360ADVANCED

SOC 2 TYPE 2 REPORT ON CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY FOR ONLINE UNDERWRITING SERVICES

R.C. GILTNER SERVICES, INC.

SEPTEMBER 1, 2016 TO AUGUST 31, 2017

Business MinuteLender

Minute Lender

PaySound®

AICPA Service Organization Control Reports
AICPA
SOC
aicpa.org/soc
Formerly SAS 70 Reports

R.C. GILTNER SERVICES, INC.

Table of Contents

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

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 R.C. Giltner Services, Inc.:

Scope

We have examined the description of R.C. Giltner Services, Inc.'s ("R.C. Giltner") Online Underwriting Services system based on the criteria set forth in paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the Security, Availability, and Confidentiality principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria), throughout the period September 1, 2016 to August 31, 2017.

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of R.C. Giltner's controls are suitably designed and operating effectively, along with the related controls of the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls. The controls included in the description are those that management of R.C. Giltner believes are likely to be relevant to meeting the applicable trust services criteria, and the description does not include those aspects of the Online Underwriting Services system that are not likely to be relevant to meeting the applicable trust services criteria.

R.C. Giltner uses Microsoft Corporation ("Microsoft"), a sub-service organization, for application cloud hosting services. The description indicates that certain applicable trust services criteria can only be met if certain types of controls at the sub-service organization are suitably designed and operating effectively. The description presents R.C. Giltner's system; its controls relevant to the applicable trust services criteria; and the types of controls that R.C. Giltner expects to be implemented, suitably designed, and operating effectively at the sub-service organization to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the sub-service organization. Our examination did not extend to the services provided by the sub-service organization, and we have not evaluated whether the controls management expects to be implemented at the sub-service organization have been implemented or whether such controls were suitably designed and operating effectively throughout the period September 1, 2016 to August 31, 2017.

Service Organization's Responsibilities

Within Section 2 of this report, R.C. Giltner has provided an assertion about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. R.C. Giltner is responsible for (1) preparing the description and assertion; (2) including the completeness, accuracy, and method of presentation of the description and assertion; (3) providing the services covered by the description; (4) identifying the risks that would prevent the applicable trust services criteria from being met; (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria; and (6) specifying the controls that meet the applicable trust services criteria and stating them in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and, accordingly, included procedures that we considered necessary in the circumstances. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period September 1, 2016 to August 31, 2017.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria involves:

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period September 1, 2016 to August 31, 2017;
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively;
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met; and
- evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in its assertion.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in R.C. Giltner's assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented throughout the period September 1, 2016 to August 31, 2017;
b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period September 1, 2016 to August 31, 2017, and the sub-service organization and user entities applied the complementary controls assumed in the design of R.C. Giltner's controls throughout the period September 1, 2016 to August 31, 2017; and
c. the controls tested operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period September 1, 2016 to August 31, 2017 if user entities and sub-service organization applied the complementary controls assumed in the design of R.C. Giltner's controls and those controls operated effectively throughout the period September 1, 2016 to August 31, 2017.

Description of Tests of Controls

The specific controls we tested, the tests we performed, and the results of our tests are presented in Section 4 of this report.

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 R.C. Giltner, user entities of R.C. Giltner's Online Underwriting Services system during some or all of the period September 1, 2016 to August 31, 2017; and prospective user entities, independent auditors and practitioners providing services to such user entities, 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, sub-service organizations, and other parties;
- Internal control and its limitations;
- The nature of user entity controls and responsibilities, and their role in the user entities internal control as they relate to, and how they interact with, related controls at the service organization to meet the applicable trust services criteria;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

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

May 9, 2018
St. Petersburg, Florida

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

May 9, 2018

We have prepared the description of R.C. Giltner Services, Inc.'s ("R.C. Giltner") Online Underwriting Services system based on the criteria for a description of a service organization's system identified in paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide users with information about the Online Underwriting Services, particularly system controls intended to meet the criteria for the Security, Availability, and Confidentiality principles set forth in TSP section 100A*, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services principles), throughout the period September 1, 2016 to August 31, 2017. We confirm, to the best of our knowledge and belief, that

1) The description fairly presents the Online Underwriting Services system throughout the period September 1, 2016 to August 31, 2017. R.C. Giltner uses Microsoft Corporation ("Microsoft"), a sub-service organization, for application cloud hosting services. The description included in Section 3 includes only the applicable trust services criteria and related controls of R.C. Giltner and excludes the applicable trust services criteria and related controls of the sub-service organization. Our assertion is based on the following description criteria:
    a) The description contains the following information:
        1. the types of services provided;
        2. the components of the system used to provide the services, which are the following:
            - *Infrastructure* - the physical structures, IT and other hardware;
            - *Software* - the application programs and IT system software that supports application programs;
            - *People* - the personnel involved in the governance, operation, and use of a system;
            - *Procedures* - the automated and manual procedures; and
            - *Data* – transaction streams, files, databases, tables, and output used or processed by the system.
        3. the boundaries or aspects of the system covered by the description;
        4. for information provided to, or received from, sub-service organizations, and other parties
            a. how such information is provided or received and the role of the sub-service organization and other parties
            b. the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls
        5. the applicable trust services criteria and related controls designed to meet those criteria, including, as applicable, the following:
            a. complementary user entity controls contemplated in the design of the service organization's system
            b. when the inclusive method is used to present a sub-service organization, controls at the sub-service organization
        6. if the service organization presents the sub-service organization using the carve-out method
            a. the nature of the services provided by the sub-service organization

b. each of the applicable trust services criteria that are intended to be met by controls at the sub-service organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out sub-service organizations to meet those criteria

7. any applicable trust services criteria that are not addressed by a control at the service organization or a sub-service organization and the reasons; and
8. relevant details of changes to the service organization's system during the period covered by the description.

b) The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

2) The controls in the description were suitable designed throughout the period September 1, 2016 to August 31, 2017, to meet the applicable trust services criteria.

3) The controls stated in the description operated effectively throughout the period September 1, 2016 to August 31, 2017, to meet the applicable trust services criteria.

/s/ R.C. Giltner Services, Inc.

Gregory S. Schreacke – Chief Executive Officer

Sam French – Chief Information Officer

SECTION 3:

R.C. GILTNER'S DESCRIPTION OF CONTROLS

SCOPE OF REPORT AND DISCLOSURES

Overview

This description of the system of controls provided by R.C. Giltner Services, Inc.'s ("R.C. Giltner") management, as related to Standards for Attestation Engagements No. 18 '*Attestation Standards: Clarification and Recodification*', specifically AT-C 105, '*Concepts Common to All Attestation Engagements*' and AT-C Section 205, '*Examination Engagements*,' considers the direct and indirect impact of risks and controls that R.C. Giltner's management has determined are likely to be relevant to its user entities' internal controls intended to mitigate risks related to security, availability, processing integrity, confidentiality, or privacy.

Principles and Related Criteria

The five attributes of a system are known as *principles*, and they are defined as follows:

- **Security**: The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements. The *security principle* refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.
- **Availability**: The system is available for operation and use to meet the entity's commitments and system requirements. The *availability principle* refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The *availability principle* does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.
- **Processing Integrity**: System processing is complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements. The *processing integrity principle* refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the system achieves its aim or the purpose for which it exists, and whether it performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Processing integrity does not automatically imply that the information received and stored by the system is complete, valid, accurate, current, and authorized. The risk that data contains errors introduced prior to its input in the system often cannot be addressed by system controls and detecting such errors is not usually the responsibility of the entity. Similarly, users outside the boundary of the system may be responsible for initiating processing. In these instances, the data may become invalid, inaccurate, or otherwise inappropriate even though the system is processing with integrity.
- **Confidentiality**: Information designated as confidential is protected to meet the entity's commitments and system requirements. The *confidentiality principle* addresses the system's ability to protect information designated as confidential, including, its final disposition and removal from the system in accordance with management's commitments and system requirements. Information is confidential if the custodian of the information is required to limit its access, use, and retention, and restrict its disclosure to defined parties. Such requirements may be contained in laws or regulations, or commitments in user contracts. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy only applies to personal information, while the confidentiality principle applies to various types of sensitive information. In addition, the privacy principle addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information.

Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

- **Privacy**: Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.

Many of the criteria used to evaluate a system are shared amongst all of the principles; for example, the criteria related to risk management apply to the security, availability, processing integrity, confidentiality, and privacy principles. As a result, the trust services criteria of (1) criteria common to all five principles (common criteria) and (2) additional principle specific criteria for the availability, processing integrity, confidentiality, and privacy principles. For the security principle, the common criteria constitute the complete set of criteria. For the principles of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of the common criteria and the criteria applicable to the principle(s) addressed by the engagement. The criteria for a principle addressed by the engagement are considered to be complete only if all of the criteria associated with that principle are addressed by the engagement.

The common criteria are organized into seven categories:

a. *Organization and management.* The criteria relevant to how the organization is structured and the processes the entity has implemented to manage and support people within its operating units to meet the criteria for the principle(s) addressed by the engagement. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

b. *Communications*. The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and system requirements to authorized users and other parties of the system to meet the criteria for the principle(s) addressed by the engagement.

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

d. *Monitoring of controls.* The criteria relevant to how the entity monitors the system, including the suitability of the design and operating effectiveness of the controls, and takes action to address deficiencies identified to meet the criteria for the principle(s) addressed by the engagement.

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

f. *System operations.* The criteria relevant to how the entity manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the criteria for the principle(s) addressed in the engagement.

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

Although the confidentiality principle applies to various types of sensitive information, the privacy principle applies only to personal information. If the entity is directly responsible for providing services to data subjects covering all of the categories noted as follows, then the privacy principle may be appropriate. If

the entity is not directly responsible for significant aspects of the following categories but retains responsibility for protecting personal information, the confidentiality principle may be more applicable.

The privacy criteria are organized into eight categories:

a. *Notice and communication of commitments and system requirements.* The entity provides notice to data subjects about its privacy practices, its privacy commitments, and system requirements.

b. *Choice and consent.* The entity communicates choice available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.

c. *Collection.* The entity collects personal information to meet its privacy commitments and system requirements.

d. *Use, retention, and disposal.* The entity limits use, retention, and disposal of personal information to meet its privacy commitments and system requirements.

e. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its privacy commitments and system requirements.

f. *Disclosure and notifications.* The entity discloses personal information, with the consent of the data subjects, to meet its privacy commitments and system requirements. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its privacy commitments and system requirements.

g. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its privacy commitments and system requirements.

h. *Monitoring and enforcement.* The entity monitors compliance to meet its privacy commitments and system requirements including procedures to address privacy-related inquiries, complaints, and disputes.

The scope management has determined appropriate for the Online Underwriting Services system includes the controls to meet the criteria for the Security, Availability, and Confidentiality principles. R.C. Giltner is responsible for identification of risks associated with the system of controls (defined as Principles), and for the design and operation of controls intended to provide reasonable assurance that the applicable trust services criteria would be met.

As part of its overall SOC 2 program, R.C. Giltner management sets and determines the scope and timing of each report. This description of the system has been prepared by R.C. Giltner management to provide information on controls applicable to meet the criteria for the Security, Availability, and Confidentiality principles for the Simpsonville, Kentucky facility.

Sub-Service Organizations

R.C. Giltner uses Microsoft Corporation (“Microsoft”), a sub-service organization, for application cloud hosting services. R.C. Giltner has agreements in place to manage the relationship with Microsoft and relies on Microsoft for the physical and environmental security over its IT infrastructure. R.C. Giltner reviews the Service Auditor’s report on an annual basis to monitor and evaluate the design and operating effectiveness of controls to secure R.C. Giltner’s data.

Significant Changes during the Examination Period

Management is not aware of any significant changes that occurred during the examination period.

Subsequent Events

Management is not aware of any relevant events that occurred subsequent to the period covered by management's description included in Section 3 of this report through the date of the service auditor's report that would have a significant effect on management's assertion.

Using the Work of the Internal Audit Function

The service auditor did not utilize any work of an Internal Audit function in preparing this report.

OVERVIEW OF OPERATIONS AND THE SYSTEM

Company Overview and Background

R.C. Giltner Services, Inc. ("R.C. Giltner") was founded in 2012 to provide revenue enhancing services to financial institutions under $10 Billion serving customers with checking and liquidity services, including small dollar loans.

