.1.01 **Organization Structure**	No Exceptions Noted
CC-1.3.01 **Position Descriptions**	Refer to CC-1.3.01 **Position Descriptions**	No Exceptions Noted
CC-1.2.03 **Policy Statements**	Refer to CC-1.2.03 **Policy Statements**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted
CC-2.1.01 Hosting-Related Organizational Structure		
A description of the entity's hosting-related organizational structure and process flows is posted on CGC's Intranet and available to CGC's internal users.	Inspected documents to determine that the entity has prepared an objective description of the system and the description included organizational structure and process flows. Inspected the intranet site for CGC to determine that the entity's hosting-related organization structure and process flows were posted for internal users.	No Exceptions Noted

CC-2.1.02	**System Description**		
	CGC has established and maintains a description of the eCMS hosted environment. CGC develops and maintains documentations that identifies the technical components of the eCMS hosted services, including communications equipment, security devices, servers, and other critical devices associated with service delivery.	Inspected documentation to determine that CGC had established and maintained a description of the CGC environment. Inspected technical diagrams to determine that they identified the technical components of the data network including communications equipment, security devices, servers, and other critical devices associated with service delivery.	No Exceptions Noted.
CC-2.1.03	**Service Level Agreement(s)**		
	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-2.1.04	**Subservice Contract(s)**		
	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

Common Criteria – System Commitments		
CC-2.2 The entity's security, availability, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal system users to enable them to carry out their responsibilities.		
Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CROSS REFERENCE – Previously Defined Controls		
CC-1.3.01 **Position Descriptions**	Refer to CC-1.3.01 **Position Descriptions**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted
CC-2.1.03 **Service Level Agreement(s)**	Refer to CC-2.1.03 **Service Level Agreement(s)**	No Exceptions Noted
CC-2.1.04 **Subservice Contract(s)**	Refer to CC-2.1.04 **Subservice Contract(s)**	No Exceptions Noted
CC-2.2.01 Service Tickets		
Technical Services is responsible for communicating security changes to CGC management before the change being promoted to the production eCMS environment. Hosting Partner is responsible for communicating security changes to Technical Services that impact security, availability, or confidentiality of the network. CGC Management is responsible for communicating security changes to eCMS client user organizations that impact security, availability, or confidentiality of the underlying infrastructure that hosts the eCMS application.	Inspected the Configuration Management Plan to determine that management approval was required before changes were deployed to production. Inspected Change Management documentation to determine that changes were reviewed and approved prior to being deployed to production. Inspected copy of the agreement between Tech Data and CGC to determine that the contract contained verbiage indicating Tech Data was responsible for notifying CGC of security breaches. Inspected user agreements for a sample of new clients to determine that procedures had been established for CGC to notify client user organizations of scheduled changes if the changes had the potential of impacting the security or availability of the eCMS application or underlying infrastructure.	No Exceptions Noted

Common Criteria – System Functions		
CC-2.3 The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.		
Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CROSS REFERENCE – Previously Defined Controls		
CC-1.2.03 **Policy Statements**	Refer to CC-1.2.03 **Policy Statements**	No Exceptions Noted
CC-1.3.01 **Position Descriptions**	Refer to CC-1.3.01 **Position Descriptions**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted
CC-2.3.01 Statement(s) of Work		
Work performed for clients outside of the scope of the standard hosted agreement is detailed in an activity-specific Statement of Work.	Inspected the Statements of Work for the activities performed outside the scope of the standard hosting agreement during the period to determine that the work was detailed.	No Exceptions Noted

Common Criteria – System Controls		
CC-2.4 Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, and confidentiality of the system, is provided to personnel to carry out their responsibilities.		
Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CROSS REFERENCE – Previously Defined Controls		
CC-1.2.03 **Policy Statements**	Refer to CC-1.2.03 **Policy Statements**	No Exceptions Noted
CC-1.3.01 **Position Descriptions**	Refer to CC-1.3.01 **Position Descriptions**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted

Common Criteria – System Anomalies		
CC-2.5 Internal and external system users have been provided with information on how to report security, availability, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.		
Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CROSS REFERENCE – Previously Defined Controls		
CC-1.2.03 **Policy Statements**	Refer to CC-1.2.03 **Policy Statements**	No Exceptions Noted
CC-2.1.03 **Service Level Agreement(s)**	Refer to CC-2.1.03 **Service Level Agreement(s)**	No Exceptions Noted

