HANDS-ON LABS SCIENCE DELIVERED

GENERAL CONTROLS SUPPORTING THE SCIENCE DISTANCE LEARNING SOLUTIONS

SOC 2 - Type II Audit Report

Independent Service Auditor's Report on Controls Placed in Operation Relevant to the Trust Services Categories of Security, Availability, and Confidentiality

For the Period September 1, 2020 to August 31, 2021

INDEPENDENT SERVICE AUDITOR'S REPORT

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

The Moore Group, CPA
SOC Audit Specialists

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality

To: Science Interactive Group,

Scope

We have examined Science Interactive Group's (SIG) accompanying description of the general controls supporting its science distance learning solutions and systems found in Section 3 titled "Description of the Service Organization's System Provided by SIG Management" (description) throughout the period September 1, 2020 to August 31, 2021 based on the criteria for a description of a service organization's system set forth in *DC 200*, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 1, 2020 to August 31, 2021, to provide reasonable assurance that SIG'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 100*, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

SIG uses a third party data center (subservice organization) to house its critical production computer servers, applications and networking equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SIG, to achieve SIG's service commitments and system requirements based on the applicable trust services criteria. The description presents SIG's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of SIG's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

The information in Section 5, "Other Information Provided by the Service Organization" that describes management's responses to testing exceptions, is presented by the management of SIG to provide additional information and is not a part of SIG's description of the general controls supporting its science distance learning solutions and systems made available to user entities during the period September 1, 2020 to August 31, 2021. SIG's responses have not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on them.

Service Organization's Responsibilities

SIG 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 SIG's service commitments and system requirements were achieved. In Section 2, SIG has provided its assertion titled "Assertions by the Service Organization's Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. SIG 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 Auditor's Responsibilities

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

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

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

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, titled "Testing Matrices" of this report.

Opinion

In our opinion, in all material respects —

a. the description presents SIG's science distance learning solutions and systems that was designed and implemented throughout the period September 1, 2020 to August 31, 2021 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period September 1, 2020 to August 31, 2021 to provide reasonable assurance that SIG's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of SIG's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period September 1, 2020 to August 31, 2021 to provide reasonable assurance that SIG's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of SIG's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of management of SIG; user entities of SIG's science distance learning solutions and systems during some or all of the period September 1, 2020 to August 31, 2021; business partners of SIG subject to risks arising from interactions with the science distance learning solutions and systems; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.

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

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

The Moore Group CPA, LLC

Nashua, NH
November 4, 2021

SECTION 2

ASSERTIONS BY THE SERVICE ORGANIZATION'S MANAGEMENT

MANAGEMENT ASSERTION OF SCIENCE INTERACTIVE GROUP

The Moore Group CPA, LLC
Nashua, NH 03060

We have prepared the accompanying description of Science Interactive Group's (SIG) general controls supporting the science distance learning solutions and systems titled "Description of the Service Organization's System Provided by SIG Management" throughout the period September 1, 2020 to August 31, 2021 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, (description criteria). The description is intended to provide report users with information about the science distance learning solutions and systems that may be useful when assessing the risks arising from interactions with SIG's system, particularly information about system controls that SIG has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

SIG uses a third party data center (subservice organization) to house its critical production computer servers, applications and networking equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SIG, to achieve SIG's service commitments and system requirements based on the applicable trust services criteria. The description presents SIG's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of SIG'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 SIG, to achieve SIG's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

1) The description presents SIG's general controls supporting the science distance learning solutions and systems that was designed and implemented throughout the period September 1, 2020 to August 31, 2021 in accordance with the description criteria.

2) The controls stated in the description were suitably designed throughout the period September 1, 2020 to August 31, 2021 to provide reasonable assurance that SIG's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of SIG's controls throughout that period.

3) The controls stated in the description operated effectively throughout the period September 1, 2020 to August 31, 2021 to provide reasonable assurance that SIG's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of SIG's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM PROVIDED BY SIG MANAGEMENT

DESCRIPTION OF CONTROLS PLACED IN OPERATION

OVERVIEW OF OPERATIONS

Company Background

Founded in 1994, Science Interactive Group (SIG) is a world leader in science distance learning, regardless of location, time zone, or language. SIG's cutting-edge lab kits are self-contained learning portals that allow instructors and students to collaborate anytime, anywhere. SIG produces online science lab kits that include modern pedagogy, cloud-based learning platforms, and hands-on lab experiments that mirror the classroom laboratory. Headquartered in Englewood, Colorado, SIG produces more than 250 lab kits in 11 science disciplines.

Scope of SOC Audit

The scope of this SOC audit includes an assessment of the general organizational and information technology controls supporting the science distance learning solutions and systems of SIG. The scope does not include an assessment of any banking, fraud protection, cash receipts/payments, accounting, or other internal or external financial responsibilities of SIG.

Description of Services Provided

SIG's science kits are self-contained college level lab kits that offer more than 350 pre-planned lessons in the following disciplines:

- Anatomy & Physiology
- Biology
- Chemistry
- Environmental Science
- Forensic Science
- Geology
- GOB (General-Organic-Bio) Chemistry
- Microbiology
- Physics
- Instructor Info Request

SIG's lab kits contain experiments and lab-grade equipment that mirror the traditional campus laboratory experience in a distance learning setting. SIG has helped nearly one-third of all U.S. colleges and universities across the country to take their science courses online. SIG combines the concierge-style package delivery of at-home convenience with a perfectly-tailored curriculum designed by teachers, for teachers, at every grade level. Students perform their work in the SIG Cloud, an interactive, accessible environment that provides automatic grading, analytics, and is fully configurable to a teacher's specific requirements. SIG offers an all-in-one solution with lab kits containing all the laboratory equipment and lab content needed for an entire semester of study.

Principal Service Commitments and System Requirements

SIG makes service commitments to its customers and has established system requirements as part of the science distance learning solutions service. Some of these commitments are principal to the performance of the service and relate to the applicable trust services criteria. SIG 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 SIG's service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in SIG's policies and procedures, system design documentation, customer agreements, or other written company materials provided to user entities as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- Security: SIG has made commitments related to a secure information technology control environment and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security, and other relevant security controls.

- Availability: SIG has made commitments related to providing reliable and consistent uptime and connectivity for the IT systems used in the services offered by SIG. These commitments include, but are not limited to, design, development or acquisition, implementation, monitoring, and maintaining environmental protection of systems, software, data back-up processes, and recovery infrastructure to meet availability commitments.

- Confidentiality: SIG has made commitments related to maintaining the confidentiality of customers' data through data classification policies, data encryption and other relevant security controls.

SIG has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in its system policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various SIG services.

Components of the System

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the description of services and the components of infrastructure, software, people, procedures, and data.

The components of the system used to provide the services are as follows:

Infrastructure

SIG's main corporate office is located in Englewood, CO. A proximity card security system is utilized by SIG, with variable rights granted for the office space, sensitive areas and server room. The security system is maintained by the building management company.

Subservice Organization – For data center services, SIG utilizes the third party data center services of Amazon Web Services. The scope of this audit report does not include the controls of AWS. Amazon had a SOC 1, SOC 2, and SOC 3 report completed for the review period October 1, 2020 to March 31, 2021.

The server and network hardware layer is managed by Amazon. The Virtual Private Cloud network (i.e., logical administrative access to creating/moving production servers) is managed by SIG via IAM (Identity and Access Management). Internal SIG administrative access to servers is made via Linux shell/root authentication using SSH keys.

SIG's EC2 web servers are backed up using a third-party software offering by Cloudberry. The backup files are archived on independent storage for resiliency in the event of an outage or degradation of primary production environment.

Production databases are housed in Amazon's RDS (Relation Database Service), using Amazon's MySQL offering.

Amazon CloudWatch is utilized by SIG for monitoring system performance and notifying of events out of prescribe thresholds.

Computer operations generally may be threatened with downtime in several areas:

- Equipment failure
- Catastrophic event
- Attack

To mitigate these risks, SIG has implemented controls to mitigate these risks, including:

- Equipment maintenance contracts
- Systems redundancy
- Network redundancy
- Power redundancy
- Firewalls
- AV software
- OS and critical application patches

Environmental controls include but are not limited to fire detection and wet pipe sprinkler systems throughout the corporate facility. UPS systems provide up to 15 minutes of power in the event of disruption of the main power feed, allowing for gradual, safe shutdown of critical computer systems. Redundant architecture is in place, including:

- Redundant servers for critical systems
- Network interface cards (NICs)
- Power supplies
- RAID storage.

Servers and workstations utilize anti-virus endpoint protection, which is kept properly updated and conducts routine scans. Windows Server and Linux operating system patches for critical production systems are updated manually to ensure adequate testing and that no production interference will result. Other servers and workstations are automatically updated via Windows Update Service.

Software

A combination of custom developed and commercial applications is utilized to support the services provided to user organizations. The applications run on Windows Server 2008R2 and above, Linux and enterprise grade server hardware platforms with commercial databases to support the applications. These software applications include:

- Spiceworks
- SharePoint
- Sophos

People

SIG is led by its CEO, Tim Loomer, and executives in the departmental areas of Operations, Finance, and Sales and Marketing. SIG's organization structure provides the overall framework for planning, directing, and controlling operations. Personnel and business functions are separated into departments according to job responsibilities. The structure provides defined responsibilities and lines of authority for reporting and communication. The assignment of roles and responsibilities within the various departments provides effective segregation of duties.

In the Control Environment section of this report, additional information is described related to organizational controls implemented at SIG. These organizational controls are intended to serve as the internal foundation for providing services to its customers.

Procedures

SIG has implemented processes and procedures to support the operations and controls over the services and systems provided to its customers. Specific examples of the relevant procedures include, but are not limited to, the following:

- Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.
- Security policies are in place to guide personnel regarding physical and information security practices.
- Policies and procedures are in place for identifying the system security requirements of authorized users.
- Third party enterprise monitoring applications are used to monitor system downtime and operations issues, which are monitored to help ensure that system downtime and performance does not exceed predefined levels.
- Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.
- Policies and procedures are in place to assign responsibility and accountability for system changes and maintenance.
- Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.
- Management utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion into the production environment. The IPS subscription for the firewall system is kept current.
- Firewall systems are in place to screen data flow between external parties and the SIG network.
- Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.
- Production server users are required to authenticate via a unique user ID and password before being granted access to the production environment.

- Application users are required to authenticate via an authorized unique user ID and password before being granted access to the production environment.
- Physical security policies and procedures are in place to guide personnel regarding restricting access to the facility.
- Intrusion and motion alarm systems are in place and monitored for all entry/exit points of the facility, including doors and windows. An audible alarm sounds upon triggering.
- Third party antivirus protection is installed at the network perimeter firewalls to mitigate exposure to virus attacks on the production equipment (perimeter protection).
- Management periodically performs internal security assessments, including reviews of server logs and other critical items.
- Policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.
- Policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.

Data

Access to data is limited to authorized personnel in accordance with SIG's system security policies. SIG is also responsible for the overall availability of data, including system backups, monitoring of data processing, and file transmissions as well as identifying and resolving problems.

For backups of critical company data, differential backups are taken on a daily basis by a third party backup service. Weekly full backups are also performed for all critical company data such as critical application and database components. The backup files are retained for a minimum of 45 days. Logs are kept to ensure backup processes are monitored for proper completion.

Encryption is utilized to protect data in transit, including SSL encryption over HTTPS connections utilized for secure communications between SIG and customer end users. Certain IT engineers access production server and data stored at the third party data center remotely, via secure portals protected by SSL encryption.

Controls in place specific to the data responsibilities of SIG include, but are not limited to, the following:

- Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Firewall systems are in place to screen data flow between external parties and the SIG network.
- A secure VPN (Virtual Private Network) connection is used for remote external access to the internal network by authorized SIG employees.
- Site-to-site VPN tunnels are locked down to specific locations via an access control list. IPsec network layer encryption is utilized.
- Policies and procedures are in place to guide personnel regarding sharing information with third parties.
- Transaction processing performed on web-based applications is secured through the use of the Secure Socket Layer (SSL) encryption protocol over HTTPS connections.
    - This includes the use of the website file upload page.
    - Traffic directed to HTTP connections for this are redirected to HTTPS connections.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of SIG's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of SIG's ethical and behavioral standards, how they are communicated, and how they are reinforced in daily practice.

These standards include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, and by personal example.

Specific control activities that SIG has implemented in this area are described below.