Based in Simpsonville, Kentucky, R.C. Giltner focuses on the improvement of financial institution service charge revenue by providing new product services with automated underwriting and delivery of small dollar loans. These products and services with related consulting and systems are marketed through financial institutions under the PaySound[SM] brand.

Overview of Online Underwriting Services System

R.C. Giltner's Online Underwriting Services web-based suite PaySound[SM] represents a combination of product, online automation, software, website, processes, consulting and training that delivers to financial institutions and their customers services defined below:

- A consumer web-based solution for in-home or in-branch use exclusively serving financial institutions;
- Automating real-time access, underwriting, and delivery of competitively priced loans $200 to $50,000;
- Providing marketing tools and process winning existing customers and new prospects;
- Using deposit data and statement balances, and credit scores at the customer's option to underwrite loans;
- Driving 30% growth in compliant service charge revenue consumers willingly pay; and
- Does not risk current revenues earned by the financial institution.

PaySound[SM] is a multi-user web-based suite allowing banks to market a package account of services including checking account services, credit score information, and small loans $200 to $50,000, underwrite loans in an automated, compliant way with the required customer electronic signatures and communication, and set up the marketing products and services in an automated way. The services can be through self-service by consumers or with bank employees in a branch environment. Further, the suite allows financial institution employees tools through the website to establish users and controls, manage customer data, customer communication, actions relative to customer service operations and reporting for financial institution use.

OVERVIEW OF RELEVANT INFRASTRUCTURE

The Online Underwriting Services system is comprised of the following components:

- Infrastructure – the physical structures, IT, and other hardware;
- Software – the application programs and IT system software that supports application programs;
- People – the personnel involved in the governance, operation, and use of a system;
- Procedures – the automated and manual procedures; and
- Data – transaction streams, files, databases, tables, and output used or processed by the system.

Infrastructure

The PaySound[SM] website and software application is hosted within the Microsoft Windows Azure datacenters. To provide PaySound[SM] services, R.C. Giltner maintains five MS Windows Server 2012 R2 servers in the Microsoft Windows Azure cloud services as follows:

- Domain Controller 1 to provide authentication and active directory services;
- Domain Controller 2 to provide for automatic rollover in the event of Domain Controller 1 failure;
- Two clustered SQL Servers that provide failover; and
- A Witness server that votes on which SQL Server is Primary in the cluster.

The PaySound[SM] application is a web-based solution accessed via the Microsoft Windows Azure cloud platform using a browser and a secure sockets layer (SSL) connection only. The architecture is wholly contained within Microsoft Windows Azure cloud and access is restricted to the web-based platform.

PaySound[SM] runs on top of Azure Cloud Services using the latest Windows Server Operating System (OS) and Microsoft Internet Information Server (IIS). Application packages are created at development time that can be used to scale out the number of OS / IIS instances that are deployed to handle web traffic automatically by Azure based on demand. Windows Azure load balances all traffic across the deployed instances.

The PaySound[SM] application stores and retrieves data from the clustered SQL Servers, database backend. The database backend runs on top of a high-availability Microsoft SQL Server cluster with automatic failover.

The following describes the in-scope components supporting the Online Underwriting Services system:

System / Application	Description	Infrastructure
PaySound[SM]	PaySound[SM] is a secure online portal that allows banks to market an application that can underwrite loans in an automated, compliant way with all necessary customer electronic signatures and communication, and set up the marketing products and services in an automated way.	MS Windows Vista/ Windows 7/Windows 8/Windows 10 MS Office 2007/2010/2013/365 Office 365 (E-mail Services) MS Windows Server 2012 R2 MS SQL Server 2012 (Failover Cluster)

Software

The Online Underwriting Services software, PaySound[SM], is web-based solution that provides financial institutions with the following functionality:

- Web-based access, financial institution branding and marketing of the services through a web site with product and loan features, pricing and information, FAQs, blog, news, privacy policy, financial institution information, required marketing documentation and policies in addition to traditional marketing methods;

- Web-based access also allows customers to use the site for learning loan availability or requesting set up of loans and checking accounts after requiring customers to log in to the website to use the site, with appropriate log in credentialing and support processes;

- Web-based bank user administration, user log in with appropriate passwords and credentialing and use under a "Management" portal as granted by an administrator;

- Underwriting in real time on the site of line of credit loans up to $1,000 with no credit score through capturing, importing, and analyzing deposit data of bank customers and at their volition using the data to define loan availability for customers. The site allows requesting customer last name, birthday and last four digits of the social security number at the web site for customer identification and loan availability presentation;

- Underwriting line of credit loans through credit score data and available deposit data for line of credit loan of $1,000, $2,500 or up to $50,000 through also interfacing with a third party credit information site, Clarity Services, that the bank contracts directly with for their site's access for credit score and related information. The site allows requesting customer last name, birthday and full social security number (but not stored) at the web site for customer identification and loan availability presentation;

- Notifications to customers concerning loan requests including documentation of their request and related deposit or credit score information collected, approval of their loan request, compliant adverse action notices if their loan request is denied, FACTA documentation if their loan request includes use of a credit score and their credit report request indicates a mismatch with name, address and / or social security or a high likelihood of fraud along with process to resolve the discrepancy;

- The opportunity for the customer to set up checking and loan accounts by reviewing and approving all necessary e-signature documents, bank disclosures, checking account feature choices, bank loan agreements and repayment methods;

- The website also provides to the customer communication of all actions taken along with copies of the documents, agreements and disclosures in pdf form by email executed by the customer;

- The website provides many specific features for the financial institution's use:
    - Administrator set up and management of authorization, passwords and levels of use for users;
    - Data management and uploading to the site by the financial institution along with activity history. File extract definition and organization behind the financial institution's firewall of information to be uploaded daily to the web site, upload processes to the web site with customer information masking and hashing prior to leaving from behind the financial institution's firewall, and secure storage of information;
    - Daily action cards and process managements for employees based on customer initiated actions of checking account set up, loan set up and disposition of these activities by

financial institution employees integrated with customer communication through the website, along with PDF archiving of data for cold storage of data for the financial institution;

- Reports for financial institution use including:
  - archive of website activity by customers;
  - analysis file download of record information including product types, balances, activity, NSF/ODs, loans, age, “reg e opt” status, debit card usage and deposit activity with all customer information removed;
  - daily loan activity by financial institution employees;
  - Checking and loan account volumes, descriptive characteristics and activity month-to-date and year-to-date; and
- General operational settings for the financial institution using the site including:
  - Customer service phone number displayed;
  - Product codes bank uses for PaySound℠ accounts; and
  - URLs the site references of the financial institution and disclosures provided by the financial institution.
- Test accounts set up and removal for training;
- Email templates set up and management;
- User management set up and settings; and
- Credit underwriting criteria used by the site under the financial institution’s direction.

People

R.C. Giltner has five main divisions: (1) Sales; (2) Client Services; (3) Implementation; (4) Technology; and (5) Human Resources (HR) / Administration.

The roles and responsibilities of key functions include the following:

- **Chief Executive Officer (CEO) and Sales**
  - Provides high-level decisions on policy, strategy, product definition, and day-to-day operations;
  - Leads the Sales and Marketing efforts;
  - Advises the Board of Directors, motivates employees, and drives change within the organization; and
  - Speaks at industry conferences and trade shows.
- **Chief Information Officer (CIO)**
  - Works with RCG team and external auditors to develop and maintain controls providing a secure and stable environment for RCG products and services;
  - Manages a team of developers utilizing an electronic ticketing system for tracking issues;
  - Maintains SOC 2 documentation and aides in all technical aspects of product delivery; and
  - Manages technical implementation of PaySound℠ engagements.

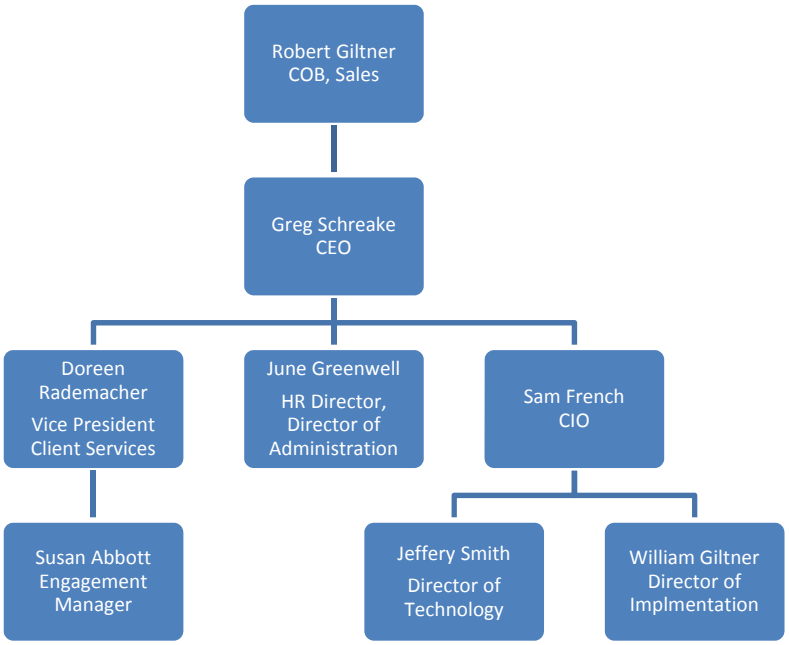
- **Director of Technology**
    - Develop the Company's proprietary software to specifications;
    - Maintain the development and proper working of the software;
    - Ensure the services are understood and implemented to ensure customer satisfaction, regulatory compliance, and operational to the Company specifications; and
    - Comply with and assist others in complying with all relevant laws, regulations, and policies.

- **Director of Implementation**
    - Kick off meeting with the customer;
    - Define and outline the project implementation schedule;
    - Guide customer through the implementation process with regular meetings ensuring the project remains on schedule;
    - Ensure the services are understood and implemented to ensure customer satisfaction, regulatory compliance, and operational to the Company specifications; and
    - Comply with and assist others in complying with all relevant laws, regulations, and policies.

- **Client Services**
    - Responsible for implementation assisting the customer marketing of the products and services;
    - Ongoing customer management and client satisfaction;
    - Ensure client is using the products and services to the fullest extent and assist client with monthly, quarterly, and annual marketing of the services;
    - Kick off meeting with the customer;
    - Define and outline the project implementation schedule;
    - Guide customer through the implementation process with regular meetings ensuring the project remains on schedule;
    - Ensure the services are understood and implemented to ensure customer satisfaction, regulatory compliance, and operational to the Company specifications; and
    - Comply with and assist others in complying with all relevant laws, regulations, and policies.

- **Director of HR and Administration**
    - Payroll and payroll administration including appropriate tax return filings;
    - Monthly billing and collections;
    - Accounts payable processing and reconciliation;
    - Prepare monthly financial statements for management and the Board of Directors;
    - Handle miscellaneous general ledger and checking account reconciliations;
    - Manage personnel records and related HR policies and procedures; and
    - Comply with and assist others in complying with all relevant laws, regulations, and policies.

The following is the organizational reporting structure as of August 31, 2017:



Procedures

R.C. Giltner has developed and communicated to its users, procedures to ensure the security, availability, and confidentiality of the Online Underwriting Services system. The policies and procedures include, but not limited to the following key areas:

- Acceptable Use Policy
- IT Policy
- Security Awareness Policy
- Communications Management Policy
- Third Party Services and Software Policy
- Confidentiality Policy
- Employee and Contractor Agreement
- Client Service Policy
- Business Continuity Plan
- Asset Management Policy
- Change Management Policy
- Incident Response Plan
- Data Classification Policy
- HR New Employee On-boarding and Employee Exit Check List

Data

The PaySound[SM] application is provided via a secure online portal that allows banks to underwrite loans in an automated, compliant way with the required customer electronic signatures and communication, and set up the marketing products and services in an automated way. The services can be through self-service by consumers or with bank employees in a branch.

Data as defined by R.C. Giltner constitutes the following:

- Financial institution uploads archived in a database;
- Credit scoring engine to determine loan thresholds to be offered to the institutions clients;
- Performance reporting; and
- Reports that can be securely downloaded to the institutions COLD Storage.

RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATIONS SYSTEMS, MONITORING, POLICIES AND PRACTICES

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal controls, providing discipline and structure. Aspects of R.C. Giltner's control environment that affect the services provided and / or the system of controls are identified in this section.

Integrity and Ethical Values

The effectiveness of controls is greatly influenced by the level of integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are important elements of R.C. Giltner control environment, affecting the design, administration, and monitoring of other components. The communication and implementation of ethical behavior throughout the organization is designed to reduce the likelihood of personnel to engage in dishonest, illegal, or unethical acts.

R.C. Giltner enforces high ethical standards in all levels of communication to and through its employees. R.C. Giltner continuously audits its employees' communication with customer and outside resources to ensure compliance with these standards and addresses any issues as soon as they arise. R.C. Giltner emphasizes high standards during all of its interpersonal communications via meetings, email and phone calls. Any questionable acts are dealt with immediately and positive acts are recognized and acknowledged in public forums in an effort to reinforce positive / constructive behaviors. Employees who violate these standards are disciplined according to company policies.

Board of Directors

R.C. Giltner's control consciousness is influenced significantly by its Board of directors. Attributes include the Board's independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors. A Board of Directors oversees R.C. Giltner's management activities and includes the company's owners and key executive members of management.

Commitment to Competence

Management has established a framework for the basic skills necessary to perform each of the jobs at R.C. Giltner. This framework is then augmented with more specific requirements for each position and for additional specialization within each position based upon any other skills an employee may have. The job descriptions for each position are descriptive, but remain fairly broad because of the nature of the work for which each position is responsible. The employee understands that there are general skills that all people within their given role must have and that the job description augments those skills.

Management's Philosophy and Operating Style

R.C. Giltner management philosophy and operating style is ultimately responsible for the system of internal controls. Virtually all employees have some role in controlling the organization. Some controls are established at the organization level, and management of the local unit establishes others. Management has formal policies and procedures in place to guide personnel on specific information processing functions.

Organizational Structure

Management has designed the organizational structure to provide quality service and accountability in support of R.C. Giltner's' mission. In order to achieve quality in performance, they strive for continuous improvement in all that is done, plan and commit to accomplish targets, and are empowered to perform their duties. R.C. Giltner's operations are highly specialized and require the ability to adapt to industry changes and best practices. R.C. Giltner has a centralized, flat management framework, which allows them to quickly react to industry changes and have excellent response times to customer needs. In addition, the CEO is an active participant in day-to-day operations and all managers' report directly to him. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.

HR Policies and Practices

R.C. Giltner's HR policies and practices are clearly written and communicated where appropriate. Policies and procedures that are listed in the employee handbook include hiring, training, disciplinary actions and termination procedures.

Risk Assessment

Risk assessment is the process of identifying and analyzing relevant risks which, if realized, could prevent R.C. Giltner from achieving its operational compliance objectives. R.C. Giltner assesses and manages risk that could affect the organization's ability to provide services to its clients on an ongoing basis. For any significant risks identified, management is responsible for implementing appropriate measures to remediate or manage these risks.

The executive management team, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on R.C. Giltner's security policies.

Changes in security threats and risks are reviewed by R.C. Giltner management and updates to existing control activities and information security policies are performed as necessary.

R.C. Giltner management maintains a series of tools for the monitoring and management of:

- Infrastructure and support application changes;
- Help desk;
- Systems;
- Vulnerabilities;
- Network protection;
- Email;
- Web;
- Workstation protection; and
- Data protection and datacenter protection.

The aforementioned list comprises the tools for monitoring and management support of R.C. Giltner's communications network, servers, applications, security, and devices utilized in R.C. Giltner's overall operation for providing business process services.

Information and Communication Systems

Information System

R.C. Giltner has security, availability, and confidentiality policies and procedures in place to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training and compliance programs and the use of email to communicate time sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems. Weekly Development meetings are held to review current and future development initiatives.

Communication System

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. R.C. Giltner management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

Monitoring

On-going Monitoring

R.C. Giltner's management performs monitoring activities in order to assess the quality of internal control over time and monitors activities throughout the year and takes corrective actions to address deviations from company policy and procedures. Management utilizes a risk-based approach to monitor business units and other auditable entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance.

R.C. Giltner monitors customer communications through Client Services department. This information is provided to management providing the ability to track, monitor, and assist in understanding customer complaints, concerns, and to evaluate and resolve special requests in a timely fashion. Management's ability to actively monitor customer's communications is an integral role in controlling the quality of the services provided.

Management is proactive in responding to customer complaints and there is a high level of inter-departmental communication about these events. Customer complaints and other issues are handled immediately via personal communication by management staff. Major customer-facing issues are immediately reported to the management for discussion and approval of action.

Sub-service Organization Monitoring

R.C. Giltner reviews the Service Auditor's report on an annual basis to monitor and evaluate the design and operating effectiveness of controls at Microsoft to secure R.C. Giltner's data.

Policies and Practices

INFRASTRUCTURE MANAGEMENT

R.C. Giltner is responsible for maintaining and implementing information technology general computer controls related to computer processing supporting the Online Underwriting Services system. These controls provide the basis for reliance on information / data from the systems used by user entities.

Policies and Procedures

R.C. Giltner has developed and communicated to its users, policies, and procedures to restrict logical access to internal systems. The procedures cover the following key security lifecycle areas:

- Policy management and communication;
- Selection, documentation, and implementation of security controls;
- Authorization, changes to, and termination of information system access;
- Monitoring security controls;
- Management of access and roles;
- Maintenance and support of the security system and necessary backups;
- Incident response; and
- Maintenance of restricted access to system configurations, administrative functionality, passwords, powerful utilities, and security devices.

Physical and Environmental Security

R.C. Giltner hosts its Online Underwriting Services application, PaySound[SM], within Microsoft Windows Azure cloud which offers the physical / logical / and environmental solutions and is SOC 2 Type 2 assessed.

Backups

R.C. Giltner's backup and recovery infrastructure is configured and managed within Microsoft Windows Azure Storage to perform continuous backups of applications, client file storage, R.C. Giltner's SQL servers, and other company and client confidential data. Additionally, employee computers are backed up on a USB backup device attached to their computers on a daily basis and encrypted at rest.

Systems Availability

The PaySound[SM] application is a SaaS delivery model provides a full service solution requiring only a web browser for user access, eliminating the need for internal IT support and hardware costs. Microsoft Azure cloud offers physical and technical solutions and is SOC 2 Type 2 Certified. The PaySound[SM] solution provides its clients with access to the Online Underwriting Services system 24x7x365.

Information Security

Information security policies have been established to set the overall framework for managing security and confidentiality of client information. These policies are approved at the management level and establish standards for information security and confidentiality throughout R.C. Giltner's information resources. The executive leadership has primary responsibility for interpreting these standards, developing procedures and processes for implementing the standards, and overseeing security for R.C. Giltner. In addition, management develops configuration / coding standards for its applications.

Logical Security

R.C. Giltner maintains logical access policies and procedures that define processes for configuration and management of logical access controls to restrict user access to its IT and PaySound[SM] application infrastructure. Policies require that unique user ID is assigned to each individual authorized to access R.C. Giltner local and Microsoft Azure cloud resources, and prompt deactivation of accounts when necessary (i.e., accounts for terminated individuals have to be removed / disabled / revoked from any computing system at the end of the individual's employment or when continued access is no longer required). When establishing accounts, standard security principle of least privilege to perform a function must always be used, where administratively feasible. The identity of users must be authenticated before providing them with account and password details.

Logical access control to R.C. Giltner's IT resources hosted within Microsoft Azure cloud is restricted via an encrypted VPN connection that requires a certificate for authentication. Administrative access to systems and applications is monitored and restricted to authorized users. Logical access to employee computers is controlled via Microsoft Windows security settings. Additionally, employee computers are encrypted using whole disk encryption.

Develop and Manage Applications

One of the primary goals of R.C. Giltner's software development team is to accomplish changes in an efficient manner while minimizing the business impact, costs, and risks. Development is performed using Microsoft Visual Studio product. Software changes are documented and monitored using Microsoft Visual Studio Online product. Additionally, the PaySound[SM] source code and version control is maintained via version control software implemented using Microsoft Visual Studio Online to manage offsite versioning repository over Hypertext Transfer Protocol Secure (HTTPS). Access to source code repository is restricted to authorized personnel only. Releases are tested internally and are reviewed and approved by authorized personnel prior to migration to the production environment.

PRINCIPLES, CRITERIA, AND RELATED CONTROLS

The principles, criteria, and related controls are included in Section 4 of this report, “Principles, Criteria, Related Controls and Tests of Operating Effectiveness”, to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the principles and related controls are included in Section 4, they are, nevertheless, an integral part of the organization’s description of controls.

COMPLEMENTARY CONTROL CONSIDERATIONS

R.C. Giltner's policies and procedures over its Online Underwriting Services system cover only a portion of the overall internal control for each user entity. It is not feasible for the principles related to the Online Underwriting Services system to be solely achieved by R.C. Giltner. R.C. Giltner's control policies and procedures were designed with the assumption that certain controls would be in place and in operation at sub-service organizations and user entities. Sub-service organization controls and user entity internal controls must be evaluated, taking into consideration R.C. Giltner controls and their own internal controls. R.C. Giltner does not make any representations regarding responsibility related to, or provide any assurance in regards to any such internal control or regulatory requirements for which the client must assess or comply.

This section describes some of the control considerations for sub-service organizations and user entities, or "complementary controls", which should be in operation at the sub-service organizations and user entities to complement the controls at the service organization. User auditors / user entities should determine whether sub-service organizations and user entities have established controls to ensure that the criteria within this report are met. The "complementary controls" presented below should not be regarded as a comprehensive list of all controls that should be employed by sub-service organizations or user entities.

Control Considerations for User Entities

1. User entities are responsible for informing R.C. Giltner of any regulatory issues that may affect the services provided by R.C. Giltner to the user entity.
2. User entities are responsible for understanding and complying with their contractual obligations to R.C. Giltner.
3. User entities are responsible for notifying R.C. Giltner, in a timely manner, when changes are made to technical, billing, or administrative contact information.
4. User entities are responsible for developing their own disaster recovery and business continuity plans that address their inability to access or utilize R.C. Giltner's services.
5. User entities are responsible for defining the communications method utilized to connect to R.C. Giltner's systems (e.g. direct connections, over public networks, etc.).
6. User entities are responsible for implementing security infrastructure and practices to prevent unauthorized access to their internal network and to limit threats from connections to external networks.
7. User entities are responsible for reviewing their access lists on a regular basis and notifying R.C. Giltner of any changes.
8. User entities are responsible for authorizing all user account requests.
9. User entities are responsible for ensuring the deactivation or removal of system user accounts.
10. User entities are responsible for ensuring that user IDs and passwords are assigned only to authorized individuals and that the roles assigned to the user accounts are appropriate.
11. User entities are responsible for ensuring the confidentiality of any user IDs and passwords assigned to them for use with R.C. Giltner's systems.
12. User entities are responsible for ensuring that access to administrative accounts is appropriately restricted to authorized personnel.
13. User entities are responsible for the administration of password security parameters and settings on their system to ensure they are in accordance with internal policies.
14. User entities are responsible for the administration of user accounts used by R.C. Giltner to connect to user entity systems.
15. User entities are responsible for immediately notifying R.C. Giltner of any actual or suspected information security breaches or fraud, including compromised user accounts.

16. User entities are responsible for determining whether R.C. Giltner's security infrastructure is appropriate for its needs and for notifying R.C. Giltner of any requested modifications.
17. User entities are responsible for developing policies and procedures to protect their systems from unauthorized or unintentional user, modification, addition, or deletion.
18. User entities are responsible for monitoring and reviewing reports and notifications provided by R.C. Giltner personnel, and are responsible for taking any necessary actions.
19. User entities are responsible for maintaining an administrator contact with R.C. Giltner who is authorized to transact with R.C. Giltner on behalf of the user entity in a timely manner.
20. User entities are responsible for ensuring the application releases / changes are functioning appropriated and providing R.C. Giltner authorization, in a timely manner, to migrate changes to their production environments.
21. User entities are responsible for administering user accounts to their installation of the PaySound[SM] application.