CC-2.5.01	**Reporting Issue(s) – User Entity Responsibility**		
	SLA between CGC and client identifies responsibilities of the client to report issues that require resolution. User entities have the option of reporting issues to CGC via the website that links to the CGC ticketing system.	Inspected the Software Support Guidelines Document and Software Support Process document to determine that it described the process for clients informing CGC about reporting issues. Inspected the agreements for a sample of new clients in the reporting period to determine verbiage within the agreement included reporting issues. Inspected the Customer Portal to determine that CGC had established a portal for client use to report issues.	No Exceptions Noted
CC-2.5.02	**Reporting Issue(s) – CGC Staff Responsibility**		
	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 Technical Services to determine next steps. Handling of the incident is outlined in the CGC IT Security Policy. ICS staff is responsible for monitoring and managing system alerts that may impact system security and respond appropriately to minimize any negative impact. 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 Security Protocol Document to determine that the policy described procedures on how to notify appropriate individuals of actual or suspected breaches. Inspected the monitoring system and alerts to determine that ICS staff was responsible for monitoring and managing system alerts. 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 agreement with an external business partner to determine that CGC management was responsible for notifying external business partners of confirmed security breaches.	No Exceptions Noted

Common Criteria – System Changes Responsibility

CC-2.6 System changes that affect internal and external system users' responsibilities or the entity's commitments and system requirements relevant to security, availability, and confidentiality are communicated to those users in a timely manner.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-2.6.01	Communication – Internal User(s)		
	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 CGC's intranet to determine that documents were available to internal users including: • Company policies • Comprehensive training materials • Organizational structure documentation	No Exceptions Noted
	CGC communicates updates and changes to internal users via email or in-person meetings, depending on the criticality of the change.	Inspected email notifications for the notices of updates and changes made during the reporting period to determine that updates and changes were communicated to internal users.	No Exceptions Noted
CC-2.6.02	Communication – External User(s)		
	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.	Inquired of management to determine whether any communication to external clients occurred during the reporting period.	Control activity did not occur during the reporting period. As a result, no testing performed.

RISK MANAGEMENT – Common Criteria Related to Risk Management and Design and Implementation of Controls

CC-3.0 Risk Management

The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

Common Criteria – Threat Analysis & Risk Mitigation Strategies

CC-3.1 The entity (1) identifies potential threats that would impair system security, availability, and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assess changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls), and (5) reassesses, and revises, as necessary, risk assessment and mitigation strategies based on the identified changes.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-3.1.01 Master List of System Components		
A master list of the entity's system components is maintained, accounting for additions and removals, for management's use.	Inspected the components spreadsheet to determine that a list of assets was maintained by CGC and included: • Name • Make and model • Remote Management IP	No Exceptions Noted
CC-3.1.02 Risk Assessment Responsibility & Frequency		
CGC has an informal risk management process wherein management assesses risk on an ongoing basis. The Director of ICS holds a weekly meeting with the Windows Team and a bi-weekly meeting with the iSeries Team to review the eCMS environment and address any known risks or threats.	Inspected the calendar for a selection of weeks and months during the period to determine that the ICS Staff had a regularly-scheduled weekly and bi-weekly meetings.	No Exceptions Noted

CC-3.1.03	**Risk Mitigation**		
	During the risk assessment and management process, management identifies environmental, regulatory, and technological changes that have occurred and had an impact security and availability of systems and the confidentiality of data.	Inspected email messages between the management team and customers to determine that as environmental, regulatory, and technological changes occur they are documented and communicated. Inquired through collaboration of CGFC management and CGC staff to determine that weekly and bimonthly meetings during the period were held and discussions were focused on known risks or threats.	No Exceptions Noted
	CGC subscribes to multiple sources for updates of vulnerabilities, viruses, etc. to proactively address known threats and risk-related events.	Inspected industry-relevant newsletters for a selection of months to determine that the Director of ICS subscribed to a source which provided technology updates related to industry, technical, and security vulnerabilities.	No Exceptions Noted

Common Criteria – Control Design and Implementation

CC-3.2 The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.

	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CROSS REFERENCE – Previously Defined Controls			
	CC-1.2.01 **Policy Development**	Refer to CC-1.2.01 **Policy Development**	No Exceptions Noted
	CC-1.2.03 **Policy Statements**	Refer to CC-1.2.03 **Policy Statements**	No Exceptions Noted
	Error! Reference source not found. Error! Reference source not found.Organization Structure	Refer to **Error! Reference source not found. Error! Reference source not found.Organization Structure**	No Exceptions Noted
CC-3.2.01	**Business Recovery Plan(s)**		
	Business recovery plans are tested annually.	Inspected the results of the business recovery plans to determine that business recovery plans were tested annually.	No Exceptions Noted

CC-3.2.02	**Vulnerability Scans**		
	Vulnerability scans are conducted upon customer request and as-needed.	Inquired of CGC management to determine whether any vulnerability scan upon customer requests were conducted.	No vulnerability scan were performed during the reporting period. As a result, no testing was performed.