- SIG maintains an employee handbook which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.
- Policies and procedures require that new employees sign an employee handbook acknowledgment form indicating that they have been given access to it and understand their responsibilities. The signed form is kept in the employee personnel file.
- Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Comprehensive background checks are performed by an independent third party for certain positions as a component of the hiring process.
- *Contract employees (1099)* must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Comprehensive background checks are performed by an independent third party for *contract employees (1099)* as a component of the hiring process.
- Management maintains a commercial general liability insurance policy which includes technology/professional errors and omissions coverage and/or employee dishonesty.

Commitment to Competence

SIG's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. SIG's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

Specific control activities that SIG has implemented in this area are described below.

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written job descriptions.
- Candidates' abilities to meet job requirements are evaluated as part of the hiring, performance review, and transfer evaluation processes.
- Roles and responsibilities for company personnel to interact with and monitor the activities of external third party information technology vendors are defined in written job descriptions and communicated to personnel.
- Management has developed a training and development program for employees. This includes:
    - Initial training/orientation with peers and supervisors in the period immediately after hire.
- Management encourages employees to complete and continue formal education and technical certification programs. (formally or informally)
- Certain approved professional development expenses incurred by the employees are paid by SIG. (training certs, classes, etc.)
- Employees undergo an annual performance review which includes discussions related to their performance related to internal control responsibilities such as data and systems security. A formal evaluation is prepared and is maintained in the employee's HR file.
- SIG utilizes an independent CPA firm to compile its financial statements and prepare tax returns.

Board of Directors' Participation

SIG's control consciousness is influenced significantly by its Board of Directors participation. The Board of Directors oversees management activities and meets quarterly to discuss strategic, operational, and compliance issues. The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.

Management's Philosophy and Operating Style

SIG's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward the science distance learning solutions, information processing, accounting functions and personnel. Management is periodically briefed on regulatory and industry changes affecting services provided. Management meetings are held on a periodic basis to discuss and monitor operational issues.

Specific control activities that SIG has implemented in this area are described below.

- Management regularly attends trade shows, utilizes trade and regulatory publications, journals, online news feeds and government sites, and belongs to industry associations to stay current on regulatory compliance or operational trends affecting the services provided.
- Operational meetings are held on a regular basis to discuss internal control responsibilities *(data and system security)* of individuals and performance measurement.
- SIG utilizes an independent CPA firm to compile its financial statements and prepare tax returns.

Organization Structure and Assignment of Authority and Responsibility

SIG's organization structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. SIG's management believes that establishing a relevant organization structure includes considering key areas of authority and responsibility and appropriate lines of reporting. SIG has developed an organization structure suited to its needs. This organization structure is based, in part, on its size and the nature of its activities.

SIG's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that all personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that SIG has implemented in this area are described below.

- Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.

Human Resource Policies and Practices

SIG's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that SIG has implemented in this area are described below.

- Management utilizes a new hire checklist to ensure that specific elements of the hiring process are consistently executed. A copy of the checklist is kept in the employee file.
- A formal process is in place to ensure HR informs IT when employee access to company IT resources needs to be added or removed.
- Comprehensive background checks are performed by an independent third party for certain positions as a component of the hiring process.
- Comprehensive background checks are performed by an independent third party for *contract employees (1099)* as a component of the hiring process.
- SIG maintains an employee handbook which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.
- Management has developed a training and development program for employees. This includes:
    - Initial training/orientation with peers and supervisors in the period immediately after hire.
- Employees undergo an annual performance review which includes discussions related to their performance related to internal control responsibilities such as data and systems security. A formal evaluation is prepared and is maintained in the employee's HR file.
- Management utilizes a termination checklist to ensure that specific elements of the termination process are consistently executed. A copy of the checklist is kept in the employee file.

RISK ASSESSMENT

Management is responsible for identifying the risks that threaten achievement of the control objectives stated in the management's description of the services and systems. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them. However, because control objectives relate to risk that controls seek to mitigate, management thoughtfully identified control objectives when designing, implementing, and documenting their system.

Objective Setting

SIG establishes objectives in order for management to identify potential events affecting their achievement. SIG has placed into operation a risk management process to help ensure that the chosen control objectives support and align with the organization's mission and are consistent with its risk framework. Objective setting enables management to identify measurement criteria for performance, with focus on success factors.

SIG has established certain broad categories including:

- **Strategic Objectives** — these pertain to the high level organizational goals and the alignment of those goals to support the overall mission
- **Operations Objectives** — these pertain to effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding of resources against loss
- **Reporting Objectives** — these pertain to the preparation of reliable reporting
- **Compliance Objectives** — these pertain to adherence to laws and regulations to which the entity is subject

Risks Identification

Regardless of whether an objective is stated or implied, an entity's risk-assessment process should consider risks that may occur. It is important that risk identification be comprehensive. SIG has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user organizations.

Management considers risks that can arise from both external and internal factors including:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives, pressures, and opportunities for employees, as well as employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired and methods of training utilized
- Changes in management responsibilities

The SIG risk assessment process focuses on supporting management decisions and responding to potential threats by assessing risks and identifying important decision factors. SIG senior management oversees risk management ownership, accountability, and is involved in risk identification process. Management identifies elements of business risk including threats, vulnerabilities, safeguards and the likelihood of a threat, to determine the actions to be taken.

Risks Analysis

SIG's methodology for analyzing risks varies, largely because many risks are difficult to quantify. Nonetheless, the process includes:

- Estimating the significance of a risk
- Assessing the likelihood (or frequency) of the risk occurring
- Considering how the risk should be managed, including an assessment of what actions need to be taken

Risk analysis is an essential process to the entity's success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring.

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

Selection and Development of Control Activities

Control activities are a part of the process by which SIG strives to achieve its business objectives. SIG has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed and improved when necessary to meet the overall objectives of the organization.

The applicable trust criteria and related control activities are included in Section 4 (the "Testing Matrices") of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in the Testing Matrices. Although the applicable trust criteria and related control activities are included in the Testing Matrices, they are, nevertheless, an integral part of SIG's description of controls and systems.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

MONITORING

SIG's management performs monitoring activities in order to continuously assess the quality of internal control over time. Monitoring activities are used to initiate corrective action through department meetings, client conference calls, and informal notifications. Management performs monitoring activities on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Ongoing and Separate Evaluations of the Control Environment

Monitoring can be done in two ways: through ongoing activities or separate evaluations. The greater the degree and effectiveness of ongoing monitoring, the less the need is for separate evaluations. Management determines the need for separate evaluations by consideration given to the following: the nature and degree of changes occurring and their associated risks, the competence and experience of the people implementing the controls, as well as the results of the ongoing monitoring. Management has implemented a combination of ongoing monitoring and separate evaluations, as deemed necessary; to help ensure that the internal control system maintains its effectiveness over time.

Ongoing Monitoring

Examples of SIG's ongoing monitoring activities include the following:

- In carrying out its regular management activities, operating management obtains evidence that the system of internal control continues to function.
- Communications from external parties and customers corroborate internally generated information or indicate problems.
- Organization structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- Training, planning sessions, and other meetings provide important feedback to management on whether controls are effective.
- Personnel are briefed on organizational policy statements and codes of conduct to communicate entity values.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often.

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. These assessments are considered by management, along with any other internal control evaluations. The findings of these efforts are utilized to ensure follow-up actions are taken and subsequent evaluations are modified as necessary.

Reporting Deficiencies

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

SUBSERVICE ORGANIZATIONS

The third party data center services provided by Amazon Web Services (AWS) are monitored by SIG management but are not included in the scope of this audit. The following criteria and controls are expected to be implemented by AWS.

SUBSERVICE ORGANIZATION CONTROLS		
Category	**Criteria**	**Applicable Controls**
Security	CC6.3 CC6.4	The third party data center has physical access controls in place to *restrict access* to authorized personnel only.
Security	CC6.5	The third party data center has physical access controls in place to *remove access* when no longer required.
Security Availability	CC4.1 A1.2	The third party data center is responsible for the controls relevant to the completeness and accuracy of specified reports provided to and used by SIG.
Security	CC8.1	The third party data center is responsible for the general IT controls relevant to its application development and/or change management.
Availability	A1.2	The environmental security and maintenance controls at the third party data center are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.

INFORMATION AND COMMUNICATION SYSTEMS

Information Systems

A combination of custom developed and commercial applications is utilized to support the science distance learning solutions and services provided to user organizations. The applications run on Linux, Windows Server 2008R2 and above, AWS virtualized hardware platforms with commercial databases to support the applications.

Redundancy is maintained for components of the data infrastructure, including firewalls, routers, servers and switches. Systems are developed and deployed to enable the addition of bandwidth and server capacity quickly to support customer requirements. External services and internal applications constantly monitor communications, job logs, system performance, and security and send alerts to the operations staff before customers are affected.

Communication Systems

Upper management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within SIG. Management believes that open communication channels help ensure that exceptions are reported and acted on. For that reason, formal communication tools such as organizational charts, employee handbooks, training classes and job descriptions are in place at SIG. Management's communication activities are made electronically, verbally, and through the actions of management.

SYSTEM INCIDENTS DURING THE PERIOD

There were no identified system incidents during the period from September 1, 2020 to August 31, 2021 that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of the service commitments and system requirements.

COMPLEMENTARY CONTROLS AT USER ORGANIZATIONS

SIG's services are designed with the assumption that certain controls will be implemented by user organizations. Such controls are called complementary user organization controls. It is not feasible for all of the control objectives related to SIG's science distance learning solutions to be solely achieved by SIG's control procedures. Accordingly, user organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of SIG.

The following complementary user organization controls should be implemented by user organizations to provide additional assurance that the control objectives described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user organizations' locations, user organizations' auditors should exercise judgment in selecting and reviewing these complementary user organization controls, which may include:

- User organizations are responsible for understanding and complying with their contractual obligations to SIG. (CC2.3; CC5.3; CC9.2)
- User organizations are responsible for developing their own disaster recovery and business continuity plans that address their ability to access or utilize SIG services. (CC5.2; CC7.2; A1.2; A1.3)
- User organizations are responsible for ensuring that user IDs and passwords used to access SIG applications are kept in a secure manner and only used by authorized employees. (CC6.1; CC6.2; CC6.3; CC6.4)
- User organizations are responsible for requesting an authorized user ID and password for user organization employees. User organizations are responsible for defining the level of access given to employees and customers. (CC6.1; CC6.2; CC6.3; CC6.4)
- User organizations are responsible for requesting the revocation of application access privileges assigned to terminated employees as a component of the employee termination process. (CC6.1; CC6.2; CC6.3; CC6.4)
- User organizations are responsible for restricting administrative privileges within the application or systems to authorized personnel and for designating internal personnel who are authorized to request user additions, deletions, and security level changes. (CC6.1; CC6.2; CC6.3; CC6.4)
- User organizations are responsible for notifying SIG of changes made to technical or administrative contact information in a timely manner. (CC6.2)
- User organizations are responsible for understanding and defining data storage requirements. (CC4.1)
- User organizations are responsible for understanding and implementing encryption protocols to protect data during transfer to SIG. (CC6.6; CC6.7)
- User organizations are responsible for immediately notifying SIG of any actual or suspected information security breaches, including compromised user accounts and passwords. (CC7.2)
- User organizations are responsible for notifying SIG of any regulatory issues that may affect the services provided by SIG. (CC2.3; CC3.2)

COMPLEMENTARY CONTROLS AT SUBSERVICE ORGANIZATIONS

In designing its system, SIG has contemplated that certain complementary controls would be implemented by its subservice organizations to achieve the applicable criteria included in this report. This section describes the subservice organization's internal controls that, in combination with the controls at SIG, provide reasonable assurance that SIG can achieve the applicable criteria included in this report.

The controls below are the responsibility of each subservice organization.