Control Considerations for Sub-Service Organizations

1. Sub-service organizations are responsible for implementing physical security controls to provide reasonable assurance that business premises and information systems are protected from unauthorized access, damage and interference.
2. Sub-service organizations are responsible for implementing environmental security controls to provide reasonable assurance that relevant information technology infrastructure is protected from certain environmental threats.

SECTION 4:

PRINCIPLES, CRITERIA, CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS

INFORMATION PROVIDED BY THE SERVICE AUDITOR

Introduction

This report is intended to provide user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding with information about controls that may affect the Online Underwriting Services system provided by R.C. Giltner and to provide information about the operating effectiveness of controls that were tested.

The scope of our testing of R.C. Giltner's controls was limited to the principles, criteria, and the related controls specified by R.C. Giltner and contained within Section 4 of this report, which management believes to be the relevant key controls for the principles and criteria included in the scope of this report. Our review was not extended to controls in place at any user entities, sub-service organizations, or any other third-party vendors.

The examination was performed in accordance with the American Institute of Certified Public Accountants ("AICPA") Standards for Attestation Engagements No. 18 '*Attestation Standards: Clarification and Recodification*', specifically AT-C Section 205, '*Examination Engagements'.* It is each interested party's responsibility to evaluate this information in relation to controls in place at user entities and sub-service organizations (if applicable) to obtain an overall understanding of internal control and to assess control risk. Controls in place at user entities, sub-service organizations (if applicable), and R.C. Giltner's controls must be evaluated together. A general, but not inclusive, listing of control considerations is provided in Section 3, "Complementary Control Considerations." If an effectively operating user entity or sub-service organization (if applicable) internal control is not in place, the controls at R.C. Giltner may not sufficiently compensate the deficiency.

Tests of Operating Effectiveness

Our tests of the operating effectiveness of the controls specified by R.C. Giltner included such tests as we considered necessary in the circumstances to obtain reasonable, but not absolute, assurance that the controls operated in a manner that achieved the specified principle during the period from September 1, 2016 to August 31, 2017. In selecting particular tests of the operating effectiveness of controls we considered 1) the nature of the controls being tested; 2) the types and completeness of available evidential matter; 3) the nature of the principle to be achieved; 4) the assessed level of control risk; 5) the expected efficiency and effectiveness of the test; and, 6) the testing of other controls relevant to the principle.

Testing exceptions, if any, and information about specific tests of the operating effectiveness performed that may be relevant to the interpretation of testing results by user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding for the controls specified to achieve the principle are presented in this section under the column heading "Results of Testing". Exceptions identified herein are not necessarily considered significant deficiencies or material weaknesses in the total system of internal controls of R.C. Giltner, as this determination can only be made after consideration of controls in place at user entities. Control considerations that should be exercised by R.C. Giltner's clients in order to complement the controls of R.C. Giltner to attain the principles are presented in relation to the nature of services being audited and the controls specified by R.C. Giltner.

Types of Tests Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of appropriate personnel seeking relevant information or representation to obtain the following information about the control: ➢ Knowledge and additional information regarding the policy or procedure; and ➢ Corroborating evidence of the policy or procedure.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: ➢ Examination / Inspection of source documentation and authorizations to verify transactions processed; ➢ Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures; ➢ Examination / Inspection of systems documentation, configurations and settings; and ➢ Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.
Observation	Observed the implementation, application or existence of specific controls as represented
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed

Sampling Methodology

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	At least 40
Manual control, daily (Note 1)	At least 25	At least 40
Manual control, weekly	At least 5	At least 10
Manual control, monthly	At least 3	At least 4
Manual control, quarterly	At least 2	At least 2
Manual control, annually	Test annually	Test annually
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	Follow guidance above for manual and automated aspects of IT general controls

Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.

PRINCIPLES, CRITERIA, AND RELATED CONTROLS

Security Principle and Criteria (Common Criteria to All Principles)