MONITORING OF CONTROLS – Common Criteria Related to Monitoring of Controls

CC-4.0 Monitoring of Controls

The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

Common Criteria – Control Design and Effectiveness

CC-4.1 The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, availability, and confidentiality and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CROSS REFERENCE – Previously Defined Controls		
CC-1.2.03 **Policy Statements**	Refer to CC-1.2.03 **Policy Statements**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.Organization Structure	Refer to **Error! Reference source not found. Error! Reference source not found.Organization Structure**	No Exceptions Noted
CC-4.1.01 Controls Monitoring by CGC Employees		
CGC employees are responsible for monitoring controls on an ongoing basis in their area of responsibility and the company overall.	Inspected the monitoring software configuration to determine that the software was configured to monitor systems and performance. Inspected an auto-generated email from the monitoring software to determine the employees were notified of monitoring of controls.	No Exceptions Noted
CC-4.1.02 Monitoring Tools		
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-generated documentation from the logging tool to determine that all servers, switches, and routers are monitored by a centralized event logging tool.	No Exceptions Noted

CC-4.1.03	**Responding to Reported Issued / Events**		
	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.	No Exceptions Noted
		Inquired of management to determine there were no security incidents during the reporting period.	Control activity did not occur during the reporting period. As a result, no testing was performed.

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

CC-5.0 Logical and Physical Access

The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.

Common Criteria – Logical Access

CC-5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-5.1.01 Standards		
The IBM i Operating System and Windows Server operating system have been installed on all production data servers within the SaaS hosted environment. The Windows operating systems have been "hardened" beyond the default configurations using a standard image for deployment which has been hardened, based on management's risk assessment of the Windows OS version. Only necessary ports and services are enabled. The IBM I Operating Systems have been "hardened" beyond the default configuration using a standard image for deployment which has been hardened, based on management's risk assessment of the IBM OS version. Only necessary ports and services are enabled. The IT Security Policy includes security standards and allowable conduct for the prevention of unauthorized access from non-approved networks, and user provisioning is set at the minimum required level.	Inspected the servers in production to determine all servers were running vendor-supported versions of the operating systems. Inspected the configuration standard template to determine that the IBM and Windows operating systems were hardened beyond the default configuration and that only necessary ports and services were enabled. Inspected the IT Security Policy to determine that the policy references the prevention of unauthorized access and user provisioning.	No Exceptions Noted

Common Criteria – Logical Access			
CC-5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.		
	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CC-5.1.02	**Access Granted**		
	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-5.1.03	**Active Directory Authentication – User ID**		
	All users are assigned a unique username, user ID and initial password to authenticate to the Windows Active Directory server allowing access to CGC resources.	Inspected Active users and groups to determine that unique user account existed.	No Exceptions Noted
CC-5.1.04	**Password Management**		
	Password controls are technically enforced for length and change frequency. User accounts are locked after a specified number of unsuccessful attempts and remain locked for a predetermined time or until reset by ICS staff.	Inspected password configuration requirements within AD to determine technical enforcement of password controls was enabled and user accounts locked after a specified number of unsuccessful attempts.	No Exceptions Noted

CC-5.1.05	**Password Reset Procedures**		
	ICS Staff has primary responsibility for system account management including password resets. Authorized ICS staff performs account password resets in Windows Active Directory and internal iSeries development servers.	Inspected iSeries password request for a development server to determine access to password resets was restricted to ICS staff.	No Exceptions Noted
CC-5.1.06	**Local Administrator Account(s)**		
	Server(s) Only accounts defined on the Windows server for hosted systems is a local administrator account. Local security officer privileges for iSeries server(s) within the hosted environment are assigned to individuals within IT based on business need and management approval.	Inspected Active Directory Domain Administrators to determine that access was assigned to ICS Staff personnel and additional Directors as required Inspected password configuration requirements within AD to determine technical enforcement was enabled.	No Exceptions Noted
CC-5.1.07	**Database(s) Access Controls**		
	Access to iSeries DB2 database(s) requires the user to enter a valid iSeries username and password. Users authorized to access the database are limited to the database administrator and ICS.	Inspected the list of users authorized to access iSeries DB2 to determine that access was restricted to database administrators and ICS.	No Exceptions Noted
CC-5.1.08	**Source Code Management Application(s) Access Controls**		
	Access to source code management application(s) is dependent on iSeries credentials. Users authorized to access source code are limited to developers and the Software Delivery Team.	Inspected the listing of users with access to source code management to determine access was limited to Software Delivery Team. Observed unauthorized user attempt to login to determine an error message was received.	No Exceptions Noted