- Subservice Organizations are responsible for ensuring that data center access for their employees, contractors, vendors, and clients is added only for authorized individuals. (CC6.3; CC6.4)
- Subservice Organizations are responsible for ensuring that data center access for their employees, contractors, vendors, and clients is removed when no longer required. (CC6.5)
- Subservice Organizations are responsible for implementing physical access mechanisms to ensure only authorized badge holders can enter the data centers. (CC6.3; CC6.4)
- Subservice Organizations are responsible for ensuring customer-specific areas with the data center can only be accessed by the customer. (CC6.3; CC6.4)
- Subservice Organizations are responsible for providing environmental security and maintenance controls that are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements. (A1.2)
- Subservice Organizations are responsible for the general IT controls relevant to its application development and/or change management. (CC8.1)
- Subservice Organizations are responsible for the controls relevant to the completeness and accuracy of specified reports provided to and used by SIG. (CC4.1; A1.2)

SECTION 4

TESTING MATRICES

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	SIG maintains an employee handbook which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.	Inspected the employee handbook to determine that it contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.	No exceptions noted.
		Policies and procedures require that new employees sign an employee handbook acknowledgment form indicating that they have been given access to it and understand their responsibilities. The signed form is kept in the employee personnel file.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee handbook and understand their responsibilities.	No exceptions noted.
		Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
		Comprehensive background checks are performed by an independent third party for *certain* positions as a component of the hiring process.	Inspected completed background checks for a judgmental sample of employees hired during the review period to determine that background checks are performed by an independent third party.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Contract employees (1099) must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inquired of management to determine that the *contract employees (1099)* signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
		Comprehensive background checks are performed by an independent third party for *contract employees (1099)* as a component of the hiring process.	Inquired of management to determine that background checks are performed by an independent third party for *contract employees (1099)* as a component of the hiring process.	No exceptions noted.
		Management maintains a commercial general liability insurance policy which includes technology/professional errors and omissions coverage and/or employee dishonesty.	Inspected insurance coverage policy declarations page to determine that management maintained a commercial general liability insurance policy which includes technology/professional errors and omissions coverage and/or employee dishonesty.	No exceptions noted.
		SIG utilizes an independent CPA firm to compile its financial statements and prepare tax returns.	Inquired of management to determine that SIG utilizes an independent CPA firm to compile its financial statements and prepare tax returns.	No exceptions noted.
			Inspected the most recent engagement letter reflecting the engagement of an independent CPA firm to determine that	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			management engages an independent CPA firm.	
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	A board of directors oversees management activities.	Inquired of management regarding the board of directors to determine that a board of directors was in place to oversee management activities.	No exceptions noted.
			Inspected the listing of the board of director members to determine that a board of directors was in place.	No exceptions noted.
		The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.	Inspected the listing of the board of director members to determine that the board has sufficient members who are independent from management and objective in evaluations and decision making.	No exceptions noted.
		The board of directors meets on a quarterly basis.	Inquired of management to determine that a board of directors meets quarterly.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written job descriptions.	Inspected a judgmental sample of written job descriptions to determine that management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written job descriptions.	No exceptions noted.
		Roles and responsibilities for company personnel to interact with and monitor the activities of external third party information	Inspected a judgmental sample of written job descriptions to determine that written job	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		technology vendors are defined in written job descriptions and communicated to personnel.	descriptions contain roles and responsibilities for company personnel to interact with and monitor the activities of external third party information technology vendors.	
		Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	Inspected organizational charts to determine that organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No exceptions noted.
		Management has authorized specific personnel to administer information security within the production environment.	Inspected the access rights listing to determine that management has authorized specific personnel to administer information security within the production environment.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place to guide personnel regarding providing for training and other resources to support its system security policies.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding training and other resources to support its system security policies.	No exceptions noted.
		Comprehensive background checks are performed by an independent third party for *certain* positions as a component of the hiring process.	Inspected completed background checks for a judgmental sample of employees hired during the review period to determine that background checks are performed by an independent third party.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written job descriptions.	Inspected a judgmental sample of written job descriptions to determine that management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written job descriptions.	No exceptions noted.
		Candidates' abilities to meet job requirements are evaluated as part of the hiring, performance review, and transfer evaluation processes.	Inquired of management to determine that candidates' abilities to meet job requirements are evaluated as part of the hiring, performance review, and transfer evaluation processes.	No exceptions noted.
		Management has developed a training and development program for employees. This includes: • Initial training/orientation with peers and supervisors in the period immediately after hire.	Inquired of management into initial and ongoing training and development for employees to determine that a program is in place.	No exceptions noted.
		Management encourages employees to complete and continue formal education and technical certification programs. (formally or informally)	Inspected training documentation to pursue formal education and technical certification programs to determine that management encourages employees to complete and continue formal education and technical certification programs.	No exceptions noted.
		Certain approved professional development expenses incurred by the employees are paid by SIG. (training certs, classes, etc.)	Inspected expense documentation to determine that certain approved professional development expenses incurred by the employees are paid by SIG.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management has authorized specific personnel to administer information security within the production environment.	Inspected the access rights listing to determine that management has authorized specific personnel to administer information security within the production environment.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A policy is in place to assign responsibility and accountability for developing and maintaining the entity's security policies, and changes and updates to those policies, to appropriate personnel.	Inspected the policies and procedures to determine that responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, were assigned to appropriate personnel.	No exceptions noted.
		Operational meetings are held on a regular basis to discuss internal control responsibilities *(data and system security)* of individuals and performance measurement.	Inspected meeting minutes to determine that operational meetings are held on a regular basis to discuss internal control responsibilities (data and system security) of individuals and performance measurement.	No exceptions noted.
		Employees undergo an annual performance review which includes discussions related to their performance related to internal control responsibilities such as data and systems security. A formal evaluation is prepared and is maintained in the employee's HR file.	Inspected a judgmental sample of annual performance reviews to determine that performance related to internal control responsibilities such as data and systems security was discussed.	No exceptions noted.
		Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	Inspected organizational charts to determine that organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC1.0 - COMMON CRITERIA RELATED TO THE CONTROL ENVIRONMENT

The criteria relevant to how the entity (i) demonstrates commitment to integrity and ethical values, (ii) exercises oversight responsibility, (iii) establishes structure, authority and responsibility, (iv) demonstrates commitment to competence, and (v) enforces accountability.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management has authorized specific personnel to administer information security within the production environment.	Inspected the access rights listing to determine that management has authorized specific personnel to administer information security within the production environment.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas: • Data security (company data and client data). • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information. • Regulatory, economic, and physical environment in which the company operates. • Business environment, including industry, competitors, regulatory environment, and consumers. • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. • Management and respective attitudes and philosophies on the system of internal control. • Vendor and business partner relationships including third party data centers. • Systems and technology environment.	Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		SIG has logical and physical security, change management, incident monitoring, and data classification, integrity, and retention controls, as necessary, with checks and balances woven into each applicable process to ensure quality of processing.	Inspected internal processes and procedures to determine that SIG has logical and physical security, change management, incident monitoring, and data classification, integrity, and retention controls, as necessary, with checks and balances woven into each applicable process to ensure quality of processing.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Policies and procedures are in place to guide personnel regarding providing for training and other resources to support its system security policies.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding training and other resources to support its system security policies.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding the handling of exceptions and situations not specifically addressed in its system security policies.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding the handling of exceptions and situations not specifically addressed in its system security policies.	No exceptions noted.
		Policies and procedures are in place to assign responsibility and accountability for system security.	Inspected the policies and procedures to determine that monitoring policies and procedures were in place to assign responsibility and accountability for system security.	No exceptions noted.
		Policies and procedures are in place for identifying the system security requirements of authorized users.	Inspected the policies and procedures to determine that the entity's system security policies were established.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Security policies are in place to guide personnel regarding physical and information security practices.	Inspected the policies and procedures manual to determine that security policies were in place to guide personnel regarding physical and information security practices.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding resolution of complaints and requests relating to system security and related issues.	No exceptions noted.
		Policies and procedures are in place to communicate responsibility and accountability for the entity's confidentiality and related security policies and changes and updates to those policies.	Inspected the policies and procedures to determine that responsibility and accountability for the entity's confidentiality and related security policies and changes and updates to those policies were communicated to entity personnel responsible for implementing them.	No exceptions noted.
		Procedures have been implemented to protect confidential information in the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive.	Inspected confidentiality policies and procedures implemented to protect confidential information in the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive.	No exceptions noted.
		SIG has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Service	Inspected a sample customer agreement to determine that service commitments to customers are documented and	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		commitments to customers are documented and communicated in customer agreements provided to user entities.	communicated in customer agreements provided to user entities.	
		Third party enterprise monitoring applications are used to monitor system downtime and operations issues, which are monitored to help ensure that system downtime and performance does not exceed predefined levels. This includes monitoring of both critical network and server hardware, as well as processes and services: • System uptime and downtime • Critical performance metrics (CPU utilization, storage, etc.). Problems with critical systems are remediated as necessary.	Inspected the enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical server and network equipment.	No exceptions noted.
			Inquired of management to determine that system downtime and operations issues were monitored.	No exceptions noted.
			Inspected a judgmental sample of tickets to determine that problems with critical systems are remediated as necessary.	No exceptions noted.
		The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via SMS text or email to appropriate support personnel.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.
		Network diagrams are in place and communicated to appropriate personnel.	Inspected network diagrams to determine that network diagrams	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			are in place and communicated to appropriate personnel.	
		SIG has implemented a backup policy, and backups of production systems and data are completed in a timely manner. The retention period for backup data has been defined by management.	Inquired of management to determine that SIG has implemented a backup policy, and that backups of production systems and data are completed in a timely manner.	No exceptions noted.
			Inspected the backup policy, backup configurations, and a judgmental sample of backup logs to determine that SIG has implemented a backup policy, and that backups of production systems and data are completed in a timely manner.	No exceptions noted.
			Inspected the backup policy and backup configurations to determine that the retention period for backup data has been defined by management.	No exceptions noted.
		SIG maintains an employee handbook which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.	Inspected the employee handbook to determine that it contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.	No exceptions noted.
		Policies and procedures require that new employees sign an employee handbook acknowledgment form indicating that they have	Inspected completed acknowledgment forms for a judgmental sample of employees	No exceptions noted.

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		been given access to it and understand their responsibilities. The signed form is kept in the employee personnel file.	hired during the review period to determine that policies and procedures require that employees sign an acknowledgment form indicating that they have been given access to the employee handbook and understand their responsibilities.	
		Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Policies and procedures are in place to assign responsibility and accountability for system security.	Inspected the policies and procedures to determine that monitoring policies and procedures were in place to assign responsibility and accountability for system security.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding sharing information with third parties.	Inspected the policies and procedures and the service level agreements to determine that the entity's policies included procedures to guide personnel regarding sharing information with third parties.	No exceptions noted.
		Procedures have been implemented to protect confidential information in the event that a	Inspected confidentiality policies and procedures implemented to protect	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC2.0 - COMMON CRITERIA RELATED TO COMMUNICATION AND INFORMATION

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		disclosed confidentiality practice is discontinued or changed to be less restrictive.	confidential information in the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive.	
		Policies and procedures are in place for identifying the system security requirements of authorized users.	Inspected the policies and procedures to determine that the entity's system security policies were established.	No exceptions noted.
		SIG has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Service commitments to customers are documented and communicated in customer agreements provided to user entities.	Inspected a sample customer agreement to determine that service commitments to customers are documented and communicated in customer agreements provided to user entities.	No exceptions noted.
		Prior to collecting personal information of external users, a privacy policy is provided that may include the purpose and use of the personal information, including detailed use, ability to opt-out, enhancement (enrichment), sharing, disclosure, access, security, retention, breach notification requirements, and disposal of personal information.	Inspected policies to determine that if personal information of external users is collected, a privacy policy is provided that may include the purpose and use of the collection of their personal information, including detailed use, ability to opt-out, enhancement (enrichment), sharing, disclosure, access, security, retention, breach notification requirements, and disposal of personal information.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas: • Data security (company data and client data). • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information. • Regulatory, economic, and physical environment in which the company operates. • Business environment, including industry, competitors, regulatory environment, and consumers. • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. • Management and respective attitudes and philosophies on the system of internal control. • Vendor and business partner relationships including third party data centers. • Systems and technology environment.	Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management regularly attends trade shows, utilizes trade and regulatory publications, journals, online news feeds and government sites, and belongs to industry associations to stay current on regulatory compliance or operational trends affecting the services provided.	Inspected company documentation of trade show agendas, online sites, publications, and association membership literature to determine that management is periodically briefed on regulatory and industry changes affecting services provided.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.	Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assessing risks on a periodic basis.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security and related security breaches and other incidents.	No exceptions noted.
		A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas: • Data security (company data and client data). • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information.	Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.	No exceptions noted.