The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.0 Organization and Management: The criteria relevant to how the organization is structured and the processes the entity has implemented to manage and support people within its operating units to meet the criteria for the principle(s) addressed by the engagement. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.			
CC1.1 The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, maintenance operation, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.			
CC1.1.1	A Security Steering Committee is in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	Inquired of the CIO to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
		Inspected the Security Steering Committee Agendas and Meeting Minutes from meetings held during the examination period to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
CC1.1.2	The Security Steering Committee meets semi-annually with the Board of Directors to discuss security issues and enhancements to security policies and procedures.	Inquired of the CIO to verify that Security Steering Committee met semi-annually with the Board of Directors and discussed security issues and enhancements to security policies and procedures.	No relevant exceptions noted.
		Inspected the Board Agendas and Meeting Minutes for the Board of Directors Meetings held during the examination period to verify that the Security Steering Committee met semi-annually with the Board of Directors and discussed security issues and enhancements to security policies and procedures.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.1.3	Written job descriptions detailing responsibilities for system security and meeting customer SLA standards are defined by HR and communicated to applicable personnel and RCG management.	Inquired of the CIO to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
		Inspected organizational job descriptions to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
CC1.2 Responsibility and accountability for designing, developing, implementing, operating, maintaining monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
CC1.2.1	A Security Steering Committee is in place to address security issues, security policy enhancements, security awareness training, and security planning for the company	Inquired of the CIO to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
		Inspected the Security Steering Committee Agendas and Meeting Minutes from meetings held during the examination period to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
CC1.2.2	The Security Steering Committee meets semi-annually with the Board of Directors to discuss security issues and enhancements to security policies and procedures.	Inquired of the CIO to verify that Security Steering Committee met semi-annually with the Board of Directors and discussed security issues and enhancements to security policies and procedures.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Board Agendas and Meeting Minutes for the Board of Directors Meetings held during the examination period to verify that the Security Steering Committee met semi-annually with the Board of Directors and discussed security issues and enhancements to security policies and procedures.	No relevant exceptions noted.
CC1.3 The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security, availability, and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.			
CC1.3.1	A Security Steering Committee is in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	Inquired of the CIO to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
		Inspected the Security Steering Committee Agendas and Meeting Minutes from meetings held during the examination period to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
CC1.3.2	The Security Steering Committee meets semi-annually with the Board of Directors to discuss security issues and enhancements to security policies and procedures.	Inquired of the CIO to verify that Security Steering Committee met semi-annually with the Board of Directors and discussed security issues and enhancements to security policies and procedures.	No relevant exceptions noted.
		Inspected the Board Agendas and Meeting Minutes for the Board of Directors Meetings held during the examination period to verify that the Security Steering Committee met semi-annually with the Board of Directors and discussed security issues and enhancements to security policies and procedures.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.3.3	Written job descriptions detailing responsibilities for system security and meeting customer SLA standards are defined by HR and communicated to applicable personnel and RCG management.	Inquired of the CIO to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
		Inspected organizational job descriptions to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
CC1.3.4	Annual reviews are completed for employees of RCG.	Inquired of the CIO to verify that annual reviews were required to be completed for employees of RCG.	No relevant exceptions noted.
		Inspected Performance Appraisals for a sample of employees to verify that annual reviews were completed for employees of RCG within the past 12 months.	No relevant exceptions noted.
CC1.4 The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.			
CC1.4.1	A Security Steering Committee is in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	Inquired of the CIO to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
		Inspected the Security Steering Committee Agendas and Meeting Minutes from meetings held during the examination period to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.4.2	The Security Steering Committee meets semi-annually with the Board of Directors to discuss security issues and enhancements to security policies and procedures.	Inquired of the CIO to verify that Security Steering Committee met semi-annually with the Board of Directors and discussed security issues and enhancements to security policies and procedures.	No relevant exceptions noted.
		Inspected the Board Agendas and Meeting Minutes for the Board of Directors Meetings held during the examination period to verify that the Security Steering Committee met semi-annually with the Board of Directors and discussed security issues and enhancements to security policies and procedures.	No relevant exceptions noted.
CC1.4.3	Written job descriptions detailing responsibilities for system security and meeting customer SLA standards are defined by HR and communicated to applicable personnel and RCG management.	Inquired of the CIO to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
		Inspected organizational job descriptions to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
CC1.4.4	Annual reviews are completed for employees of RCG.	Inquired of the CIO to verify that annual reviews were required to be completed for employees of RCG.	No relevant exceptions noted.
		Inspected Performance Appraisals for a sample of employees to verify that annual reviews were completed for employees of RCG within the past 12 months.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.0 Communications: The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and uses to the effective operation of the system.			
CC2.1 Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users to permit users to understand their role in the system and the results of system operation.			
CC2.1.1	RCG maintains infrastructure documentation that describes the system and its boundaries. Infrastructure documentation is published on the Business Dropbox that is available to employees and contractors.	Inquired of the CIO to verify that RCG maintained infrastructure documentation that described the system and its boundaries. Infrastructure documentation was published on the Business Dropbox that was available to employees and contractors.	No relevant exceptions noted.
		Inspected the Infrastructure document and the RCG Drop Box to verify that RCG maintained infrastructure documentation that described the system and its boundaries. Infrastructure documentation was published on the Business Dropbox that was available to employees and contractors.	No relevant exceptions noted.
CC2.1.2	A Digital Lending Technology and Deposit Services Agreement is executed between the client and RCG prior to receipt of services.	Inquired of the CIO to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
		Inspected the executed Digital Lending Technology and Deposit Services Agreement for the population of clients on-boarded during the examination period to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.2 The entity's security, availability, and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.			
CC2.2.1	A security awareness program is in place to communicate RCG security policies to employees and contractors.	Inquired of the CIO to verify that a security awareness program was in place to communicate RCG security policies to employees and contractors.	No relevant exceptions noted.
		Inspected the Security Awareness Guide to verify that a security awareness program was in place to communicate RCG security policies to employees and contractors.	No relevant exceptions noted.
CC2.2.2	New employees and contractors are required to sign a statement signifying that they have read, understand, and will follow policies for security, availability, and confidentiality. Each year employees and contractors are required to reaffirm their understanding and compliance to the RCG security policies.	Inquired of the CIO to verify that new employees and contractors were required to sign a statement signifying that they had read, understand, and will follow policies for security, availability, and confidentiality. Each year employees and contractors were required to reaffirm their understanding and compliance to the RCG security policies.	No relevant exceptions noted.
		Inspected the signed Statement of Understanding and Agreement for current employees to verify that employees and contractors were required to sign a statement signifying that they had read, understand, and will follow policies for security, availability, and confidentiality within the past 12 months.	No relevant exceptions noted.
CC2.2.3	The Associate Handbook and Agreement for Employees and Contractors includes a statement signifying that the employee / contractor has read, understands, and will follow these policies. This agreement is required to be signed during the new employee orientation.	Inquired of the CIO to verify that Associate Handbook and Agreement for Employees and Contractors included a statement signifying that the employee / contractor will read, understood, and will follow these policies. This agreement was required to be signed during the new employee orientation.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.2.4	RCG maintains an Information Classification Policy that classifies information entrusted to RCG from a third-party to its level of confidentiality and protection.	Inquired of the CIO to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
		Inspected the Information Classification Policy to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
CC2.2.5	A Digital Lending Technology and Deposit Services Agreement is executed between the client and RCG prior to receipt of services.	Inquired of the CIO to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
		Inspected the executed Digital Lending Technology and Deposit Services Agreement for the population of clients on-boarded during the examination period to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
CC2.2.6	RCG publishes its policies on the Business Dropbox that is available to employees and contractors.	Inquired of the CIO to verify that RCG published its policies on the Business Dropbox that was available to employees and contractors.	No relevant exceptions noted.
		Inspected the RCG Dropbox to verify that RCG published its policies on the Business Dropbox that was available to employees and contractors.	No relevant exceptions noted.
CC2.3 The responsibility of internal and external users and other whose roles affect system operation are communicated to those parties.			
CC2.3.1	A security awareness program is in place to communicate RCG security policies to employees and contractors.	Inquired of the CIO to verify that a security awareness program was in place to communicate RCG security policies to employees and contractors.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Security Awareness Guide to verify that a security awareness program was in place to communicate RCG security policies to employees and contractors.	No relevant exceptions noted.
CC2.3.2	New employees and contractors are required to sign a statement signifying that they have read, understand, and will follow policies for security, availability, and confidentiality. Each year employees and contractors are required to reaffirm their understanding and compliance to the RCG security policies.	Inquired of the CIO to verify that new employees and contractors were required to sign a statement signifying that they had read, understand, and will follow policies for security, availability, and confidentiality. Each year employees and contractors were required to reaffirm their understanding and compliance to the RCG security policies.	No relevant exceptions noted.
		Inspected the signed Statement of Understanding and Agreement for current employees to verify that employees and contractors were required to sign a statement signifying that they had read, understand, and will follow policies for security, availability, and confidentiality within the past 12 months.	No relevant exceptions noted.
CC2.3.3	The Associate Handbook and Agreement for Employees and Contractors includes a statement signifying that the employee / contractor has read, understands, and will follow these policies. This agreement is required to be signed during the new employee orientation.	Inquired of the CIO to verify that Associate Handbook and Agreement for Employees and Contractors included a statement signifying that the employee / contractor will read, understood, and will follow these policies. This agreement was required to be signed during the new employee orientation.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A
CC2.3.4	RCG maintains an Information Classification Policy that classifies information entrusted to RCG from a third-party to its level of confidentiality and protection.	Inquired of the CIO to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Information Classification Policy to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
CC2.3.5	A Digital Lending Technology and Deposit Services Agreement is executed between the client and RCG prior to receipt of services.	Inquired of the CIO to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
		Inspected the executed Digital Lending Technology and Deposit Services Agreement for the population of clients on-boarded during the examination period to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
CC2.3.6	RCG publishes its policies on the Business Dropbox that is available to employees and contractors.	Inquired of the CIO to verify that RCG published its policies on the Business Dropbox that was available to employees and contractors.	No relevant exceptions noted.
		Inspected the RCG Dropbox to verify that RCG published its policies on the Business Dropbox that was available to employees and contractors.	No relevant exceptions noted.
CC2.3.7	A Security Steering Committee is in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	Inquired of the CIO to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
		Inspected the Security Steering Committee Agendas and Meeting Minutes from meetings held during the examination period to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.3.8	Written job descriptions detailing responsibilities for system security and meeting customer SLA standards are defined by HR and communicated to applicable personnel and RCG management.	Inquired of the CIO to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
		Inspected organizational job descriptions to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
CC2.4 Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, and confidentiality of the system, is provided to personnel to carry out their responsibilities.			
CC2.4.1	A security awareness program is in place to communicate RCG security policies to employees and contractors.	Inquired of the CIO to verify that a security awareness program was in place to communicate RCG security policies to employees and contractors.	No relevant exceptions noted.
		Inspected the Security Awareness Guide to verify that a security awareness program was in place to communicate RCG security policies to employees and contractors.	No relevant exceptions noted.
CC2.4.2	New employees and contractors are required to sign a statement signifying that they have read, understand, and will follow policies for security, availability, and confidentiality. Each year employees and contractors are required to reaffirm their understanding and compliance to the RCG security policies.	Inquired of the CIO to verify that new employees and contractors were required to sign a statement signifying that they had read, understand, and will follow policies for security, availability, and confidentiality. Each year employees and contractors were required to reaffirm their understanding and compliance to the RCG security policies.	No relevant exceptions noted.
		Inspected the signed Statement of Understanding and Agreement for current employees to verify that employees and contractors were required to sign a statement signifying that they had read, understand, and will follow policies for security, availability, and confidentiality within the past 12 months.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.4.3	The Associate Handbook and Agreement for Employees and Contractors includes a statement signifying that the employee / contractor has read, understands, and will follow these policies. This agreement is required to be signed during the new employee orientation.	Inquired of the CIO to verify that Associate Handbook and Agreement for Employees and Contractors included a statement signifying that the employee / contractor will read, understood, and will follow these policies. This agreement was required to be signed during the new employee orientation.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A
CC2.4.4	RCG maintains an Information Classification Policy that classifies information entrusted to RCG from a third-party to its level of confidentiality and protection.	Inquired of the CIO to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
		Inspected the Information Classification Policy to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
CC2.4.5	A Digital Lending Technology and Deposit Services Agreement is executed between the client and RCG prior to receipt of services.	Inquired of the CIO to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
		Inspected the executed Digital Lending Technology and Deposit Services Agreement for the population of clients on-boarded during the examination period to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
CC2.4.6	RCG publishes its policies on the Business Dropbox that is available to employees and contractors.	Inquired of the CIO to verify that RCG published its policies on the Business Dropbox that was available to employees and contractors.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the RCG Dropbox to verify that RCG published its policies on the Business Dropbox that was available to employees and contractors.	No relevant exceptions noted.
CC2.4.7	A Security Steering Committee is in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	Inquired of the CIO to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
		Inspected the Security Steering Committee Agendas and Meeting Minutes from meetings held during the examination period to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
CC2.4.8	Written job descriptions detailing responsibilities for system security and meeting customer SLA standards are defined by HR and communicated to applicable personnel and RCG management.	Inquired of the CIO to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
		Inspected organizational job descriptions to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
CC2.5 Internal and external users have been provided with information on how to report security, availability, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.			
CC2.5.1	RCG Incident Response Plan includes information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	Inquired of the CIO to verify that RCG Incident Response Plan included information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Incident Response Plan to verify that it included information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	No relevant exceptions noted.
CC2.5.2	The process for clients to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents is outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy.	Inquired of the CIO to verify that the process for client to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents was outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy.	No relevant exceptions noted.
		Inspected the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy to verify that the process for client to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents was outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy	No relevant exceptions noted.
CC2.5.3	Written job descriptions detailing responsibilities for system security and meeting customer SLA standards are defined by HR and communicated to applicable personnel and RCG management.	Inquired of the CIO to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
		Inspected organizational job descriptions to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.6 System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security, availability, and confidentiality are communicated to those users in a timely manner.			
CC2.6.1	Planned changes to production systems and the scheduling of those changes are reviewed by management prior to implementation. Management alerts clients of potential downtime that may affect client deliveries.	Inquired of the CIO to verify that planned changes to production systems and the scheduling of those changes were reviewed by management prior to implementation. Management alerted clients of potential downtime that may affect client deliveries.	No relevant exceptions noted.
		Inspected the Release Notes for a sample of changes implemented during the examination period to verify that planned changes to production systems and the scheduling of those changes were reviewed by management prior to implementation and management alerted clients of potential downtime that may affect client deliveries.	No relevant exceptions noted.
CC2.6.2	Changes that affect system security, availability, and confidentiality are incorporated into the RCG annual security awareness program.	Inquired of the CIO to verify that changes that affected system security, availability, and confidentiality were incorporated into the RCG annual security awareness program.	No relevant exceptions noted.
		Inspected the Security Awareness Guide to verify that changes that affected system security, availability, and confidentiality were incorporated into the RCG annual security awareness program.	No relevant exceptions noted.
CC2.6.3	Changes that may affect clients and their security, availability, and confidentiality obligations or RCG security commitments are communicated to clients via email and / or phone by the VP of Client Services or the CIO.	Inquired of the CIO to verify that changes that may affect clients and their security, availability, and confidentiality obligations or RCG security commitments were communicated to clients via email and / or phone by the VP of Client Services or the CIO.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Release Notes for a sample of changes implemented during the examination period to verify that changes that may affect clients and their security, availability, and confidentiality obligations or RCG security commitments were communicated to clients via email and / or phone by the VP of Client Services or the CIO.	No relevant exceptions noted.
CC3.0 Risk Management and Design and Implementation of Controls: The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.			
CC3.1 The entity (1) identifies potential threats that could impair system security, availability, and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and other with access to the system), (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods and services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.			
CC3.1.1	RCG performs a threat assessment at least annually to identify potential threats to its environment. Threats are reviewed and updated within the Business Continuity Plan.	Inquired of the CIO to verify that RCG performed a threat assessment at least annually to identify potential threats to its environment. Threats were reviewed and updated within the Business Continuity Plan.	No relevant exceptions noted.
		Inspected the Business Continuity Plan to verify that RCG performed a threat assessment at least annually to identify potential threats to its environment. Threats were reviewed and updated within the Business Continuity Plan.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC3.1.2	RCG performs vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments.	Inquired of the CIO to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments	No relevant exceptions noted.