CC-5.1.09	**Network(s) Access Controls**		
	ICS Staff has sole control over the configuration and provisioning of network assets. Access to networks is based on Active Directory credentials. Network configuration is performed solely by the ICS staff.	Inspected Active Directory Domain Administrators to determine that access was assigned to ICS personnel. Inspected Windows policy to determine password controls are technically enforced.	No Exceptions Noted
CC-5.1.10	**Communications Equipment & /Security Device(s)**		
	The CGC internal network firewalls are managed by the ICS Team.	Inspected the internal environment access listing to determine that access was assigned to ICS personnel.	No Exceptions Noted
CC-5.1.11	**Workstation(s) Access Controls**		
	Workstations are CGC owned and configured. Access to the desktop or laptop requires valid Active Directory credentials. Workstations lock after a specified period approved by management and require the user to enter valid credentials to unlock the workstation.	Observed an authorized user attempt to login to determine that access was granted after valid credentials were entered. Observed an authorized user attempt to login to determine that access was granted to unlock a lock workstations after valid credentials were entered. Inspected Windows policy to determine controls were technically enforced.	Exception Noted: The screen saver timeout was set to a different time than stated in the policy.
CC-5.1.12	**SaaS Environment Access - VPN**		
	An IPSEC VPN tunnel controls access to the eCMS SaaS Partner environment by CGC staff to the hosting partner data center. Users are then required to authenticate to specific systems using a valid username and password. All access to the SaaS servers occurs over site-to-site IPSEC VPN tunnels or HTTPS SSL access.	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

Common Criteria – User Account Administration

CC-5.2 New internal and external system users are registered and authorized prior to being issued system credentials and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-5.2.01	**User Account(s) - New**		
	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. Only authorized staff within ICS have been assigned privileges to create user accounts and related permissions.	Inspected New User Request e-mail from the Controller for a selection of hires to determine that approval was obtained from CGC management to grant access. Inspected Active Directory Domain Administrators to determine that access was assigned to ICS personnel	No Exceptions Noted
CC-5.2.02	**User Account(s) - Changes**		
	Requests to change existing user access are first approved by the department manager and then reviewed by ICS.	Inquired of management to determine whether any requests to changes existing access were made during the reporting period.	No changes request were made during the reporting period. As a result, no testing was performed.
CC-5.2.03	**User Account(s) – Disable / Delete**		
	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 documentation for the terminated users during the period to determine that passwords were changed upon notification.	No Exceptions Noted

CC-5.2.04 User Account Periodic Validation		
Semi-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 a sample of semi-annual reviews in the period to determine that access reviews were completed and documented.	No Exceptions Noted

Common Criteria – User Identity Management

CC-5.3 Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CROSS REFERENCE – Previously Defined Controls		
CC-1.2.03 **Policy Statements**	Refer to CC-1.2.03 **Policy Statements**	No Exceptions Noted
CC-5.1.04	Refer to CC-5.1.04	No Exceptions Noted
CC-5.3.01 Password Reset Procedures	**CC-5.3.02 Password Reset Procedures**	
CC-5.1.06 **Local Administrator Account(s)**	Refer to CC-5.1.06 **Local Administrator Account(s)**	No Exceptions Noted
CC-5.1.11 **Workstation(s) Access Controls**	Refer to CC-5.1.11 **Workstation(s) Access Controls**	No Exceptions Noted
0	Refer to 0	No Exceptions Noted
CC-5.3.03 User Account Periodic Validation	**CC-5.3.04 User Account Periodic Validation**	

Common Criteria – Segregation of Duties

CC-5.4 Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CROSS REFERENCE – Previously Defined Controls		
CC-1.2.03 **Policy Statements**	Refer to CC-1.2.03 **Policy Statements**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted
CC-5.1.07 **Database(s) Access Controls**	Refer to CC-5.1.07 **Database(s) Access Controls**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted
0 **CC-5.4.01 Network(s) Access Controls**	Refer to 0 **CC-5.4.02 Network(s) Access Controls**	No Exceptions Noted
CC-5.1.11 **Workstation(s) Access Controls**	Refer to CC-5.1.11 **Workstation(s) Access Controls**	No Exceptions Noted
Error! Reference source not found. Organization Structure	Refer to **Error! Reference source not found. Organization StructureError! Reference source not found.**	No Exceptions Noted
CC-5.2.01 **User Account(s) - New**	Refer to CC-5.2.01 **User Account(s) - New**	No Exceptions Noted
CC-5.2.02 **User Account(s) - Changes**	Refer to CC-5.2.02 **User Account(s) - Changes**	No Exceptions Noted
0 **CC-5.4.03 User Account Periodic Validation**	Refer to 0 **CC-5.4.04 User Account Periodic Validation**	No Exceptions Noted