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		• Regulatory, economic, and physical environment in which the company operates. • Business environment, including industry, competitors, regulatory environment, and consumers. • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. • Management and respective attitudes and philosophies on the system of internal control. • Vendor and business partner relationships including third party data centers. • Systems and technology environment.		
		Management regularly attends trade shows, utilizes trade and regulatory publications, journals, online news feeds and government sites, and belongs to industry associations to stay current on regulatory compliance or operational trends affecting the services provided.	Inspected company documentation of trade show agendas, online sites, publications, and association membership literature to determine that management is periodically briefed on regulatory and industry changes affecting services provided.	No exceptions noted.
		Redundant architecture is built into server infrastructure, including, but not limited to the: • Network interface cards (NICs) • Power supplies • RAID storage.	Observed the redundant system infrastructure components to determine that redundant architecture was built into certain aspects of the systems infrastructure.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Critical production equipment is maintained under warranty and maintenance or Service Level Agreements (SLAs) with 3rd party vendors.	Inquired of management to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.	No exceptions noted.
			Inspected current agreements with third party vendors to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas: • Data security (company data and client data). • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information. • Regulatory, economic, and physical environment in which the company operates. • Business environment, including industry, competitors, regulatory environment, and consumers. • Potential impact of new business lines, dramatically altered business lines, acquired or divested business	Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. • Management and respective attitudes and philosophies on the system of internal control. • Vendor and business partner relationships including third party data centers. • Systems and technology environment.		
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas: • Data security (company data and client data). • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information. • Regulatory, economic, and physical environment in which the company operates. • Business environment, including industry, competitors, regulatory environment, and consumers. • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal	Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC3.0 - COMMON CRITERIA RELATED TO RISK ASSESSMENT

The criteria relevant to how the entity (i) specifies suitable objectives, (ii) identifies and analyzes risk, and (iii) assess fraud risk.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		control, rapid growth, changing reliance on foreign geographies, and new technologies. • Management and respective attitudes and philosophies on the system of internal control. • Vendor and business partner relationships including third party data centers. • Systems and technology environment.		

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC4.0 - COMMON CRITERIA RELATED TO MONITORING ACTIVITIES

The criteria relevant to how the entity (i) conducts ongoing and/or separate evaluations, and (ii) evaluates and communicates deficiencies.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.	Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assessing risks on a periodic basis.	No exceptions noted.
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.	No exceptions noted.
		Third party enterprise monitoring applications are used to monitor system downtime and operations issues, which are monitored to help ensure that system downtime and performance does not exceed predefined levels. This includes monitoring of both critical network and server hardware, as well as processes and services: • System uptime and downtime • Critical performance metrics (CPU utilization, storage, etc.). Problems with critical systems are remediated as necessary.	Inspected the enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical server and network equipment.	No exceptions noted.
			Inquired of management to determine that system downtime and operations issues were monitored.	No exceptions noted.
			Inspected a judgmental sample of tickets to determine that problems	No exceptions noted.

CC4.0 - COMMON CRITERIA RELATED TO MONITORING ACTIVITIES

The criteria relevant to how the entity (i) conducts ongoing and/or separate evaluations, and (ii) evaluates and communicates deficiencies.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			with critical systems are remediated as necessary.	
		The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via SMS text or email to appropriate support personnel.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.
		SIG periodically contracts with a third party network security company to conduct external network penetration tests and vulnerability assessments. A report is generated and reviewed by management, and tickets are generated for any necessary remedial action.	Inquired of management to determine that SIG periodically contracts with a third party network security company to conduct external network penetration tests and vulnerability assessments, and that management reviews any reports and generates tickets for any necessary remedial action.	No exceptions noted.
			Inspected report from a judgmental sample of external network penetration tests during the review period to determine that a report is generated and reviewed by management.	No exceptions noted.
			Inquired of management to determine tickets are generated for any necessary remedial action.	No exceptions noted.
		Certain network events are logged and maintained for management review. Critical servers have auditing enabled, and for security, system management and network functions.	Inspected the network account and local event monitoring configurations, and event logs to determine that certain network events were logged and maintained for management review.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC4.0 - COMMON CRITERIA RELATED TO MONITORING ACTIVITIES

The criteria relevant to how the entity (i) conducts ongoing and/or separate evaluations, and (ii) evaluates and communicates deficiencies.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Certain application events are logged and maintained for management review.	Inspected application logs to determine that certain Web server events were logged and maintained for management review.	No exceptions noted.
		SIG utilizes the services and controls of a third party data center for housing critical production computer servers, applications, and networking equipment. The third party data center is responsible for the controls relevant to the completeness and accuracy of specified reports provided to and used by SIG.	Inspected the most recent SOC audit report for the third party data center to determine that SIG utilizes relevant reports provided by the third party data center.	No exceptions noted.
		SIG management reviews the SOC audit report of the third party data center annually and documents the results of the review of the SOC audit report in a memo.	Inquired of management to determine that SIG management reviews the SOC audit report of the third party data center annually.	No exceptions noted.
			Inspected management's memo to determine that SIG management documents the results of the review of the SOC report in a memo.	No exceptions noted.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Security policies and procedures are in place and periodically reviewed by a designated individual or group.	Inspected the policies and procedures manual to determine that the entity's system security policies and procedures are in place and periodically reviewed by a designated individual or group.	No exceptions noted.
		Third party enterprise monitoring applications are used to monitor system downtime and operations issues, which are monitored to help ensure that system downtime and performance	Inspected the enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor	No exceptions noted.

CC4.0 - COMMON CRITERIA RELATED TO MONITORING ACTIVITIES

The criteria relevant to how the entity (i) conducts ongoing and/or separate evaluations, and (ii) evaluates and communicates deficiencies.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		does not exceed predefined levels. This includes monitoring of both critical network and server hardware, as well as processes and services: • System uptime and downtime • Critical performance metrics (CPU utilization, storage, etc.). Problems with critical systems are remediated as necessary.	performance criteria for critical server and network equipment.	
			Inquired of management to determine that system downtime and operations issues were monitored.	No exceptions noted.
			Inspected a judgmental sample of tickets to determine that problems with critical systems are remediated as necessary.	No exceptions noted.
		The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via SMS text or email to appropriate support personnel.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.	No exceptions noted.
		SIG periodically contracts with a third party network security company to conduct external network penetration tests and vulnerability	Inquired of management to determine that SIG periodically contracts with a third party network	No exceptions noted.

CC4.0 - COMMON CRITERIA RELATED TO MONITORING ACTIVITIES

The criteria relevant to how the entity (i) conducts ongoing and/or separate evaluations, and (ii) evaluates and communicates deficiencies.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		assessments. A report is generated and reviewed by management, and tickets are generated for any necessary remedial action.	security company to conduct external network penetration tests and vulnerability assessments, and that management reviews any reports and generates tickets for any necessary remedial action.	
			Inspected report from a judgmental sample of external network penetration tests during the review period to determine that a report is generated and reviewed by management.	No exceptions noted.
			Inquired of management to determine tickets are generated for any necessary remedial action.	No exceptions noted.
		Certain network events are logged and maintained for management review. Critical servers have auditing enabled, and for security, system management and network functions.	Inspected the network account and local event monitoring configurations, and event logs to determine that certain network events were logged and maintained for management review.	No exceptions noted.
		Certain application events are logged and maintained for management review.	Inspected application logs to determine that certain Web server events were logged and maintained for management review.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.	Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assessing risks on a periodic basis.	No exceptions noted.
		Security policies and procedures are in place and periodically reviewed by a designated individual or group.	Inspected the policies and procedures manual to determine that the entity's system security policies and procedures are in place and periodically reviewed by a designated individual or group.	No exceptions noted.
		A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas: • Data security (company data and client data). • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information. • Regulatory, economic, and physical environment in which the company operates. • Business environment, including industry, competitors, regulatory environment, and consumers. • Potential impact of new business lines, dramatically altered business lines, acquired or divested business	Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. • Management and respective attitudes and philosophies on the system of internal control. • Vendor and business partner relationships including third party data centers. • Systems and technology environment.		
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that management periodically performs internal security assessments.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.	Inspected the policies and procedures manual to determine that the entity's policies included procedures regarding assessing risks on a periodic basis.	No exceptions noted.
		Security policies and procedures are in place and periodically reviewed by a designated individual or group.	Inspected the policies and procedures manual to determine that the entity's system security policies and procedures are in place and periodically reviewed by a designated individual or group.	No exceptions noted.
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			management periodically performs internal security assessments.	
		SIG periodically contracts with a third party network security company to conduct external network penetration tests and vulnerability assessments. A report is generated and reviewed by management, and tickets are generated for any necessary remedial action.	Inquired of management to determine that SIG periodically contracts with a third party network security company to conduct external network penetration tests and vulnerability assessments, and that management reviews any reports and generates tickets for any necessary remedial action.	No exceptions noted.
			Inspected report from a judgmental sample of external network penetration tests during the review period to determine that a report is generated and reviewed by management.	No exceptions noted.
			Inquired of management to determine tickets are generated for any necessary remedial action.	No exceptions noted.
		Firewall systems are in place to screen data flow between external parties and the SIG network. All inbound and outbound data packets on all interfaces are intercepted and inspected. Packets that are not explicitly permitted by the security policy definition are rejected.	Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and SIG network.	No exceptions noted.
			Inspected the firewall system configuration to determine that packets that are not explicitly permitted by the security policy definition are rejected.	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Firewall configurations filter internet traffic based on content and destination site address. The configurations include: • The firewall performs stateful packet inspection. • Network Address Translation (NAT) services are enabled on all network firewalls to hide internal servers. • Firewall ports are configured to allow only specific types of traffic between certain destinations. All unused ports on the firewall are blocked. • The firewall is configured to deny all traffic that is not specifically authorized in the rule set.	Inspected firewall configurations to determine that firewall configurations filter internet traffic based on content and destination site address, and that the firewall performs stateful packet inspection.	No exceptions noted.
			Inspected the firewall configuration to determine that the NAT services are enabled on all network firewalls.	No exceptions noted.
			Inspected the firewall system configuration to determine that firewalls are configured to allow only specific types of traffic between certain destinations, and that unused ports are disabled.	No exceptions noted.
			Inspected the firewall rule sets to determine that the firewall was configured to deny traffic that was not specifically authorized in the rule set.	No exceptions noted.
		Management utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion	Inspected IPS configurations to determine that management	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		into the production environment. The IPS subscription for the firewall system is kept current.	utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion into the production environment.	
			Inspected a judgmental sample of alerts or notifications from the intrusion prevention system of any attempt at unauthorized intrusion into the production environment.	No exceptions noted.
			Inspected the IPS subscription to determine that the IPS subscription for the firewall system is kept current.	No exceptions noted.
		The IPS is configured to both detect and mitigate known attacks based on signatures. It is also configured to protect against attacks based on protocol anomalies (DoS/DDoS). Signatures are automatically updated as new attack signatures are made available. The system is configured to log events and packet data on violation of the configured signatures.	Inquired of management to determine that the IPS is configured to both detect and mitigate known attacks based on signatures and protocol anomalies.	No exceptions noted.
			Inspected the IPS application configurations to determine that it is configured to automatically update as new attack signatures are made available.	No exceptions noted.
		Management maintains a commercial general liability insurance policy which includes technology/professional errors and omissions coverage and/or employee dishonesty.	Inspected insurance coverage policy declarations page to determine that management maintained a commercial general liability insurance policy which includes technology/professional	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			errors and omissions coverage and/or employee dishonesty.	
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	SIG's policies and procedures address controls over significant aspects of system operations. Policies and procedures addressed include: • security requirements for authorized users • data classification and associated protection, access rights, retention, and destruction requirements • risk assessment • access protection requirements • user provisioning and deprovisioning • responsibility and accountability for security • responsibility and accountability for system changes and maintenance • change management • complaint intake and resolution • security and other incidents identification, response, and mitigation • security training • handling of exceptions and situations not specifically addressed in policies • commitment and requirement identification and compliance measurement • information sharing and disclosure.	Inspected the policies and procedures to determine the policies and procedures addressed controls over significant aspects of the system operations.	No exceptions noted.
		SIG's security policies are reviewed and updated annually by senior management for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.	Inspected documentation of the annual review and update of the security policies to determine the policies are reviewed annually by senior management for consistency with the organization's risk	No exceptions noted.