		Inspected the vendor risk evaluations for current vendors and due diligence evaluations for “high risk” vendors to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors within the past 12 months.	No relevant exceptions noted.
CC3.1.3	Key performance metrics are monitored using the Microsoft Azure Endpoint Monitor that is configured to monitor and log the uptime and the response time of the PaySound[SM] website.	Inquired of the CIO to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
		Inspected the Microsoft Azure Endpoint Monitor to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
CC3.1.4	RCG maintains an Information Classification Policy that classifies information entrusted to RCG from a third-party to its level of confidentiality and protection.	Inquired of the CIO to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
		Inspected the Information Classification Policy to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC3.1.5	RCG utilizes consultants who are formally engaged and on retainer to get updates and consultation regarding regulatory changes and contracts that affect the PaySound[SM] application.	Inquired of the CIO to verify that RCG utilized consultants who were formally engaged and on retainer to get updates and consultation regarding regulatory changes and contracts that affect the PaySound[SM] application	No relevant exceptions noted.
		Inspected an example risk management consultant's invoice from the examination period to verify that RCG utilized consultants who were formally engaged and on retainer to get updates and consultation regarding regulatory changes and contracts that affect the PaySound[SM] application	No relevant exceptions noted.
CC3.1.6	RCG retains legal counsel to consult with regarding any regulatory or industry related topics.	Inquired of the CIO to verify that RCG retained legal counsel to consult with regarding any regulatory or industry related topics.	No relevant exceptions noted.
		Inspected a recent invoice to verify that RCG retained legal counsel to consult with regarding any regulatory or industry related topics.	No relevant exceptions noted.
CC3.2 The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy, reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, and updates the controls, as necessary.			
CC3.2.1	RCG maintains written security policies that address security, availability, and confidentiality. The policies are reviewed at least annually and changes are discussed with the Security Steering Committee and Board of Directors.	Inquired of the CIO to verify that RCG maintained written security policies that addressed security, availability, and confidentiality. The policies were reviewed at least annually and changes were discussed with the Security Steering Committee and Board of Directors.	No relevant exceptions noted.
		Inspected the Security Awareness Guide to verify that RCG maintained written security policies that addressed security, availability, and confidentiality and were approved within the past 12 months.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC3.2.2	Proposed changes to the Security Awareness Guide are to be accepted by the Board of Directors at the Security Steering Committee and Board of Directors semi-annual meetings.	Inquired of the CIO to verify that proposed changes to the Security Awareness Guide had to be accepted by the Board of Directors at the Security Steering Committee and Board of Directors semi-annual meetings.	No relevant exceptions noted.
		Inspected the Meeting Minutes from the Steering Committee meetings and the Board meetings held during the examination period to verify that proposed changes to the Security Awareness Guide had to be accepted by the Board of Directors at the Security Steering Committee and Board of Directors semi-annual meetings.	No relevant exceptions noted.
CC3.2.3	New employees and contractors are required to sign a statement signifying that they have read, understand, and will follow policies for security, availability, and confidentiality. Each year employees and contractors are required to reaffirm their understanding and compliance to the RCG security policies.	Inquired of the CIO to verify that new employees and contractors were required to sign a statement signifying that they had read, understand, and will follow policies for security, availability, and confidentiality. Each year employees and contractors were required to reaffirm their understanding and compliance to the RCG security policies.	No relevant exceptions noted.
		Inspected the signed Statement of Understanding and Agreement for current employees to verify that employees and contractors were required to sign a statement signifying that they had read, understand, and will follow policies for security, availability, and confidentiality within the past 12 months.	No relevant exceptions noted.
CC3.2.4	A Digital Lending Technology and Deposit Services Agreement is executed between the client and RCG prior to receipt of services.	Inquired of the CIO to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the executed Digital Lending Technology and Deposit Services Agreement for the population of clients on-boarded during the examination period to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
CC3.2.5	Policies and standard operating procedures that address security, availability, and confidentiality are in place to guide personnel.	Inquired of the CIO to verify that policies and standard operating procedures that addressed security, availability, and confidentiality were in place to guide personnel.	No relevant exceptions noted.
		Inspected policies and standard operating procedures that address security, availability, and confidentiality to verify that policies and standard operating procedures that addressed security, availability, and confidentiality were in place to guide personnel.	No relevant exceptions noted.
CC3.2.6	A Security Steering Committee is in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	Inquired of the CIO to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
		Inspected the Security Steering Committee Agendas and Meeting Minutes from meetings held during the examination period to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
CC3.2.7	Written job descriptions detailing responsibilities for system security and meeting customer SLA standards are defined by HR and communicated to applicable personnel and RCG management.	Inquired of the CIO to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected organizational job descriptions to verify that written job descriptions detailing responsibilities for system security and meeting customer SLA standards were defined by HR and communicated to applicable personnel and RCG management.	No relevant exceptions noted.
CC4.0 Monitoring Controls: The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.			
CC4.1 The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security, availability, and confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.			
CC4.1.1	RCG performs a threat assessment at least annually to identify potential threats to its environment. Threats are reviewed and updated within the Business Continuity Plan.	Inquired of the CIO to verify that RCG performed a threat assessment at least annually to identify potential threats to its environment. Threats were reviewed and updated within the Business Continuity Plan.	No relevant exceptions noted.
		Inspected the Business Continuity Plan to verify that RCG performed a threat assessment at least annually to identify potential threats to its environment. Threats were reviewed and updated within the Business Continuity Plan.	No relevant exceptions noted.
CC4.1.2	RCG performs vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments.	Inquired of the CIO to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the vendor risk evaluations for current vendors and due diligence evaluations for "high risk" vendors to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors within the past 12 months.	No relevant exceptions noted.
CC4.1.3	Key performance metrics are monitored using the Microsoft Azure Endpoint Monitor that is configured to monitor and log the uptime and the response time of the PaySound[SM] website.	Inquired of the CIO to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
		Inspected the Microsoft Azure Endpoint Monitor to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
CC4.1.4	RCG Incident Response Plan includes information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	Inquired of the CIO to verify that RCG Incident Response Plan included information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	No relevant exceptions noted.
		Inspected the Incident Response Plan to verify that it included information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	No relevant exceptions noted.
CC4.1.5	RCG performs a threat assessment at least annually to identify potential threats to its environment. Threats are reviewed and updated within the Business Continuity Plan.	Inquired of the CIO to verify that RCG performed a threat assessment at least annually to identify potential threats to its environment. Threats were reviewed and updated within the Business Continuity Plan.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Business Continuity Plan to verify that RCG performed a threat assessment at least annually to identify potential threats to its environment. Threats were reviewed and updated within the Business Continuity Plan.	No relevant exceptions noted.
CC4.1.6	Microsoft Windows Azure Endpoint Monitor is configured to generate alert notifications when network performance exceeds predefined thresholds. Alert notifications are sent to the Director of Technology.	Inquired of the CIO to verify that Microsoft Windows Azure Endpoint Monitor was configured to generate alert notifications when network performance exceeds predefined thresholds. Alert notifications were sent to the Director of Technology.	No relevant exceptions noted.
		Inspected the Microsoft Windows Azure Endpoint dashboard and an example alert notification sent during the examination period to verify that Endpoint was configured to generate alert notifications when network performance exceeds predefined thresholds. Alert notifications were sent to the Director of Technology.	No relevant exceptions noted.
CC4.1.7	Computers used by RCG employees and contractors run anti-virus software to protect against viruses, malware, and malicious code.	Inquired of the CIO to verify that computers used by RCG employees and contractors ran anti-virus software to protect against viruses, malware, and malicious code.	No relevant exceptions noted.
		Inspected anti-virus configurations to verify that computers used by RCG employees and contractors ran anti-virus software to protect against viruses, malware, and malicious code.	No relevant exceptions noted.
CC4.1.8	RCG managed VMs hosted with Microsoft Windows Azure have antivirus software installed to protect against viruses, malware, and malicious code.	Inquired of the CIO to verify that RCG managed VMs hosted with Microsoft Windows Azure had antivirus software installed to protect against viruses, malware, and malicious code.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Endpoint anti-virus configurations to verify that RCG managed VMs hosted with Microsoft Windows Azure had antivirus software installed to protect against viruses, malware, and malicious code.	No relevant exceptions noted.
CC5.0 Logical and Physical Access Controls: The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principle(s) addressed in the engagement.			
CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
CC5.1.1	Computers used by RCG employees and contractors are configured to restrict access to the operating system via unique user ID and password.	Inquired of the CIO to verify that computers used by RCG employees and contractors were configured to restrict access to the operating system via unique user ID and password.	No relevant exceptions noted.
		Inspected the password configurations to verify that computers used by RCG employees and contractors were configured to restrict access to the operating system via unique user ID and password.	No relevant exceptions noted.
CC5.1.2	Computers used by RCG employees and contractors are configured to meet a minimum of the following password requirements: ➢ Password history = three passwords remembered ➢ Minimum password length = eight characters ➢ Maximum password age = 60 days	Inquired of the CIO to verify that computers used by RCG employees and contractors were configured to meet a minimum of the following password requirements: ➢ Password history = three passwords remembered ➢ Minimum password length = eight characters ➢ Maximum password age = 60 days	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the password configurations for employees and contractors to verify that computers used by RCG employees and contractors were configured to meet a minimum of the following password requirements: ➢ Password history = three passwords remembered ➢ Minimum password length = eight characters ➢ Maximum password age = 60 days	No relevant exceptions noted.
CC5.1.3	Access to the Azure environment is restricted via unique user ID and password.	Inquired of the CIO to verify that access to the Azure environment was restricted via unique user ID and password.	No relevant exceptions noted.
		Inspected the Azure User List to verify that access to the Azure environment was restricted via unique user ID and password.	No relevant exceptions noted.
CC5.1.4	Administrative access to Microsoft Azure Portal is restricted to the following personnel: ➢ CIO ➢ Director of Technology	Inquired of the CIO to verify that administrative access to Microsoft Azure Portal was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
		Inspected the Azure Administrators listing to verify that administrative access to Microsoft Azure Portal was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
CC5.1.5	Remote access to the Azure environment is granted through an encrypted VPN connection that requires a certificate for authentication.	Inquired of the CIO to verify that remote access to the Azure environment was granted through an encrypted VPN connection that requires a certificate for authentication.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the VPN configuration to verify that remote access to the Azure environment was granted through an encrypted VPN connection that requires a certificate for authentication.	No relevant exceptions noted.
CC5.1.6	Access to the PaySound[SM] application is restricted via application account settings requiring a unique user ID and password.	Inquired of the CIO to verify that access to the PaySound[SM] application was restricted via application account settings requiring a unique user ID and password.	No relevant exceptions noted.
		Inspected the PaySound[SM] application to verify that access was restricted via application account settings requiring a unique user ID and password.	No relevant exceptions noted.
CC5.1.7	Full administrative access to the application is restricted to the following employees: ➢ COB ➢ CEO ➢ CIO ➢ VP Client Services ➢ Director of Technology ➢ Director of Administration ➢ Engagement Manager	Inquired of the CIO to verify that full administrative access to the application was restricted to the following employees: ➢ COB ➢ CEO ➢ CIO ➢ VP Client Services ➢ Director of Technology ➢ Director of Administration ➢ Engagement Manager	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Global Admins listing for the application to verify that full administrative access to the application was restricted to the following employees: ➢ COB ➢ CEO ➢ CIO ➢ VP Client Services ➢ Director of Technology ➢ Director of Administration ➢ Engagement Manager	No relevant exceptions noted.
CC5.1.9	Administrative access to the production database is restricted to the following personnel: ➢ CIO ➢ Director of Technology	Inquired of the CIO to verify that administrative access to the production database was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
		Inspected the database administrative access permissions to verify that administrative access to the production database was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
CC5.1.10	Internal IT access requests are administered using a new employee on-boarding checklist and are required to be approved by the Director of Technology prior to granting access to systems.	Inquired of the CIO to verify that internal IT access requests were administered using a new employee on-boarding checklist and were required to be approved by the Director of Technology prior to granting access to systems.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.1.11	System accounts assigned to terminated employees are deactivated upon notification of termination.	Inquired of the CIO to verify that system accounts assigned to terminated employees were deactivated upon notification of termination.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A
CC5.1.12	Termination of client access is approved by the Project Manager, COB, or CEO prior to removing access to client environment.	Inquired of the CIO to verify that termination of client access was approved by the Project Manager, COB, or CEO prior to removing access to client environment.	No relevant exceptions noted.
		Inspected the Termination Procedures and Termination Notifications for the population of clients terminated during the examination period to verify that termination of client access was approved by the Project Manager, COB, or CEO prior to removing access to client environment.	No relevant exceptions noted.
CC5.2 New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC5.2.1	Internal IT access requests are administered using a new employee on-boarding checklist and are required to be approved by the Director of Technology prior to granting access to systems.	Inquired of the CIO to verify that internal IT access requests were administered using a new employee on-boarding checklist and were required to be approved by the Director of Technology prior to granting access to systems.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A
CC5.2.2	System accounts assigned to terminated employees are deactivated upon notification of termination.	Inquired of the CIO to verify that system accounts assigned to terminated employees were deactivated upon notification of termination.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A
CC5.2.3	Termination of client access is approved by the Project Manager, COB, or CEO prior to removing access to client environment.	Inquired of the CIO to verify that termination of client access was approved by the Project Manager, COB, or CEO prior to removing access to client environment.	No relevant exceptions noted.
		Inspected the Termination Procedures and Termination Notifications for the population of clients terminated during the examination period to verify that termination of client access was approved by the Project Manager, COB, or CEO prior to removing access to client environment.	No relevant exceptions noted.
CC5.3 Internal and external users are identified and authenticated when accessing the system components (that is, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
CC5.3.1	Computers used by RCG employees and contractors are configured to restrict access to the operating system via unique user ID and password.	Inquired of the CIO to verify that computers used by RCG employees and contractors were configured to restrict access to the operating system via unique user ID and password.	No relevant exceptions noted.
		Inspected the password configurations to verify that computers used by RCG employees and contractors were configured to restrict access to the operating system via unique user ID and password.	No relevant exceptions noted.
CC5.3.2	Computers used by RCG employees and contractors are configured to meet a minimum of the following password requirements: ➢ Password history = three passwords remembered ➢ Minimum password length = eight characters ➢ Maximum password age = 60 days	Inquired of the CIO to verify that computers used by RCG employees and contractors were configured to meet a minimum of the following password requirements: ➢ Password history = three passwords remembered ➢ Minimum password length = eight characters ➢ Maximum password age = 60 days	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the password configurations to verify that computers used by RCG employees and contractors were configured to meet a minimum of the following password requirements: ➢ Password history = three passwords remembered ➢ Minimum password length = eight characters ➢ Maximum password age = 60 days	No relevant exceptions noted.
CC5.3.3	Access to the Azure environment is restricted via unique user ID and password.	Inquired of the CIO to verify that access to the Azure environment was restricted via unique user ID and password.	No relevant exceptions noted.
		Inspected the Azure User List to verify that access to the Azure environment was restricted via unique user ID and password.	No relevant exceptions noted.
CC5.3.4	Remote access to the Azure environment is granted through an encrypted VPN connection that requires a certificate for authentication.	Inquired of the CIO to verify that remote access to the Azure environment was granted through an encrypted VPN connection that requires a certificate for authentication.	No relevant exceptions noted.
		Inspected the VPN configuration to verify that remote access to the Azure environment was granted through an encrypted VPN connection that requires a certificate for authentication.	No relevant exceptions noted.
CC5.3.5	Administrative access to Microsoft Azure Portal is restricted to the following personnel: ➢ CIO ➢ Director of Technology	Inquired of the CIO to verify that administrative access to Microsoft Azure Portal was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Azure Administrators listing to verify that administrative access to Microsoft Azure Portal was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
CC5.3.6	Access to the PaySound[SM] application is restricted via application account settings requiring a unique user ID and password.	Inquired of the CIO to verify that access to the PaySound[SM] application was restricted via application account settings requiring a unique user ID and password.	No relevant exceptions noted.
		Inspected the PaySound[SM] application to verify that access was restricted via application account settings requiring a unique user ID and password.	No relevant exceptions noted.
CC5.3.7	Full administrative access to the application is restricted to the following employees: ➢ COB ➢ CEO ➢ CIO ➢ VP Client Services ➢ Director of Technology ➢ Director of Administration ➢ Engagement Manager	Inquired of the CIO to verify that full administrative access to the application was restricted to the following employees: ➢ COB ➢ CEO ➢ CIO ➢ VP Client Services ➢ Director of Technology ➢ Director of Administration ➢ Engagement Manager	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Global Admins listing for the application to verify that full administrative access to the application was restricted to the following employees: ➢ COB ➢ CEO ➢ CIO ➢ VP Client Services ➢ Director of Technology ➢ Director of Administration ➢ Engagement Manager	No relevant exceptions noted.
CC5.3.8	Administrative access to the production database is restricted to the following personnel: ➢ CIO ➢ Director of Technology	Inquired of the CIO to verify that administrative access to the production database was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
		Inspected the database administrative access permissions to verify that administrative access to the production database was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
CC5.4 Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
CC5.4.1	Internal IT access requests are administered using a new employee on-boarding checklist and are required to be approved by the Director of Technology prior to granting access to systems.	Inquired of the CIO to verify that internal IT access requests were administered using a new employee on-boarding checklist and were required to be approved by the Director of Technology prior to granting access to systems.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A
CC5.4.2	System accounts assigned to terminated employees are deactivated upon notification of termination.	Inquired of the CIO to verify that system accounts assigned to terminated employees were deactivated upon notification of termination.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A
CC5.4.3	Termination of client access is approved by the Project Manager, COB, or CEO prior to removing access to client environment.	Inquired of the CIO to verify that termination of client access was approved by the Project Manager, COB, or CEO prior to removing access to client environment.	No relevant exceptions noted.
		Inspected the Termination Procedures and Termination Notifications for the population of clients terminated during the examination period to verify that termination of client access was approved by the Project Manager, COB, or CEO prior to removing access to client environment.	No relevant exceptions noted.
CC5.5 Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
N/A - RCG IT environment is hosted in Microsoft Windows Azure cloud. Access to the environment is restricted via user IDs and password and protected by HTTPS (SSL) encrypted sessions.			