Common Criteria – Physical Access

CC-5.5 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-5.5.01 Entrances		
CGC office space is controlled by electronic security cards and are locked during non-business 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 non-business hours.	No Exceptions Noted
CC-5.5.02 Electronic Security Card – Issuance		
Employees who need access to the CGC office space are issued electronic key cards.	Inspected CGC Asset Forms for the new hires in the period to determine that access cards issued to new hires were documented.	No Exceptions Noted:

Common Criteria – External Logical Access			
CC-5.6	Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.		
	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CROSS REFERENCE – Previously Defined Controls			
	CC-5.1.12 **SaaS Environment Access - VPN**	Refer to CC-5.1.12 **SaaS Environment Access - VPN**	No Exceptions Noted
CC-5.6.01	**Standards**		
	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.	No Exceptions Noted
CC-5.6.02	**Wi-Fi - Employees**		
	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-5.6.03	**Wi-Fi – Visitors**		
	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-5.6.04	**Firewall(s)**		
	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.	No Exceptions Noted
CC-5.6.05	**Server & Workstation Patching**		
	WSUS is used for server and workstation operating system patches. Updates are pushed daily to CGC workstations and servers. iSeries patches are installed as required by IBM.	Inspected the configuration of WSUS to determine that Windows servers and workstation patches were applied.	No Exceptions Noted
		Inquired of management to determine whether there were any required security patches for iSeries servers during the reporting period.	No iSeries security patches during the reporting period. As a result, no testing performed.

Common Criteria – Data Transmission / Transfer [Movement]

CC-5.7 The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal enabling the entity to meet its commitments and system requirements as they relate to security, availability, and confidentiality.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-5.7.01	**Private Communications**		
	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. CGC employees access the internal network via an encrypted VPN connection.	Observed the logon process to determine that a connection was established using a company-provided device using a VPN client. Inspected the Client VPN configuration to determine that a IP Sec tunnel with a valid certificate was required to establish a connection.	No Exceptions Noted

Common Criteria – Data Transmission / Transfer [Movement]

CC-5.7 The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal enabling the entity to meet its commitments and system requirements as they relate to security, availability, and confidentiality.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-5.7.02 External Connectivity		
Customers access their hosted environment via a site-to-site IPSEC VPN tunnel or a web interface using HTTPS.	Inspected system generated documentation to determine that access to the Hosting Services environment by client users was through a site-to-site dedicated VPN tunnel, or via a web browser using HTTPS.	No Exceptions Noted

Common Criteria – Unauthorized / Malicious Software

CC-5.8 Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security, availability, and, confidentiality..

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-5.8.01 Anti-Virus Software - Installation		
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-5.8.02 Anti-Virus Software – Updates		
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-5.8.03 Software Installation		
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

SYSTEM(s) OPERATIONS – Common Criteria Related to System(s) Operation

CC-6.0 System Operations

The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.

Common Criteria – Vulnerabilities

CC-6.1 Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CROSS REFERENCE – Previously Defined Controls		
0 **CC-6.1.01 Vulnerability Scans**	Refer to 0 **CC-6.1.02 Vulnerability Scans**	No Exceptions Noted
CC-5.1.03 **Active Directory Authentication – User ID**	Refer to CC-5.1.03 **Active Directory Authentication – User ID**	No Exceptions Noted
CC-5.1.04 **Password Management**	Refer to CC-5.1.04 **Password Management**	No Exceptions Noted
0 **CC-6.1.03 Password Reset Procedures**	Refer to 0 **CC-6.1.04 Password Reset Procedures**	No Exceptions Noted