CC5.0 - COMMON CRITERIA RELATED TO CONTROL ACTIVITIES

The criteria relevant to how the entity (i) selects and develops control activities, (ii) selects and develops general controls over technology, and (iii) deploys through policies and procedures.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			mitigation strategy and updated as necessary for changes in the strategy.	
		Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written job descriptions.	Inspected a judgmental sample of written job descriptions to determine that management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written job descriptions.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Procedures have been implemented related to confidentiality of inputs, data processing, and outputs which are consistent with the documented confidentiality policies.	Inspected confidentiality policies and procedures to determine that procedures have been implemented related to confidentiality of inputs, data processing, and outputs which are consistent with the documented confidentiality policies.	No exceptions noted.
		Users are required to authenticate via a unique user ID and password before being granted access to SIG internal network domain. Multifactor authentication is enabled.	Inspected the internal network domain authentication process to determine that users are required to authenticate via a unique user ID and password before being granted access to SIG internal network domain and that multifactor authentication is enabled.	No exceptions noted.
		Internal network domain (default domain) passwords must conform to the following requirements: • Enforce password history • Maximum password age • Minimum password age • Minimum password length • Complexity requirement enabled.	Inspected the network authentication configurations to determine that network domain passwords must conform to stated requirements.	No exceptions noted.
		Management has segregated specific duties within the internal network domain for administering critical areas such as network administration and database management. Management restricts network domain administration privileges to approved positions only.	Inquired of management to determine that management has authorized specific personnel to administer information security within the internal network domain and has segregated duties.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the administrative access rights listing to confirm that management has authorized specific personnel to administer information security within the internal network domain and has segregated specific duties within the internal network domain for administering critical areas such as network administration, and database management.	No exceptions noted.
		Users are assigned to pre-defined roles and access rights within all SIG systems: • Access to sensitive production server directories and files is restricted based on job responsibilities. • Users are granted variable access rights according to a rights authorization methodology. • Access to systems is granted on a “least privilege” basis, with employees acquiring access only to those systems necessary to perform their job functions.	Inquired of management to determine that users are assigned to pre-defined roles and access rights within all SIG production systems, and that variable rights are assigned based on job responsibilities and least privilege.	No exceptions noted.
			Inspected the access rights listing to determine that users are assigned to variable, pre-defined roles and access rights within all SIG production systems.	No exceptions noted.
		Database and application server operating system account policies are controlled by the default domain (authentication controls for employees are integrated).	Inquired of the network administrator regarding operating system account policies to determine that database and	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			application server operating system account policies were controlled by the internal active directory.	
			Inspected a judgmental sample of application and database server configurations to determine that the database and application server operating system account policies were controlled by an internal active directory.	No exceptions noted.
		Production server users are required to authenticate via a unique user ID and password before being granted access to the production environment.	Inspected the production network domain authentication process to determine that users are required to authenticate via a unique user ID and password before being granted access to the production environment.	No exceptions noted.
		Production domain passwords must conform to the following requirements: • Enforce password history • Maximum password age • Minimum password age • Minimum password length • Complexity requirement enabled.	Inspected the production domain authentication configurations to determine that production domain passwords must conform to stated requirements.	No exceptions noted.
		Application users are required to authenticate via an authorized unique user ID and password before being granted access to the production environment.	Inspected logon screens to determine that application users were required to authenticate via an authorized unique user ID and password before being granted access to the production environment.	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Hosted user application passwords must conform to the following requirements: • Minimum password length.	Inspected the hosted user application authentication configurations to determine that hosted user application passwords must conform to stated requirements.	No exceptions noted.
		Firewall systems are in place to screen data flow between external parties and the SIG network. All inbound and outbound data packets on all interfaces are intercepted and inspected. Packets that are not explicitly permitted by the security policy definition are rejected.	Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and SIG network.	No exceptions noted.
			Inspected the firewall system configuration to determine that packets that are not explicitly permitted by the security policy definition are rejected.	No exceptions noted.
		Management utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion into the production environment. The IPS subscription for the firewall system is kept current.	Inspected IPS configurations to determine that management utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion into the production environment.	No exceptions noted.
			Inspected a judgmental sample of alerts or notifications from the intrusion prevention system of any attempt at unauthorized intrusion into the production environment.	No exceptions noted.
			Inspected the IPS subscription to determine that the IPS subscription	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			for the firewall system is kept current.	
		The IPS is configured to both detect and mitigate known attacks based on signatures. It is also configured to protect against attacks based on protocol anomalies (DoS/DDoS). Signatures are automatically updated as new attack signatures are made available. The system is configured to log events and packet data on violation of the configured signatures.	Inquired of management to determine that the IPS is configured to both detect and mitigate known attacks based on signatures and protocol anomalies.	No exceptions noted.
			Inspected the IPS application configurations to determine that it is configured to automatically update as new attack signatures are made available.	No exceptions noted.
		A secure VPN (Virtual Private Network) connection is used for remote external access to the internal network by authorized SIG employees.	Inquired of management to determine that a secure VPN connection is used for remote external access to the internal network by authorized SIG employees.	No exceptions noted.
		The use of client-based VPN connections is restricted to authorized employees through usernames and passwords. Standard IKEV2 suite encryption is utilized.	Inspected Active Directory configurations to determine that the use of client-based VPN connections is restricted to authorized employees through usernames and passwords.	No exceptions noted.
			Inspected the VPN encryption certificates to determine that standard IKEV2 suite encryption is utilized.	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Onsite customers and visitors can utilize a wireless access point (WAP) located on a stand-alone network. This WAP only allows access to the internet, with no direct access to the internal company network. Security measures have been implemented on this WAP.	Inquired of management regarding the wireless access point to determine that it is located on a stand-alone network, and that access is limited to the internet.	No exceptions noted.
			Inspected the WAP configuration settings and encryption certificates to determine that security measures have been implemented on this wireless access point.	No exceptions noted.
		Onsite *SIG employees* can utilize a wireless access point (WAP) to directly access the internal network environment. Security measures have been implemented on this WAP.	Inspected the firewall/WAP configuration settings and encryption certificates to determine that access to internal network is granted and security measures have been implemented on this wireless access point.	No exceptions noted.
		Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
		Production systems backup data is encrypted in motion.	Inspected the backup configurations to determine that the backups are encrypted in motion.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Access to data is restricted to authorized applications through access control software. Access rules are created and maintained by information security personnel during the application development process.	Inspected data access to determine that access to data is restricted to authorized applications through access control software.	No exceptions noted.
			Inquired of management to determine that access rules are created and maintained by information security personnel during the application development process.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.	Inspected the policies and procedures to determine that new user access, modification, and removal policies are in place.	No exceptions noted.
		Management utilizes a new hire checklist to ensure that specific elements of the hiring process are consistently executed. A copy of the checklist is kept in the employee file.	Inspected a judgmental sample of new hire checklists used for employees hired during the review period to determine that management utilizes a new hire checklist for the employees and that the checklist is kept in the employee files.	Exception noted: No new hire checklists were available for review from the new hire list. Management Response: See Section 5.
		Management revokes corporate network and production server connection privileges assigned to terminated employees as a	Inspected a judgmental sample of domain user listings to determine that management revoked	Exception noted: Accounts for three of the six terminated