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.6 Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.			
CC5.6.1	Administrative access to Microsoft Azure Portal is restricted to the following personnel: ➢ CIO ➢ Director of Technology	Inquired of the CIO to verify that administrative access to Microsoft Azure Portal was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
		Inspected the Azure Administrators listing to verify that administrative access to Microsoft Azure Portal was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
CC5.6.2	Microsoft Windows firewall is in place on RCG VMs hosted in the Microsoft Azure cloud and configured to filter unauthorized inbound traffic from the Internet.	Inquired of the CIO to verify that Microsoft Windows Firewall was in place on RCG VMs hosted in the Microsoft Windows Azure cloud and configured to filter unauthorized inbound traffic from the Internet.	No relevant exceptions noted.
		Inspected the configuration of Microsoft Windows firewall on one of the RCG VMs hosted in the Microsoft Azure cloud to verify that Microsoft Firewall was in place on RCG VMs hosted in the Microsoft Azure cloud and configured to filter unauthorized inbound traffic from the Internet.	No relevant exceptions noted.
CC5.6.3	Computers used by RCG employees and contractors are configured with whole disk encryption to restrict unauthorized access to stored data.	Inquired of the CIO to verify that computers used by RCG employees and contractors were configured with whole disk encryption to restrict unauthorized access to stored data.	No relevant exceptions noted.
		Inspected the encryption configurations to verify that computers used by RCG employees and contractors were configured with whole disk encryption to restrict unauthorized access to stored data.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.6.4	System accounts assigned to terminated employees are deactivated upon notification of termination.	Inquired of the CIO to verify that system accounts assigned to terminated employees were deactivated upon notification of termination.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A
CC5.6.5	Termination of client access is approved by the Project Manager, COB, or CEO prior to removing access to client environment.	Inquired of the CIO to verify that termination of client access was approved by the Project Manager, COB, or CEO prior to removing access to client environment.	No relevant exceptions noted.
		Inspected the Termination Procedures and Termination Notifications for the population of clients terminated during the examination period to verify that termination of client access was approved by the Project Manager, COB, or CEO prior to removing access to client environment.	No relevant exceptions noted.
CC5.6.6	Remote access to the Azure environment is granted through an encrypted VPN connection that requires a certificate for authentication.	Inquired of the CIO to verify that remote access to the Azure environment was granted through an encrypted VPN connection that requires a certificate for authentication.	No relevant exceptions noted.
		Inspected the VPN configuration to verify that remote access to the Azure environment was granted through an encrypted VPN connection that requires a certificate for authentication.	No relevant exceptions noted.
CC5.6.7	Access to the PaySound[SM] application is restricted via application account settings requiring a unique user ID and password.	Inquired of the CIO to verify that access to the PaySound[SM] application was restricted via application account settings requiring a unique user ID and password.	No relevant exceptions noted.
		Inspected the PaySound[SM] application to verify that access was restricted via application account settings requiring a unique user ID and password.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.6.8	Backup media is encrypted at rest.	Inquired of the CIO to verify that backup media is encrypted at rest.	No relevant exceptions noted.
		Inspected the Microsoft Azure backup access keys to verify that backup media was encrypted at rest.	No relevant exceptions noted.
CC5.7 The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security, availability, and confidentiality.			
CC5.7.1	Data transfers to and from the RCG environment hosted in Microsoft Azure are encrypted using SSL over HTTPS.	Inquired of the CIO to verify that data transfers to and from the RCG environment hosted in Microsoft Azure were encrypted using SSL over HTTPS.	No relevant exceptions noted.
		Inspected the configuration of the PaySound[SM] session to verify that data transfers to and from the RCG environment hosted in Microsoft Azure were encrypted using SSL over HTTPS.	No relevant exceptions noted.
CC5.8 Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
CC5.8.1	Computers used by RCG employees and contractors run anti-virus software to protect against viruses, malware, and malicious code.	Inquired of the CIO to verify that computers used by RCG employees and contractors ran anti-virus software to protect against viruses, malware, and malicious code.	No relevant exceptions noted.
		Inspected anti-virus configurations to verify that computers used by RCG employees and contractors ran anti-virus software to protect against viruses, malware, and malicious code.	No relevant exceptions noted.
CC5.8.2	RCG managed VMs hosted with Microsoft Windows Azure have antivirus software installed to protect against viruses, malware, and malicious code.	Inquired of the CIO to verify that RCG managed VMs hosted with Microsoft Windows Azure had antivirus software installed to protect against viruses, malware, and malicious code.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Endpoint anti-virus configurations to verify that RCG managed VMs hosted with Microsoft Windows Azure had antivirus software installed to protect against viruses, malware, and malicious code.	No relevant exceptions noted.
CC5.8.3	Antivirus software within the Azure environment is automatically updated with current virus signatures on a daily basis.	Inquired of the CIO to verify that antivirus software within the Azure environment was automatically updated with current virus signatures on a daily basis.	No relevant exceptions noted.
		Inspected the configuration of Symantec Endpoint Protection to verify that antivirus software within the Azure environment was automatically updated with current virus signatures on a daily basis.	No relevant exceptions noted.
CC6.0 System Operations: The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objective(s) of the principle(s) addressed in the engagement.			
CC6.1 Vulnerabilities of system components to security, availability, and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
CC6.1.1	The Incident Response Plan includes information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	Inquired of the CIO to verify that the Incident Response Plan included information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	No relevant exceptions noted.
		Inspected the Incident Response Plan to verify that it included information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC6.1.2	A Security Steering Committee is in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	Inquired of the CIO to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
		Inspected the Security Steering Committee Agendas and Meeting Minutes from meetings held during the examination period to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
CC6.1.3	Key performance metrics are monitored using the Microsoft Azure Endpoint Monitor that is configured to monitor and log the uptime and the response time of the PaySound[SM] website.	Inquired of the CIO to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
		Inspected the Microsoft Azure Endpoint Monitor to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
CC6.2 security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.			
CC6.2.1	The Incident Response Plan includes information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	Inquired of the CIO to verify that the Incident Response Plan included information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Incident Response Plan to verify that it included information concerning the identification of possible security breaches and the process for informing the appropriate internal and external resources.	No relevant exceptions noted.
CC6.2.2	A Security Steering Committee is in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	Inquired of the CIO to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
		Inspected the Security Steering Committee Agendas and Meeting Minutes from meetings held during the examination period to verify that a Security Steering Committee was in place to address security issues, security policy enhancements, security awareness training, and security planning for the company.	No relevant exceptions noted.
CC6.2.3	Key performance metrics are monitored using the Microsoft Azure Endpoint Monitor that is configured to monitor and log the uptime and the response time of the PaySound[SM] website.	Inquired of the CIO to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
		Inspected the Microsoft Azure Endpoint Monitor to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
CC6.2.4	The process for clients to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents is outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy.	Inquired of the CIO to verify that the process for client to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents was outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy to verify that the process for client to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents was outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy	No relevant exceptions noted.
CC7.0 Change Management: The criteria relevant to how the entity identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement.			
CC7.1 The entity's commitments and system requirements, as they relate to security, availability, and confidentiality, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.			
CC7.1.1	Change management policies and procedures are documented and available to guide personnel in the change management process.	Inquired of the CIO to verify that change management policies and procedures were documented and available to guide personnel in the change management process.	No relevant exceptions noted.
		Inspected the Change Management Policy to verify that change management policies and procedures were documented and available to guide personnel in the change management process.	No relevant exceptions noted.
CC7.1.2	A ticketing system is utilized to prioritize, track, and monitor client change requests.	Inquired of the CIO to verify that a ticketing system was utilized to prioritize, track, and monitor client change requests.	No relevant exceptions noted.
		Inspected the ticketing system to verify that a ticketing system was utilized to prioritize, track, and monitor client change requests.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.1.3	Development meetings are held on a weekly basis to assess and prioritize changes prior to performing development work.	Inquired of the CIO to verify that development meetings were held on a weekly basis to assess and prioritize changes prior to performing development work.	No relevant exceptions noted.
		Inspected the meeting invitation for a sample of weeks during the examination period to verify that development meetings were held on a weekly basis to assess and prioritize changes prior to performing development work.	No relevant exceptions noted.
CC7.1.4	Development changes and enhancements to the production environment are required to be reviewed and approved by the COB, CEO, or Client Services Manager before the changes are migrated to production.	Inquired of the CIO to verify that development changes and enhancements to the production environment were required to be reviewed and approved by the COB, CEO, or Client Services Manager before the changes were migrated to production.	No relevant exceptions noted.
		Inspected the JIRA tickets and Release Notes for a sample of releases during the examination period to verify that development changes and enhancements to the production environment were required to be reviewed and approved by the COB, CEO, or Client Services Manager before the changes were migrated to production.	No relevant exceptions noted.
CC7.1.5	Version control software is used to manage version control of developed code.	Inquired of the CIO to verify that version control software was used to manage version control of developed code.	No relevant exceptions noted.
		Inspected the configuration settings of the version control software to verify that version control software was used to manage version control of developed code.	No relevant exceptions noted.
CC7.1.6	Audit logs are used to track changes made to the production environment and are available for review as needed.	Inquired of the CIO to verify that audit logs were used to track all changes made to the production environment and were available for review as needed.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected an example Operations Log to verify that audit logs were used to track changes made to the production environment and were available for review as needed.	No relevant exceptions noted.
CC7.1.7	RCG maintains separate development and production environments.	Inquired of the CIO to verify that RCG maintained separate development and production environments.	No relevant exceptions noted.
		Inspected the configuration of RCG environment to verify that RCG maintained separate development and production environments.	No relevant exceptions noted.
CC7.2 Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
CC7.2.1	RCG systems are configured and maintained to meet the defined requirements of the IT Policy as contained within the Security Awareness Training Guide.	Inquired of the CIO to verify that RCG systems were required to be configured and maintained to meet the defined requirements of the IT Policy as contained within the Security Awareness Training Guide.	No relevant exceptions noted.
		Inspected the Security Awareness Guide documentation to verify that RCG systems were required to be configured and maintained to meet the defined requirements of the IT Policy as contained within the Security Awareness Training Guide.	No relevant exceptions noted.
CC7.2.2	Key performance metrics are monitored using the Microsoft Azure Endpoint Monitor that is configured to monitor and log the uptime and the response time of the PaySound[SM] website.	Inquired of the CIO to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
		Inspected the Microsoft Azure Endpoint Monitor to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.2.3	RCG performs vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments.	Inquired of the CIO to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments	No relevant exceptions noted.
		Inspected the vendor risk evaluations for current vendors and due diligence evaluations for "high risk" vendors to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors within the past 12 months.	No relevant exceptions noted.
CC7.3 Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
CC7.3.1	Change management policies and procedures are documented and available to guide personnel in the change management process.	Inquired of the CIO to verify that change management policies and procedures were documented and available to guide personnel in the change management process.	No relevant exceptions noted.
		Inspected the Change Management Policy to verify that change management policies and procedures were documented and available to guide personnel in the change management process.	No relevant exceptions noted.
CC7.3.2	A ticketing system is utilized to prioritize, track, and monitor client change requests.	Inquired of the CIO to verify that a ticketing system was utilized to prioritize, track, and monitor client change requests.	No relevant exceptions noted.
		Inspected the ticketing system to verify that a ticketing system was utilized to prioritize, track, and monitor client change requests.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.3.3	Development meetings are held on a weekly basis to assess and prioritize changes prior to performing development work.	Inquired of the CIO to verify that development meetings were held on a weekly basis to assess and prioritize changes prior to performing development work.	No relevant exceptions noted.
		Inspected the meeting invitation for a sample of weeks during the examination period to verify that development meetings were held on a weekly basis to assess and prioritize changes prior to performing development work.	No relevant exceptions noted.
CC7.4 Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and confidentiality commitments and system requirements.			
CC7.4.1	Change management policies and procedures are documented and available to guide personnel in the change management process.	Inquired of the CIO to verify that change management policies and procedures were documented and available to guide personnel in the change management process.	No relevant exceptions noted.
		Inspected the Change Management Policy to verify that change management policies and procedures were documented and available to guide personnel in the change management process.	No relevant exceptions noted.
CC7.4.2	Development meetings are held on a weekly basis to assess and prioritize changes prior to performing development work.	Inquired of the CIO to verify that development meetings were held on a weekly basis to assess and prioritize changes prior to performing development work.	No relevant exceptions noted.
		Inspected the recurring meeting invitation to the weekly Development Meeting to verify that development meetings were held on a weekly basis to assess and prioritize changes prior to performing development work.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.4.3	Development changes and enhancements to the production environment are required to be tested in the staging environment before being promoted to production.	Inquired of the CIO to verify that development changes and enhancements to the production environment were required to be tested in the staging environment before being promoted to production.	No relevant exceptions noted.
		Inspected the Jira tickets for a sample of releases during the examination period to verify that development changes and enhancements to the production environment were required to be tested in the staging environment before being promoted to production.	No relevant exceptions noted.
CC7.4.4	Development changes and enhancements to the production environment are required to be reviewed and approved by the COB, CEO, or Client Services Manager before the changes are migrated to production.	Inquired of the CIO to verify that development changes and enhancements to the production environment were required to be reviewed and approved by the COB, CEO, or Client Services Manager before the changes were migrated to production.	No relevant exceptions noted.
		Inspected the JIRA tickets and Release Notes for a sample of releases during the examination period to verify that development changes and enhancements to the production environment were required to be reviewed and approved by the COB, CEO, or Client Services Manager before the changes were migrated to production.	No relevant exceptions noted.
CC7.4.5	Access to source code is restricted to authorized personnel.	Inquired of the CIO to verify that access to source code was restricted to authorized personnel.	No relevant exceptions noted.
		Inspected Bitbucket Users and Groups to verify that that access to source code was restricted to authorized personnel.	No relevant exceptions noted.
CC7.4.6	Access to move the code from staging to production is restricted to the Director of Technology.	Inquired of the CIO to verify that access to move the code from staging to production was restricted to the Director of Technology.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Bitbucket Administrators group to verify that access to move the code from staging to production was restricted to the Director of Technology.	No relevant exceptions noted.
CC7.4.7	Version control software is used to manage version control of developed code.	Inquired of the CIO to verify that version control software was used to manage version control of developed code.	No relevant exceptions noted.
		Inspected the configuration settings of the version control software to verify that version control software was used to manage version control of developed code.	No relevant exceptions noted.
CC7.4.8	Audit logs are used to track changes made to the production environment and are available for review as needed.	Inquired of the CIO to verify that audit logs were used to track all changes made to the production environment and were available for review as needed.	No relevant exceptions noted.
		Inspected an example Operations Log to verify that audit logs were used to track changes made to the production environment and were available for review as needed.	No relevant exceptions noted.
CC7.4.9	RCG maintains separate development and production environments.	Inquired of the CIO to verify that RCG maintained separate development and production environments.	No relevant exceptions noted.
		Inspected the configuration of RCG environment to verify that RCG maintained separate development and production environments.	No relevant exceptions noted.
CC7.4.10	Emergency change guidelines are documented within the Change Management Policy and outline the process for implementing emergency changes to the production environment.	Inquired of the CIO to verify that emergency change guidelines were documented within the Change Management Policy and outline the process for implementing emergency changes to the production environment.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Emergency Change Process to verify that emergency change guidelines were documented within the Change Management Policy and outline the process for implementing emergency changes to the production environment.	No relevant exceptions noted.