Common Criteria – Vulnerabilities

CC-6.1 Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
0	Refer to 0	No Exceptions Noted
CC-6.1.05 Firewall(s)	**CC-6.1.06 Firewall(s)**	
CC-5.8.01 **Anti-Virus Software - Installation**	Refer to CC-5.8.01 **Anti-Virus Software - Installation**	No Exceptions Noted
CC-5.8.02 **Anti-Virus Software – Updates**	Refer to CC-5.8.02 **Anti-Virus Software – Updates**	No Exceptions Noted
CC-6.1.07 Logging & Monitoring Software		
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. ICS staff is notified of events that impact the security or availability of systems or the confidentiality of data.	Inspected system logs generated from the network monitoring tool to determine that activity was logged and available for review and was used as the basis for generating alerts. 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.	No Exceptions Noted

Common Criteria – Incident Management			
CC-6.2	Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel, and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.		
	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CC-6.2.01	**Incident Response Protocol**		
	CGC employees follow defined protocols for evaluating and escalating reported events. Security related events are assigned to the ICS group for evaluation. Hosting Partner is responsible for communicating security breaches to CGC.	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.	No Exceptions Noted
		Inquired of management to determine whether there were any security incidents in the reporting period.	No security-related incidents occurred during the reporting period. As a result, no testing performed.
CC-6.2.02	**Incident Logged**		
	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.	No security-related incidents occurred during the reporting period. As a result, no testing performed.
CC-6.2.03	**Incident Status**		
	Customers can check the status of incidents directly via the self-service web portal.	Observed ticketing system to determine that the system allowed the customer to view the customer related tickets.	No Exceptions Noted

CC-6.2.04	**Incident Escalation**		
	Incidents are monitored live by all departments. Beginning in February of 2018, the Director of ICS generates a weekly report to give ticket metrics to the President of CGC.	Inspected weekly reports and emails to the President for a selection of weeks since February 2018 in the period to determine that ticket metrics were documented and communicated to the President of CGC.	No Exceptions Noted
CC-6.2.05	**Noncompliance with policies**		
	CGC employees are instructed to contact management regarding any issues that deviate from normal operating procedure and/or are not specifically addressed in CGC policy statements or the Employee Handbook.	Inspected the Employee Handbook to determine that language existed for noncompliance.	No Exceptions Noted

CHANGE MANAGEMENT – Common Criteria Related to Change Management

CC-7.0 Change Management

The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.

Common Criteria – System Development Lifecycle

CC-7.1 The entity's commitments and system requirements, as they relate to security, availability, and confidentiality are addressed during the system development lifecycle including authorization, design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-7.1.01	**System Development Lifecycle**		
	System Development Lifecycle controls were not in scope for this examination.	Not applicable	Not applicable

Common Criteria – System Updates

CC-7.2 Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security, availability, and confidentiality.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
CC-7.2.01	**Infrastructure Changes – Authorization and Implementation**		
	All infrastructure changes are initiated, authorized, and tracked in the incident management system.	Inspected tickets for a selection of eCMS Incident Tickets from a list of changes during the reporting period to determine that changes were initiated, authorized, and tracked in the incident management system.	No Exceptions Noted
CC-7.2.02	**Source Code**		
	Changes to the eCMS application within the Hosting Partner Environment require approval from the Software Delivery Manager.	Inspected documentation for selection of Rocket Aldon Lifecycle Manager Change Tickets that from a list of changes during the reporting period to determine that changes had been documented, tested and approved by the Software Delivery Manager prior to being promoted to the Hosted Environment for the eCMS application.	No Exceptions Noted
CC-7.2.03	**Change Testing**		
	Any changes to the hosted environment are tested prior to promoting to production. CGC is responsible for the testing of the changes.	Inspected documentation to determine that the document identified approved changes to the hosting environment by data center during the reporting period Inspected documentation for a selection of eCMS Incident Tickets from a list of changes during the reporting period to determine changes had been tested and approved by the PMO prior to being promoted to the Hosted Environment for the eCMS application.	No Exceptions Noted

Common Criteria – System Design/Control Effectiveness Deficiencies		
CC-7.3 Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.		
Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CROSS REFERENCE – Previously Defined Controls		
CC-7.2.01 **Infrastructure Changes – Authorization and Implementation**	Refer to CC-7.2.01 **Infrastructure Changes – Authorization and Implementation**	No Exceptions Noted
Error! Reference source not found. Error! Reference source not found.	Refer to **Error! Reference source not found. Error! Reference source not found.**	No Exceptions Noted
CC-7.2.02 **Source Code**	Refer to CC-7.2.02 **Source Code**	No Exceptions Noted

Common Criteria – Change Management Procedures		
CC-7.4 Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.		
Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CROSS REFERENCE – Previously Defined Controls		
CC-7.2.01 **Infrastructure Changes – Authorization and Implementation**	Refer to CC-7.2.01 **Infrastructure Changes – Authorization and Implementation**	No Exceptions Noted
CC-7.2.02 **Source Code**	Refer to CC-7.2.02 **Source Code**	No Exceptions Noted