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		component of the employee termination process.	corporate network access privileges assigned to terminated employees as a component of the employee termination process.	employees sampled were still active. Management Response: See Section 5.
		A formal process is in place to ensure HR informs IT when employee access to company IT resources needs to be added or removed.	Inspected a judgmental sample of communications between HR and IT (tickets or emails or checklists) to determine that a formal process is in place to ensure HR informs IT when employee access to company IT resources needs to be added or removed.	Exception noted: No communications between HR and IT were available for review from the new hire or termination list. Management Response: See Section 5.
		Management utilizes a termination checklist to ensure that specific elements of the termination process are consistently executed. A copy of the checklist is kept in the employee file.	Inspected a judgmental sample of termination checklists utilized during the review period, to determine that management utilizes a termination checklist to ensure that specific elements of the termination process are consistently executed, and that the checklist is retained in the employee file.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.	Inspected the policies and procedures to determine that new user access, modification, and removal policies are in place.	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management revokes corporate network and production server connection privileges assigned to terminated employees as a component of the employee termination process.	Inspected a judgmental sample of domain user listings to determine that management revoked corporate network access privileges assigned to terminated employees as a component of the employee termination process.	Exception noted: Accounts for three of the six terminated employees sampled were still active. Management Response: See Section 5.
		Management has segregated specific duties within the internal network domain for administering critical areas such as network administration and database management. Management restricts network domain administration privileges to approved positions only.	Inquired of management to determine that management has authorized specific personnel to administer information security within the internal network domain and has segregated duties.	No exceptions noted.
			Inspected the administrative access rights listing to confirm that management has authorized specific personnel to administer information security within the internal network domain and has segregated specific duties within the internal network domain for administering critical areas such as network administration, and database management.	No exceptions noted.
		Users are assigned to pre-defined roles and access rights within all SIG systems: • Access to sensitive production server directories and files is restricted based on job responsibilities. • Users are granted variable access rights according to a rights authorization methodology.	Inquired of management to determine that users are assigned to pre-defined roles and access rights within all SIG production systems, and that variable rights are assigned based on job responsibilities and least privilege.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		• Access to systems is granted on a "least privilege" basis, with employees acquiring access only to those systems necessary to perform their job functions.		
			Inspected the access rights listing to determine that users are assigned to variable, pre-defined roles and access rights within all SIG production systems.	No exceptions noted.
		Security groups are utilized to manage access privileges within the hosted user application.	Inspected a judgmental sample of security groups and access privileges to determine that security groups were utilized to manage access privileges within the hosted user application.	No exceptions noted.
		SIG utilizes the services and controls of a third party data center for housing critical production computer servers, applications, and networking equipment. The third party data center has physical access controls in place to *restrict access* to authorized personnel only.	Inspected the most recent SOC audit report for the third party data center to determine that the third party data center has physical access controls in place to restrict access to authorized personnel only.	No exceptions noted.
		SIG management reviews the SOC audit report of the third party data center annually and documents the results of the review of the SOC audit report in a memo.	Inquired of management to determine that SIG management reviews the SOC audit report of the third party data center annually.	No exceptions noted.
			Inspected management's memo to determine that SIG management documents the results of the review of the SOC report in a memo.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Physical security policies and procedures are in place to guide personnel regarding restricting access to the facility.	Inspected the policies and procedures manual to determine that physical security policies and procedures were in place to guide personnel regarding restricting access to the facility.	No exceptions noted.
		Access into the corporate suite is restricted by a key fob access system. Access is granted to employees only. All accesses are logged by the system and stored in digital format for ad hoc review. (Denver office)	Observed the access system at the facility to determine that access into the corporate suite is restricted by a key fob access system.	No exceptions noted.
			Inspected a judgmental sample of printouts of logged accesses to determine that all accesses are logged and stored in digital format for ad hoc review.	No exceptions noted.
		The employee termination process includes the removal of the terminated personnel's ability to gain access to the facility, including deactivation and retrieval of all electronic access means. This process is documented in the termination checklist.	Inquired of management to determine that electronic access is deactivated and proximity cards and physical keys are retrieved where possible.	No exceptions noted.
			Inspected a judgmental sample of termination checklists for any employees terminated during the review period to determine that this process is documented in the checklist.	No exceptions noted.
		Visitors to the company facility may only enter through the main entrance, where access is monitored at the manned reception desk.	Inquired of management to determine that visitors to the company facility may only enter	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			through the main entrance, where access is monitored at the manned reception desk.	
		All visitors are required to be escorted by an authorized employee at all times.	Inquired of management to determine that all visitors are required to be escorted by an authorized employee at all times.	No exceptions noted.
		The server room is equipped with an access security system requiring a proximity card access system for entry. (Denver office)	Observed access into the server room to determine that access to the server room was equipped with an access security system requiring a proximity card for entry, with a physical key override for power outages.	No exceptions noted.
		Server room access is restricted based on job responsibility and is limited to approved positions only. (Denver office)	Inspected the server room access listing to determine that the ability to access the server room was restricted based on job responsibility and was limited to approved positions only.	No exceptions noted.
		Intrusion and motion alarm systems are in place and monitored for all entry/exit points of the facility, including doors and windows. An audible alarm sounds upon triggering.	Observed the alarm systems at the facility to determine that alarm systems are in place to monitor all entry and exit points to the facilities.	No exceptions noted.
		SIG computer and network components are installed in either locked cabinets or in a secured room with no customer access. (Denver office)	Observed areas of computer and network components to determine that SIG computer and network components are installed in either locked cabinets or in a secured room with no customer access.	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Server room walls extend from the physical floor to the physical ceiling structure.	Observed server room walls to determine they extend from the physical floor to the physical ceiling structure.	No exceptions noted.
		No windows to the exterior exist within the server room.	Observed server room to determine that no windows to the exterior exist.	No exceptions noted.
		Sensitive physical papers are stored onsite in locked filing cabinets.	Observed the locked filing cabinets to determine that sensitive physical papers are stored in locked filing cabinets.	No exceptions noted.
		All sensitive physical papers are disposed in accordance with SIG policy. Paperwork with sensitive customer data is discarded into a locked bin and is shredded on site by an independent contractor on a monthly basis.	Inquired of management to determine that all sensitive physical papers are disposed in accordance with SIG policy and that paperwork with sensitive customer data is discarded into a locked bin and is shredded on site by an independent contractor on a monthly basis.	No exceptions noted.
			Observed shredding bins to determine that paperwork with sensitive customer data is discarded into locked bins.	No exceptions noted.
			Inspected a judgmental sample of invoices from the review period to determine that paperwork with sensitive customer data is shredded on site by an independent contractor on a monthly basis.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		SIG utilizes the services and controls of a third party data center for housing critical production computer servers, applications, and networking equipment. The third party data center has physical access controls in place to *restrict access* to authorized personnel only.	Inspected the most recent SOC audit report for the third party data center to determine that the third party data center has physical access controls in place to restrict access to authorized personnel only.	No exceptions noted.
		SIG management reviews the SOC audit report of the third party data center annually and documents the results of the review of the SOC audit report in a memo.	Inquired of management to determine that SIG management reviews the SOC audit report of the third party data center annually.	No exceptions noted.
			Inspected management's memo to determine that SIG management documents the results of the review of the SOC report in a memo.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Physical security policies and procedures are in place to guide personnel regarding restricting access to the facility.	Inspected the policies and procedures manual to determine that physical security policies and procedures were in place to guide personnel regarding restricting access to the facility.	No exceptions noted.
		The employee termination process includes the removal of the terminated personnel's ability to gain access to the facility, including deactivation and retrieval of all electronic access means. This process is documented in the termination checklist.	Inquired of management to determine that electronic access is deactivated and proximity cards and physical keys are retrieved where possible.	No exceptions noted.
			Inspected a judgmental sample of termination checklists for any employees terminated during the review period to determine that this	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			process is documented in the checklist.	
		Management revokes corporate network and production server connection privileges assigned to terminated employees as a component of the employee termination process.	Inspected a judgmental sample of domain user listings to determine that management revoked corporate network access privileges assigned to terminated employees as a component of the employee termination process.	Exception noted: Accounts for three of the six terminated employees sampled were still active. Management Response: See Section 5.
		All sensitive physical papers are disposed in accordance with SIG policy. Paperwork with sensitive customer data is discarded into a locked bin and is shredded on site by an independent contractor on a monthly basis.	Inquired of management to determine that all sensitive physical papers are disposed in accordance with SIG policy and that paperwork with sensitive customer data is discarded into a locked bin and is shredded on site by an independent contractor on a monthly basis.	No exceptions noted.
			Observed shredding bins to determine that paperwork with sensitive customer data is discarded into locked bins.	No exceptions noted.
			Inspected a judgmental sample of invoices from the review period to determine that paperwork with sensitive customer data is shredded on site by an independent contractor on a monthly basis.	No exceptions noted.
		SIG utilizes the services and controls of a third party data center for housing critical production computer servers, applications, and networking	Inspected the most recent SOC audit report for the third party data center to determine that the third	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		equipment. The third party data center has physical access controls in place to *remove access* when no longer required.	party data center has physical access controls in place to remove access when no longer required.	
		SIG management reviews the SOC audit report of the third party data center annually and documents the results of the review of the SOC audit report in a memo.	Inquired of management to determine that SIG management reviews the SOC audit report of the third party data center annually.	No exceptions noted.
			Inspected management's memo to determine that SIG management documents the results of the review of the SOC report in a memo.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Policies and procedures are in place to guide personnel regarding sharing information with third parties.	Inspected the policies and procedures and the service level agreements to determine that the entity's policies included procedures to guide personnel regarding sharing information with third parties.	No exceptions noted.
		Procedures have been implemented to provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies.	Inspected confidentiality policies and procedures related to disclosure to third parties to determine that confidential information is disclosed to third parties is done in accordance with the entity's defined confidentiality and related security policies.	No exceptions noted.
		Firewall systems are in place to screen data flow between external parties and the SIG network. All inbound and outbound data packets on all interfaces are intercepted and inspected. Packets that are not explicitly	Inspected the firewall system rule sets to determine that firewall systems are in place to handle data flow between external parties and SIG network.	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		permitted by the security policy definition are rejected.		
			Inspected the firewall system configuration to determine that packets that are not explicitly permitted by the security policy definition are rejected.	No exceptions noted.
		All firewall administrator accounts have been changed from their default password.	Inspected the administrator account ID configurations to determine that all firewall administrator accounts have been changed from their default password.	No exceptions noted.
		Firewall administrative rights are restricted based on job responsibility and are limited to approved positions only.	Inspected firewall system administration rights to determine that rights are restricted based on job responsibility and are limited to approved positions only.	No exceptions noted.
		Hardware-based firewalls and routers are placed at all network perimeter and third-party entry points to SIG networks.	Inspected the network diagram and firewall system rule sets to determine that hardware-based firewalls and routers are placed at all network perimeter and third party entry points to SIG networks.	No exceptions noted.
			Observed the network firewalls and routers to determine that hardware-based firewalls and routers are placed at all network perimeter and third-party entry points to SIG networks.	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Software-based firewalls are in place, utilizing third party firewall applications. The firewall applications are set up locally on each server.	Inspected the firewall configurations for a judgmental sample of servers to determine that software-based firewall applications are in use, and that they are set up locally on each server.	No exceptions noted.
		Firewall configurations filter internet traffic based on content and destination site address. The configurations include: • The firewall performs stateful packet inspection. • Network Address Translation (NAT) services are enabled on all network firewalls to hide internal servers. • Firewall ports are configured to allow only specific types of traffic between certain destinations. All unused ports on the firewall are blocked. • The firewall is configured to deny all traffic that is not specifically authorized in the rule set.	Inspected firewall configurations to determine that firewall configurations filter internet traffic based on content and destination site address, and that the firewall performs stateful packet inspection.	No exceptions noted.
			Inspected the firewall configuration to determine that the NAT services are enabled on all network firewalls.	No exceptions noted.
			Inspected the firewall system configuration to determine that firewalls are configured to allow only specific types of traffic between certain destinations, and that unused ports are disabled.	No exceptions noted.
			Inspected the firewall rule sets to determine that the firewall was	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			configured to deny traffic that was not specifically authorized in the rule set.	
		Management utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion into the production environment. The IPS subscription for the firewall system is kept current.	Inspected IPS configurations to determine that management utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion into the production environment.	No exceptions noted.
			Inspected a judgmental sample of alerts or notifications from the intrusion prevention system of any attempt at unauthorized intrusion into the production environment.	No exceptions noted.
			Inspected the IPS subscription to determine that the IPS subscription for the firewall system is kept current.	No exceptions noted.
		The IPS is configured to both detect and mitigate known attacks based on signatures. It is also configured to protect against attacks based on protocol anomalies (DoS/DDoS). Signatures are automatically updated as new attack signatures are made available. The system is configured to log events and packet data on violation of the configured signatures.	Inquired of management to determine that the IPS is configured to both detect and mitigate known attacks based on signatures and protocol anomalies.	No exceptions noted.
			Inspected the IPS application configurations to determine that it is configured to automatically update as new attack signatures are made available.	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A secure VPN (Virtual Private Network) connection is used for remote external access to the internal network by authorized SIG employees.	Inquired of management to determine that a secure VPN connection is used for remote external access to the internal network by authorized SIG employees.	No exceptions noted.
		The use of client-based VPN connections is restricted to authorized employees through usernames and passwords. Standard IKEV2 suite encryption is utilized.	Inspected Active Directory configurations to determine that the use of client-based VPN connections is restricted to authorized employees through usernames and passwords.	No exceptions noted.
			Inspected the VPN encryption certificates to determine that standard IKEV2 suite encryption is utilized.	No exceptions noted.
		Site-to-site VPN tunnels are locked down to specific locations via an access control list. IPsec network layer encryption is utilized.	Inspected a judgmental sample of access control lists to determine that site-to-site VPN tunnels are locked down to specific locations via an access control list.	No exceptions noted.
			Inspected the VPN encryption certificates to determine that VPN tunnels utilize the IPsec network layer encryption protocols to protect customer and SIG data in transit.	No exceptions noted.
		The production network is logically and physically segregated from the internal corporate network.	Inspected a network diagram to determine that the production network was logically and physically segregated from the internal corporate network.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Logical access to stored data is restricted to the application and database administrators.	Inquired of management to determine that logical access to stored data is restricted to the application and database administrators.	No exceptions noted.
			Inspected the access rights listing to determine that logical access to stored data is restricted to the application and database administrators.	No exceptions noted.
		Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected completed acknowledgment forms for a judgmental sample of employees hired during the review period to determine that the employees signed a confidentiality agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Policies and procedures are in place to guide personnel regarding sharing information with third parties.	Inspected the policies and procedures and the service level agreements to determine that the entity's policies included procedures to guide personnel regarding sharing information with third parties.	No exceptions noted.
		The use of client-based VPN connections is restricted to authorized employees through usernames and passwords. Standard IKEV2 suite encryption is utilized.	Inspected Active Directory configurations to determine that the use of client-based VPN connections is restricted to	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			authorized employees through usernames and passwords.	
			Inspected the VPN encryption certificates to determine that standard IKEV2 suite encryption is utilized.	No exceptions noted.
		Site-to-site VPN tunnels are locked down to specific locations via an access control list. IPsec network layer encryption is utilized.	Inspected a judgmental sample of access control lists to determine that site-to-site VPN tunnels are locked down to specific locations via an access control list.	No exceptions noted.
			Inspected the VPN encryption certificates to determine that VPN tunnels utilize the IPsec network layer encryption protocols to protect customer and SIG data in transit.	No exceptions noted.
		Transaction processing performed on web-based applications is secured through the use of the Secure Socket Layer (SSL) encryption protocol over HTTPS connections. • This includes the use of the website file upload page. • Traffic directed to HTTP connections for this are redirected to HTTPS connections.	Inspected the web application SSL certificates to determine that transaction processing performed on web-based applications is secured through the use of the Secure Socket Layer (SSL) protocol, and that licensing is current.	No exceptions noted.
		Security groups are utilized to manage access privileges within the hosted user application.	Inspected a judgmental sample of security groups and access privileges to determine that security groups were utilized to manage access privileges within the hosted user application.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security breaches and other incidents.	No exceptions noted.
		Only authorized system administrators are able to install software on system devices.	Inquired of management to determine that only authorized system administrators are able to install software on system devices.	No exceptions noted.
		Third party antivirus software is installed on all SIG servers (endpoint protection).	Inquired of management to determine that third party antivirus software is installed on all SIG servers.	No exceptions noted.
			Inspected antivirus software installed on judgmental sample of SIG servers to determine that antivirus software is installed on all SIG servers.	No exceptions noted.
		Antivirus applications are managed by a central antivirus server. • Definition updates are performed on a periodic basis. • System scans are performed on a weekly basis.	Inspected the antivirus system's update settings to determine that a central antivirus server monitored for updates to antivirus definitions on a periodic basis and that system scans are performed on a weekly basis.	No exceptions noted.
			Inspected the list of servers configured to receive updates from the central antivirus server to determine that antivirus software was installed on specific production servers.	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Third party antivirus protection is installed at the network perimeter firewalls to mitigate exposure to virus attacks on the production equipment (perimeter protection). Antivirus definition updates are performed by the perimeter antivirus application on a regular basis.	Inspected antivirus software installed at the perimeter firewalls to determine that a third party antivirus application is installed at the network perimeter and that antivirus definition updates are current.	No exceptions noted.
		A third party antivirus and spam filtering functionality in the hosted email service scans and filters incoming SIG email for viruses and spam (perimeter protection).	Inspected antivirus and spam filtering software installed at the perimeter to determine that a third party antivirus and spam filtering application scans and filters incoming SIG email for viruses and spam.	No exceptions noted.
		An automated methodology is utilized for managing workstation updates using a dedicated update service.	Inspected update configurations to determine that an automated methodology is utilized to roll out workstation updates.	No exceptions noted.
		Third party antivirus software is installed on all SIG workstations and laptops (endpoint protection). Antivirus definition updates are performed by the antivirus application on a regular basis.	Inspected antivirus software installed on judgmental sample of SIG workstations and laptops to determine that antivirus software is installed on all SIG workstations and laptops.	No exceptions noted.
			Inspected AV software configuration to determine that antivirus definition updates are performed on a regular basis.	No exceptions noted.
		A management-approved methodology is utilized to monitor operating system patch	Inquired of management to determine that a methodology is utilized to monitor operating system	No exceptions noted.