CC-7.4.01	**Change Management Procedures**		
	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 tickets for a selection of eCMS Incident Tickets from a list of changes during the reporting period to determine changes had been tested and approved by the PMO prior to being promoted to the Hosted Environment for the eCMS application. Inspected a selection of eCMS Incident Tickets from a list of changes during the reporting period to determine that changes were identified as either having an impact on service levels or having no impact on service levels.	No Exceptions Noted
CC-7.4.02	**Change Management Environments**		
	CGC has established an environment separate from production for design and testing purposes for critical infrastructure	Inspected system generated documentation to determine that separate environment existed.	No Exceptions Noted
CC-7.4.03	**Production Access**		
	CGC has established an environment separate from production for design and testing purposes.	Inspected system generated documentation to determine that separate environment existed.	No Exceptions Noted
	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

CC-7.4.04	**Change Management Emergency Changes**		
	Emergency changes follow the same procedures as scheduled changes. Emergency eCMS application changes follow the same procedures as scheduled changes with the exception that they are delivered manually for promotion to production rather than waiting for the next scheduled package release.	Inspected procedures to determine that emergency changes procedures are the same procedures as scheduled changes. Inquired of the Application Change Management Specialist regarding the emergency change process for the eCMS application to determine that structured procedures existed for handling emergency changes.	No Exceptions Noted No emergency changes were noted in the reporting period. As a result, no testing performed.

Availability Trust Principle – Additional Criteria

AVAILABILITY – Additional Criteria Specific to the Availability Principle	
A-1.0	**Availability** Additional Criteria Specific to the Availability Principle

Availability Criteria – Capacity	
A-1.1	Current processing capacity and usage are maintained, monitored and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.

	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
A-1.1.01	**Capacity Monitoring**		
	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 the monitoring system configuration to determine that alerting and communication were defined when performance thresholds had been exceeded. Inspected an alert message from the monitoring system to determine that alerts were produced after a threshold was exceeded.	No Exceptions Noted
A-1.1.02	**Infrastructure review**		
	CGC provides redundancy in their support design and server and network platforms to meet SLA requirements.	Inspected the Network System Diagram to determine that CGC provided redundancy in the support design and server and network platforms to meet SLA requirements.	No Exceptions Noted

A-1.1.03	**Future Planning**		
	Future processing capacity demand is evaluated by ICS Team during weekly and bi-weekly meetings, including but not limited to: • Internet connectivity • Network bandwidth • CPU • Disk • RAM • Server failover • Switches / Routers • Firewalls	Inspected the calendar for a selection of weeks and months during the period to determine that the ICS Staff had regularly-scheduled weekly and bi-weekly meetings during which future processing capacity demand is addressed by the team. Inspected the weekly report the Director of ICS sends to the President to determine that system metrics, including future capacity, was included as a result of the weekly and bi-weekly team meetings.	No Exceptions Noted

Availability Criteria – Environmental Protection

A-1.2 Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.

	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
A-1.2.01	**Access to Backup**		
	Backups are stored on dedicated physical backup servers with access limited to the ICS Team.	Inspected the Network Diagram to determine that backups were stored on dedicated physical backup servers. Inspected list of users with access to offline storage, backup data, systems, and media to determine that access was based on number and job function to determine access was restricted to ICS individuals.	No Exceptions Noted
A-1.2.02	**Backup Monitoring**		
	An automated backup system is used to monitor replication and backup jobs for any failure.	Inspected the configuration of the automated backup system to determine the system monitored for failures.	No Exceptions Noted

A-1.2.03	**Backup Methodology**		
	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.	Inspected Windows Task Scheduler to determine that rSync runs daily to copy image files not stored in the database. Inspected iSeries job scheduler to determine that database backups execute nightly and were sent via FTP to the backup server.	No Exceptions Noted
A-1.2.04	**Multi-location Strategy**		
	CGC maintains dual data centers to facilitate disaster recovery.	Inspected the network diagram to determine that a multi-location strategy was being utilized.	No Exceptions Noted

Availability Criteria – System Recovery

A-1.3 Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
A-1.3.01	**System Restore(s)**		
	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

A-1.3.02	**Business Continuity / Disaster Recovery Plan(s) Tests**		
	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
A-1.3.03	**Test Results**		
	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

Confidentiality Trust Principle – Additional Criteria

CONFIDENTIALITY – Additional Criteria Specific to the Confidentiality Principle	
C-1.0	**Confidentiality** Additional Criteria Specific to the Confidentiality Principle

Confidentiality Criteria – Protection of Data in Non-Production Environments	
C-1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.

	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
C-1.1.1	**Data in Non-Production**		
	Not applicable as client confidential information is not used during the system development, testing, and change process.	Not Applicable	Not Applicable

Confidentiality Criteria – Access to Data During Processing or System Output	
C-1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, out-put, and disposition in accordance with confidentiality commitments and requirements.

	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
CROSS REFERENCE – Previously Defined Controls			
	CC-5.1.03 **Active Directory Authentication – User ID**	Refer to CC-5.1.03 **Active Directory Authentication – User ID**	No Exceptions Noted
	CC-5.1.07 **Database(s) Access Controls**	Refer to CC-5.1.07 **Database(s) Access Controls**	No Exceptions Noted

C-1.2.1	**Client Data**		
	By administrative policy, CGC prohibits employees from storing client-supplied data on desktop or laptop workstations or to provide to any third-party entity.	Inspected the IT Security Policy to determine that storing locally or sharing client-supplied data was prohibited.	No Exceptions Noted

Confidentiality Criteria – Access to Data Beyond System Boundaries

C-1.3 Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
C-1.3.1	**Data Transmission**		
	Contracts between clients and CGC prohibit CGC from sharing or transmitting information.	Inspected agreements with clients for a sample of new hosted clients in the period to determine verbiage related to data transmission was contained within the document.	No Exceptions Noted

Confidentiality Criteria – Handling of Data by Related Party or Vendor Personnel

C-1.4 The entity obtains confidentiality commitments that are consistent with the entity's confidentiality requirements from vendors and other third parties whose products and services comprise part of the system and have access to confidential information.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
C-1.4.1	**Sharing of data**		
	CGC client data is not shared or disclosed with any third party unless required by law as outlined in the contractual agreement between CGC and client user organization.	Inspected the IT Security Policy to determine that client data was prohibited from being shared or disclosed with any third party.	No Exceptions Noted

Confidentiality Criteria – Vendor's Control Environment

C-1.5 Compliance with confidentiality commitments and requirements by vendors and others third parties whose products and services comprise part of the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
C-1.5.1	**Vendor's Access**		
	The Data Centers' SOC2 reports are obtained and reviewed by CGC's Director of ICS to determine if the Service Auditor's Opinion provided assurance that controls were described accurately, the design of controls was adequate for the operational environment of the vendor, and the controls operated effectively during the reporting period.	Inspected the Data Center's SOC reports as provided by the Director of ICS to determine that the most recent SOC2 from the Data Centers had been reviewed.	No Exceptions Noted

Confidentiality Criteria – Practices and Commitments

C-1.6 Changes to confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are included in the system.

	Controls Specified by Computer Guidance Corporation, Inc.	Test(s) of Controls Performed by CliftonLarsonAllen LLP	Results of Test(s)
C-1.6.1	**Confidentiality Practices**		
	The President and Director of ICS is responsible for approving changes to confidentiality practices and commitments.	Inquired of CGC management to determine responsibility and accountability for approving changes to confidentiality practices and commitments was the responsibility of the President and Director of ICS. Inquired of CGC management to determine whether any changes to confidentiality practices and commitments were changed during the period under review.	No changes to confidentiality commitments were noted. As a result, no testing performed.

C-1.6.2	**Communication**		
	A formal process is used to communicate changes to users, related parties, and vendors.	Inquired of CGC management to determine procedures had been established for CGC to notify client user organizations of scheduled changes if the changes have the potential of impacting the security or availability of the eCMS application or underlying infrastructure. Inquired of CGC management to determine whether any changes to confidentiality practices and commitments were changed during the period under review.	No changes to confidentiality commitments were noted. As a result, no testing performed.

Confidentiality Criteria – Data Retention

C-1.7 The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.

	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
C-1.7.1	**Data Retention**		
	Data is retained for a period of time according to the SAAS DR Data Sheet.	Inspected the SAAS DR Data Sheet and evidence of backups performed to determine that data was backed up and maintained.	No Exceptions Noted

Confidentiality Criteria – Data Disposal			
C-1.8	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.		
	Controls Specified by Computer Guidance Corporation, Inc.	**Test(s) of Controls Performed by CliftonLarsonAllen LLP**	**Results of Test(s)**
C-1.8.1	**Technology Asset Destruction**		
	Any devices containing client data are destroyed prior to disposal in a secure manner consistent with industry best practices.	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.	No devices containing client data were destroyed during the reporting period. As a result no testing was period.