CC6.0 - COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS

The criteria relevant to how an entity (i) restricts logical and physical access, (ii) provides and removes that access, and (iii) prevents unauthorized access.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		releases, distribute patches to relevant devices and apply the patches to the device.	patch releases, distribute patches to relevant devices and apply the patches to the device. Inspected a judgmental sample of servers and workstations to determine that a management-approved methodology is utilized to monitor operating system patch releases, distribute patches to relevant devices and apply the patches to the device.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Third party enterprise monitoring applications are used to monitor system downtime and operations issues, which are monitored to help ensure that system downtime and performance does not exceed predefined levels. This includes monitoring of both critical network and server hardware, as well as processes and services: • System uptime and downtime • Critical performance metrics (CPU utilization, storage, etc.). Problems with critical systems are remediated as necessary.	Inspected the enterprise monitoring applications to determine that third party enterprise monitoring applications are used to monitor performance criteria for critical server and network equipment.	No exceptions noted.
			Inquired of management to determine that system downtime and operations issues were monitored.	No exceptions noted.
			Inspected a judgmental sample of tickets to determine that problems with critical systems are remediated as necessary.	No exceptions noted.
		The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via SMS text or email to appropriate support personnel.	Inspected the enterprise monitoring application configuration screens to determine that performance thresholds are set and alerts are communicated if pre-determined metrics are reached.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts,	A management-approved methodology is utilized to monitor operating system patch releases, distribute patches to relevant devices and apply the patches to the device.	Inquired of management to determine that a methodology is utilized to monitor operating system patch releases, distribute patches	No exceptions noted.

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		to relevant devices and apply the patches to the device.	
			Inspected a judgmental sample of servers and workstations to determine that a management-approved methodology is utilized to monitor operating system patch releases, distribute patches to relevant devices and apply the patches to the device.	No exceptions noted.
		Management utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion into the production environment. The IPS subscription for the firewall system is kept current.	Inspected IPS configurations to determine that management utilizes intrusion prevention systems (IPS) to prevent unauthorized intrusion into the production environment.	No exceptions noted.
			Inspected a judgmental sample of alerts or notifications from the intrusion prevention system of any attempt at unauthorized intrusion into the production environment.	No exceptions noted.
			Inspected the IPS subscription to determine that the IPS subscription for the firewall system is kept current.	No exceptions noted.
		Management periodically performs internal security assessments, including reviews of server logs and other critical items.	Inspected a judgmental sample of results from internal security assessments performed during the review period to determine that	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			management periodically performs internal security assessments.	
		SIG periodically contracts with a third party network security company to conduct external network penetration tests and vulnerability assessments. A report is generated and reviewed by management, and tickets are generated for any necessary remedial action.	Inquired of management to determine that SIG periodically contracts with a third party network security company to conduct external network penetration tests and vulnerability assessments, and that management reviews any reports and generates tickets for any necessary remedial action.	No exceptions noted.
			Inspected report from a judgmental sample of external network penetration tests during the review period to determine that a report is generated and reviewed by management.	No exceptions noted.
			Inquired of management to determine tickets are generated for any necessary remedial action.	No exceptions noted.
		SIG has implemented a backup policy, and backups of production systems and data are completed in a timely manner. The retention period for backup data has been defined by management.	Inquired of management to determine that SIG has implemented a backup policy, and that backups of production systems and data are completed in a timely manner.	No exceptions noted.
			Inspected the backup policy, backup configurations, and a judgmental sample of backup logs to determine that SIG has implemented a backup policy, and that backups of production systems	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			and data are completed in a timely manner.	
			Inspected the backup policy and backup configurations to determine that the retention period for backup data has been defined by management.	No exceptions noted.
		Logs track the backup events, and success and failure alerts are sent to IT staff, which investigate any failures, and remediate as necessary.	Inspected a judgmental sample of backup event logs and success/failure alerts to determine that logs track the backup events, and success and failure alerts are sent to IT staff.	No exceptions noted.
			Inquired of management to determine that failures are investigated and remediated.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security and related security breaches and other incidents.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding resolution of complaints and requests relating to system security and related issues.	No exceptions noted.
		A ticketing system is utilized to manage systems infrastructure issues and changes.	Inspected a judgmental sample of logs from the ticketing system	No exceptions noted.

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Tickets are assigned to support personnel based on the nature of the ticket.	showing closed tickets to determine that a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on the nature of the ticket.	
		Helpdesk calls are entered into the ticketing system and call tracking utility and given a ticket number. • A priority level is assigned in accordance with company policy. • All issues that cannot be addressed within appropriate time intervals are escalated to management to assure timely resolution. • Call volume and open tickets are reviewed periodically by helpdesk staff.	Inquired of management to determine that helpdesk calls are entered into the call tracking utility and given a ticket number, a priority level is assigned in accordance with company policy, and all issues that cannot be addressed within appropriate time intervals are escalated to management to assure timely resolution.	No exceptions noted.
			Inspected the ticketing system to determine that a priority level is assigned in accordance with company policy, all issues that cannot be addressed within appropriate time intervals are escalated to management to assure timely resolution, and call volume and open tickets are reviewed periodically by helpdesk staff.	No exceptions noted.
		Documented change requests are completed for significant enhancements and new development. Emails serve as documentation for bug fixes and minor enhancements.	Inspected a judgmental sample of product changes from the review period for entries in the tracking system to determine that requests were completed for significant	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			enhancements and new development.	
			Inquired of management to determine that documented change requests are completed for significant enhancements and new development while emails serve as documentation for bug fixes and minor enhancements	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security and related security breaches and other incidents.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding resolution of complaints and requests relating to system security and related issues.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding identifying and mitigating system security and related security breaches and other incidents.	No exceptions noted.
		Policies and procedures are in place to guide personnel regarding addressing how complaints	Inspected the policies and procedures to determine that the	No exceptions noted.

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		and requests relating to security issues are resolved.	entity's policies included procedures regarding resolution of complaints and requests relating to system security and related issues.	
		A ticketing system is utilized to manage systems infrastructure issues and changes. Tickets are assigned to support personnel based on the nature of the ticket.	Inspected a judgmental sample of logs from the ticketing system showing closed tickets to determine that a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on the nature of the ticket.	No exceptions noted.
		Helpdesk calls are entered into the ticketing system and call tracking utility and given a ticket number. • A priority level is assigned in accordance with company policy. • All issues that cannot be addressed within appropriate time intervals are escalated to management to assure timely resolution. • Call volume and open tickets are reviewed periodically by helpdesk staff.	Inquired of management to determine that helpdesk calls are entered into the call tracking utility and given a ticket number, a priority level is assigned in accordance with company policy, and all issues that cannot be addressed within appropriate time intervals are escalated to management to assure timely resolution.	No exceptions noted.
			Inspected the ticketing system to determine that a priority level is assigned in accordance with company policy, all issues that cannot be addressed within appropriate time intervals are escalated to management to assure timely resolution, and call volume and open tickets are reviewed periodically by helpdesk staff.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC7.0 - COMMON CRITERIA RELATED TO SYSTEM OPERATIONS

The criteria relevant to how an entity (i) manages the operation of system(s) and (ii) detects and mitigates processing deviations, including logical and physical security deviations.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Documented change requests are completed for significant enhancements and new development. Emails serve as documentation for bug fixes and minor enhancements.	Inspected a judgmental sample of product changes from the review period for entries in the tracking system to determine that requests were completed for significant enhancements and new development. Inquired of management to determine that documented change requests are completed for significant enhancements and new development while emails serve as documentation for bug fixes and minor enhancements	No exceptions noted. No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	Inspected relevant policies and procedures to determine that policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	No exceptions noted.
		Policies and procedures are in place for classifying data based on its criticality and sensitivity and that classification is one of many factors used to define protection requirements, access rights and restrictions, and retention and destruction requirements.	Inspected the policies and procedures to determine that data classification, protection requirements, access rights, access restrictions, and retention and destruction policies were established.	No exceptions noted.
		Policies and procedures are in place to assign responsibility and accountability for system changes and maintenance.	Inspected the policies and procedures to determine that the entity's policies included procedures regarding assigning responsibility and accountability for system changes and maintenance.	No exceptions noted.
		Policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	Observed and inspected relevant policies and procedures to determine that policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or operating effectiveness of controls	No exceptions noted.

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			are identified during system operation and monitoring.	
		Policies and procedures are in place to guide personnel regarding testing, evaluating, and authorizing system components before implementation.	Inspected the policies and procedures related to testing, evaluating, and authorizing before implementation of components.	No exceptions noted.
		A software development life cycle is utilized to designate milestones that must be achieved throughout the development and testing process.	Inspected software development life cycle documentation to determine that a software development life cycle was utilized to designate milestones that must be achieved throughout the development and testing process.	No exceptions noted.
		Program development is performed on distinct development servers, separate from the production environment.	Observed the location of the servers for each environment to determine that development environment is physically separated from the production environment.	No exceptions noted.
		Version control software is utilized to maintain and control access to current and prior versions of application source code, and the associated reporting and logging functions.	Inspected and observed the version control software to determine that version control software is utilized to maintain and control access to current and prior versions of application code.	No exceptions noted.
		Access to version control software is restricted based upon job responsibilities. Access is restricted to approved positions only.	Inspected access rights to determine that access to version control software is restricted based upon job responsibilities, and that access is restricted to approved positions only.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Documented change requests are completed for significant enhancements and new development. Emails serve as documentation for bug fixes and minor enhancements.	Inspected a judgmental sample of product changes from the review period for entries in the tracking system to determine that requests were completed for significant enhancements and new development.	No exceptions noted.
			Inquired of management to determine that documented change requests are completed for significant enhancements and new development while emails serve as documentation for bug fixes and minor enhancements	No exceptions noted.
		Change management software is utilized to manage application changes, and the associated reporting and logging functions.	Inspected and observed the application to determine that change management software is utilized to manage application changes, and the associated reporting and logging functions.	No exceptions noted.
		Changes to source code results in the creation of a new version of the application code. If necessary, changes can be rolled back to prior versions of the application code.	Inspected a judgmental sample of versioning history to determine that changes to source code resulted in the creation of a new version of the application code.	No exceptions noted.
		Logs are utilized to maintain and record changes to manage and monitor development and maintenance activities.	Inspected a sampling of logs to determine that logs are utilized to maintain and record changes to manage and monitor development and maintenance activities.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The quality assurance and testing efforts are performed in a distinct test environment that is logically separated from the production environment.	Observed the location of the servers for each environment to determine that quality assurance and test environments are logically separated from the production environment.	No exceptions noted.
		Application testing takes place at several different phases of the development cycle: • QA Testing, including regression testing, during feature updates/development. • QA in staging environment.	Inquired of management to determine that application testing takes place at different phases of the development cycle.	No exceptions noted.
		Management approvals are obtained before application code changes are migrated to the production environment.	Inquired of management to determine that management approvals were obtained before application code changes were migrated to the production environment.	No exceptions noted.
		Major changes requiring significant downtime to the application are rolled to production after hours. Emergency changes take place immediately.	Inquired of management to determine that major changes requiring significant downtime are rolled to production after hours, while emergency changes take place immediately.	No exceptions noted.
		A ticketing system is utilized to manage systems infrastructure issues and changes. Tickets are assigned to support personnel based on the nature of the ticket.	Inspected a judgmental sample of logs from the ticketing system showing closed tickets to determine that a ticketing system was utilized to manage systems infrastructure issues, and tickets were assigned to support personnel based on the nature of the ticket.	No exceptions noted.

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A standard hardened template for virtualized environments is utilized for installation and maintenance of certain critical virtual machines.	Inspected the virtualization configurations to determine that a standard template is used for installation and maintenance of certain critical SIG virtual machines.	No exceptions noted.
		Critical production equipment is maintained under warranty and maintenance or Service Level Agreements (SLAs) with 3rd party vendors.	Inquired of management to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.	No exceptions noted.
			Inspected current agreements with third party vendors to determine that certain production equipment is maintained under warranty and maintenance or service level agreements with 3rd party vendors.	No exceptions noted.
		A management-approved methodology is utilized to monitor operating system patch releases, distribute patches to relevant devices and apply the patches to the device.	Inquired of management to determine that a methodology is utilized to monitor operating system patch releases, distribute patches to relevant devices and apply the patches to the device.	No exceptions noted.
			Inspected a judgmental sample of servers and workstations to determine that a management-approved methodology is utilized to monitor operating system patch releases, distribute patches to relevant devices and apply the patches to the device.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC8.0 - COMMON CRITERIA RELATED TO CHANGE MANAGEMENT

The criteria relevant to how an entity (i) identifies the need for changes, (ii) makes the changes using a controlled change management process, and (iii) prevents unauthorized changes from being made.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Infrastructure changes, patches and upgrades to critical services are tested by the technical support department before being applied to a production server.	Inquired of management to determine that infrastructure changes, patches and upgrades to critical services are tested by the technical support department after hours before being introduced to a production server.	No exceptions noted.
		SIG utilizes the services and controls of a third party data center for housing critical production computer servers, applications, and networking equipment. The third party data center is responsible for the general IT controls relevant to its application development.	Inspected the most recent SOC audit report for the third party data center to determine that the third party data center is responsible for the general IT controls relevant to its application development.	No exceptions noted.
		SIG utilizes the services and controls of a third party data center for housing critical production computer servers, applications, and networking equipment. The third party data center is responsible for the general IT controls relevant to its change management.	Inspected the most recent SOC audit report for the third party data center to determine that the third party data center is responsible for the general IT controls relevant to its change management.	No exceptions noted.
		SIG management reviews the SOC audit report of the third party data center annually and documents the results of the review of the SOC audit report in a memo.	Inquired of management to determine that SIG management reviews the SOC audit report of the third party data center annually.	No exceptions noted.
			Inspected management's memo to determine that SIG management documents the results of the review of the SOC report in a memo.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC9.0 - COMMON CRITERIA RELATED TO RISK MITIGATION

The criteria relevant to how the entity identifies, selects and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A formal risk assessment is performed on an annual basis. Risks identified are evaluated along with mitigation strategies and are formally documented in memo form. The risk assessment includes, but is not limited to, the following areas: • Data security (company data and client data). • Potential fraud and misconduct including how management and staff might engage in inappropriate actions from the use of IT and access to information. • Regulatory, economic, and physical environment in which the company operates. • Business environment, including industry, competitors, regulatory environment, and consumers. • Potential impact of new business lines, dramatically altered business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies. • Management and respective attitudes and philosophies on the system of internal control. • Vendor and business partner relationships including third party data centers. • Systems and technology environment.	Inspected the annual risk assessment documentation to determine that a formal risk assessment was performed during the review period and that identified risks and mitigation strategies were formally documented.	No exceptions noted.

MATRIX 1 CRITERIA COMMON TO CATEGORIES OF SECURITY, AVAILABILITY, AND CONFIDENTIALITY

CC9.0 - COMMON CRITERIA RELATED TO RISK MITIGATION

The criteria relevant to how the entity identifies, selects and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Procedures have been implemented to provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies.	Inspected confidentiality policies and procedures related to disclosure to third parties to determine that confidential information is disclosed to third parties is done in accordance with the entity's defined confidentiality and related security policies.	No exceptions noted.
		Procedures have been implemented to obtain assurance or representation that the policies of third parties to whom information is transferred are in conformity with the SIG policies related to confidentiality.	Inspected confidentiality policies and procedures implemented which help to obtain assurance or representation that the policies of third parties to whom information is transferred are in conformity with the SIG policies related to confidentiality.	No exceptions noted.
		Prior to collecting personal information of external users, a privacy policy is provided that may include the purpose and use of the personal information, including detailed use, ability to opt-out, enhancement (enrichment), sharing, disclosure, access, security, retention, breach notification requirements, and disposal of personal information.	Inspected policies to determine that if personal information of external users is collected, a privacy policy is provided that may include the purpose and use of the collection of their personal information, including detailed use, ability to opt-out, enhancement (enrichment), sharing, disclosure, access, security, retention, breach notification requirements, and disposal of personal information.	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR CATEGORY OF AVAILABILITY

Availability Category and Criteria Table
The availability category refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Policies and procedures are in place to guide personnel regarding monitoring system capacity to achieve customer commitments or other agreements regarding availability.	Inspected the policies and procedures to determine that policies and procedures were in place to guide personnel regarding monitoring system capacity to achieve customer commitments or other agreements regarding availability.	No exceptions noted.
		Policies and procedures are in place for identifying and documenting the system availability and related security requirements of authorized users.	Inspected the policies and procedures to determine that the entity's system availability and related security policies were established.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Policies and procedures are in place to guide personnel regarding the identification of and consistency with defined commitments, service-level agreements, and other contractual requirements.	Inspected the policies and procedures and the service level agreements to determine that the entity's policies included procedures regarding the identification of and consistency with defined commitments, service-level agreements, and other contractual requirements.	No exceptions noted.
		The climate control system regulates both temperature and humidity levels within the facilities.	Observed climate control system to determine that it regulates temperature and humidity levels within the facilities.	No exceptions noted.
		The property manager inspects and maintains the climate control systems on a regular basis.	Inspected the most recent inspection results to determine that the property manager inspects the climate control systems on a regular basis.	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR CATEGORY OF AVAILABILITY

Availability Category and Criteria Table
The availability category refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Equipment in the server room is connected to UPS systems to provide temporary electricity in the event of short term power outages, and to mitigate the risk of power fluctuations impacting equipment in the server room.	Observed the UPS systems to determine that the equipment in the server room was connected to UPS systems to provide temporary electricity in the event of a power outage and mitigate the risk of power fluctuations impacting equipment in the server room.	No exceptions noted.
		The UPS and battery systems are inspected and maintained on a regular basis by IT staff.	Inspected the most recent maintenance reports results to determine that IT staff inspects and maintains the UPS and battery systems on a regular basis.	No exceptions noted.
		SIG utilizes the services and controls of a third party data center for housing critical production computer servers, applications, and networking equipment. The environmental security and maintenance controls at the third party data center are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	Inspected the most recent SOC audit report for the third party data center to determine that the environmental security and maintenance controls at the third party data center are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	No exceptions noted.
		SIG utilizes the services and controls of a third party data center for housing critical production computer servers, applications, and networking equipment. The third party data center is responsible for the controls relevant to the completeness and accuracy of specified reports provided to and used by SIG.	Inspected the most recent SOC audit report for the third party data center to determine that SIG utilizes relevant reports provided by the third party data center.	No exceptions noted.
		SIG management reviews the SOC audit report of the third party data center annually and documents the results of the review of the SOC audit report in a memo.	Inquired of management to determine that SIG management reviews the SOC audit report of the third party data center annually.	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR CATEGORY OF AVAILABILITY

Availability Category and Criteria Table
The availability category refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected management's memo to determine that SIG management documents the results of the review of the SOC report in a memo.	No exceptions noted.
		SIG has implemented a backup policy, and backups of production systems and data are completed in a timely manner. The retention period for backup data has been defined by management.	Inquired of management to determine that SIG has implemented a backup policy, and that backups of production systems and data are completed in a timely manner.	No exceptions noted.
			Inspected the backup policy, backup configurations, and a judgmental sample of backup logs to determine that SIG has implemented a backup policy, and that backups of production systems and data are completed in a timely manner.	No exceptions noted.
			Inspected the backup policy and backup configurations to determine that the retention period for backup data has been defined by management.	No exceptions noted.
		Logs track the backup events, and success and failure alerts are sent to IT staff, which investigate any failures, and remediate as necessary.	Inspected a judgmental sample of backup event logs and success/failure alerts to determine that logs track the backup events, and success and failure alerts are sent to IT staff.	No exceptions noted.
			Inquired of management to determine that failures are investigated and remediated.	No exceptions noted.

MATRIX 2 ADDITIONAL CRITERIA FOR CATEGORY OF AVAILABILITY

Availability Category and Criteria Table
The availability category refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Certain servers are replicated to an offsite server environment.	Inspected the server configurations to determine that certain servers are replicated to an offsite server environment.	No exceptions noted.
		SIG employs block level replication, allowing for operating system and data restoration of any production server. Servers can be quickly rolled back to a previous virtual instance of that server environment in the event of patch related or other issues.	Inspected a judgmental sample of snapshot configurations on the backup server to determine that any production server could be quickly rolled back to a previous virtual instance of that server environment in the event of patch related or other issues.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Policies and procedures are in place to guide personnel regarding recovering and continuing service in accordance with documented customer commitments or other agreements.	Inspected the policies and procedures and service level agreements to determine that policies and procedures were in place to guide personnel regarding recovering and continuing service in accordance with documented customer commitments or other agreements.	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR CATEGORY OF CONFIDENTIALITY

Confidentiality Category and Criteria Table
The confidentiality category refers to the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Policies and procedures are in place to communicate retention periods for confidential information maintained by SIG. Procedures are in place to: • Automatically delete confidential information in accordance with specific retention requirements. • Delete backup information in accordance with defined schedules. • Require approval for confidential information to be retained beyond its retention period. • Review annually information marked for retention.	Inspected SIG's retention policies for confidential information to determine that the policies included procedures to: • Automatically delete confidential information in accordance with specific retention requirements. • Delete backup information in accordance with defined schedules. • Require approval for confidential information to be retained beyond its retention period. • Review annually information marked for retention.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Policies and procedures are in place to communicate SIG's destruction policy for confidential information.	Inspected the destruction policy to determine that policies and procedures are in place to communicate SIG's destruction policy for confidential information.	No exceptions noted.
		The entity: • locates and removes or redacts specified confidential information as required. • regularly and systematically destroys, erases, or makes anonymous confidential information that is no longer required for the purposes identified in its confidentiality commitments or system requirements.	Inquired of management to determine that the entity: • locates and removes or redacts specified confidential information as required. • regularly and systematically destroys, erases, or makes anonymous confidential	No exceptions noted.

MATRIX 3 ADDITIONAL CRITERIA FOR CATEGORY OF CONFIDENTIALITY

Confidentiality Category and Criteria Table
The confidentiality category refers to the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives.

Control Point	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		• erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based). • disposes of original, archived, backup, and ad hoc or personal copies of records in accordance with its destruction policies. • documents the disposal of confidential information.	information that is no longer required for the purposes identified in its confidentiality commitments or system requirements. • erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based). • disposes of original, archived, backup, and ad hoc or personal copies of records in accordance with its destruction policies. • documents the disposal of confidential information. Inspected documentation to determine that the entity documents the disposal of confidential information.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT RESPONSE TO TESTING EXCEPTIONS

Criteria Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Management Response to Testing Exceptions
CC6.2	Management utilizes a new hire checklist to ensure that specific elements of the hiring process are consistently executed. A copy of the checklist is kept in the employee file.	Inspected a judgmental sample of new hire checklists used for employees hired during the review period to determine that management utilizes a new hire checklist for the employees and that the checklist is kept in the employee files.	Exception noted: No new hire checklists were available for review from the new hire list. Management Response: On boarding and off boarding forms are used to automate communications between HR and IT. This includes a checklist for the required setup. When HR submits their requests, those requests are added to the IT Team project board to be prioritized.
CC6.2	A formal process is in place to ensure HR informs IT when employee access to company IT resources needs to be added or removed.	Inspected a judgmental sample of communications between HR and IT (tickets or emails or checklists) to determine that a formal process is in place to ensure HR informs IT when employee access to company IT resources needs to be added or removed.	Exception noted: No communications between HR and IT were available for review from the new hire or termination list. Management Response: On boarding and off boarding forms are used to automate communications between HR and IT. When HR submits their requests, those requests are added to the IT Team project board and prioritized.
CC6.2 CC6.3 CC6.5	Management revokes corporate network and production server connection privileges assigned to terminated employees as a component of the employee termination process.	Inspected a judgmental sample of domain user listings to determine that management revoked corporate network access privileges assigned to terminated employees as a component of the employee termination process.	Exception noted: Accounts for three of the six terminated employees sampled were still active. Management Response: On occasion, terminated employees remain as contract employees and retain some level of network access. We also have terminated employees whose direct access has been blocked, but their accounts remain active and are shared with active employees for the purpose of account management until customers are familiar with new account managers and a formal transition of account owner occurs.

END OF REPORT