Availability Principle and Criteria

The system is available for operation and use to meet the entity's commitments and system requirements.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.1 Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.			
A1.1.1	RCG performs a threat assessment at least annually to identify potential threats to its environment. Threats are reviewed and updated within the Business Continuity Plan.	Inquired of the CIO to verify that RCG performed a threat assessment at least annually to identify potential threats to its environment. Threats were reviewed and updated within the Business Continuity Plan.	No relevant exceptions noted.
		Inspected the Business Continuity Plan to verify that RCG performed a threat assessment at least annually to identify potential threats to its environment. Threats were reviewed and updated within the Business Continuity Plan.	No relevant exceptions noted.
A1.1.2	RCG performs vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments.	Inquired of the CIO to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments	No relevant exceptions noted.
		Inspected the vendor risk evaluations for current vendors and due diligence evaluations for "high risk" vendors to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors within the past 12 months.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.1.3	Key performance metrics are monitored using the Microsoft Azure Endpoint Monitor that is configured to monitor and log the uptime and the response time of the PaySound[SM] website.	Inquired of the CIO to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
		Inspected the Microsoft Azure Endpoint Monitor to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
A1.1.4	Microsoft Windows Azure Endpoint Monitor is configured to generate alert notifications when network performance exceeds predefined thresholds. Alert notifications are sent to the Director of Technology.	Inquired of the CIO to verify that Microsoft Windows Azure Endpoint Monitor was configured to generate alert notifications when network performance exceeds predefined thresholds. Alert notifications were sent to the Director of Technology.	No relevant exceptions noted.
		Inspected the Microsoft Windows Azure Endpoint dashboard and an example alert notification sent during the examination period to verify that Endpoint was configured to generate alert notifications when network performance exceeds predefined thresholds. Alert notifications were sent to the Director of Technology.	No relevant exceptions noted.
A1.2 Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.			
A1.2.1	RCG performs a threat assessment at least annually to identify potential threats to its environment. Threats are reviewed and updated within the Business Continuity Plan.	Inquired of the CIO to verify that RCG performed a threat assessment at least annually to identify potential threats to its environment. Threats were reviewed and updated within the Business Continuity Plan.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Business Continuity Plan to verify that RCG performed a threat assessment at least annually to identify potential threats to its environment. Threats were reviewed and updated within the Business Continuity Plan.	No relevant exceptions noted.
A1.2.2	RCG performs vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments.	Inquired of the CIO to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments	No relevant exceptions noted.
		Inspected the vendor risk evaluations for current vendors and due diligence evaluations for "high risk" vendors to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors within the past 12 months.	No relevant exceptions noted.
A1.2.3	Key performance metrics are monitored using the Microsoft Azure Endpoint Monitor that is configured to monitor and log the uptime and the response time of the PaySound[SM] website.	Inquired of the CIO to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.
		Inspected the Microsoft Azure Endpoint Monitor to verify that key performance metrics were monitored using the Microsoft Azure Endpoint Monitor that was configured to monitor and log the uptime and the response time of the PaySound[SM] website.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.2.4	Management has implemented a strategy for backup and restoration based on a review of business requirements. Full SQL database backups are performed weekly and database log backups are performed every 30 minutes. Backups are stored in Microsoft Windows Azure storage.	Inquired of the CIO to verify that management had implemented a strategy for backup and restoration based on a review of business requirements. Full SQL database backups were performed weekly and database log backups were performed every 30 minutes. Backups were stored in Microsoft Windows Azure storage.	No relevant exceptions noted.
		Inspected the database backup Job Properties and Log File to verify that management had implemented a strategy for backup and restoration based on a review of business requirements. Full SQL database backups were performed weekly and database log backups were performed every 30 minutes. Backups were stored in Microsoft Windows Azure storage.	No relevant exceptions noted.
		Inspected the SOC 2 Type 2 Service Auditor's report for Microsoft Cloud Infrastructure and Operations to verify that storage was geo-replicated across regions to ensure the integrity and availability of stored data.	No relevant exceptions noted.
A1.2.5	Backup jobs are configured to generate email alert notification in case of backup failure or error.	Inquired of the CIO to verify that backup jobs were configured to generate email alert notification in case of backup failure or error.	No relevant exceptions noted.
		Inspected the Database Backup Job Properties E-mail configurations to verify that backup jobs were configured to generate email alert notification in case of backup failure or error.	No relevant exceptions noted.
A1.2.6	Backup media is encrypted at rest.	Inquired of the CIO to verify that backup media is encrypted at rest.	No relevant exceptions noted.
		Inspected the Microsoft Windows Azure backup access keys to verify that backup media was encrypted at rest.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.2.7	RCG has developed a Business Continuity Plan that is required to be tested on a semi-annually basis to ensure system availability.	Inquired of the CIO to verify that RCG had developed a Business Continuity Plan that was required to be tested on a semi-annually basis to ensure system availability.	No relevant exceptions noted.
		Inspected the Business Continuity Plan to verify that RCG had developed a Business Continuity Plan that was required to be tested on a semi-annually basis to ensure system availability.	No relevant exceptions noted.
A1.3 Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.			
A1.3.1	Management has implemented a strategy for backup and restoration based on a review of business requirements. Full SQL database backups are performed weekly and database log backups are performed every 30 minutes. Backups are stored in Microsoft Windows Azure storage.	Inquired of the CIO to verify that management had implemented a strategy for backup and restoration based on a review of business requirements. Full SQL database backups were performed weekly and database log backups were performed every 30 minutes. Backups were stored in Microsoft Windows Azure storage.	No relevant exceptions noted.
		Inspected the database backup Job Properties and Log File to verify that management had implemented a strategy for backup and restoration based on a review of business requirements. Full SQL database backups were performed weekly and database log backups were performed every 30 minutes. Backups were stored in Microsoft Windows Azure storage.	No relevant exceptions noted.
		Inspected the SOC 2 Type 2 Service Auditor's report for Microsoft Cloud Infrastructure and Operations to verify that storage was geo-replicated across regions to ensure the integrity and availability of stored data.	No relevant exceptions noted.
A1.3.2	Backup jobs are configured to generate email alert notification in case of backup failure or error.	Inquired of the CIO to verify that backup jobs were configured to generate email alert notification in case of backup failure or error.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Database Backup Job Properties E-mail configurations to verify that backup jobs were configured to generate email alert notification in case of backup failure or error.	No relevant exceptions noted.
A1.3.3	RCG has developed a Business Continuity Plan that is required to be tested on a semi-annually basis to ensure system availability.	Inquired of the CIO to verify that RCG had developed a Business Continuity Plan that was required to be tested on a semi-annually basis to ensure system availability.	No relevant exceptions noted.
		Inspected the Business Continuity Plan to verify that RCG had developed a Business Continuity Plan that was required to be tested on a semi-annually basis to ensure system availability.	No relevant exceptions noted.

Confidentiality Principle and Criteria

Information designated as confidential is protected to meet the entity's commitments and system requirements.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
C1.1 Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.			
C1.1.1	RCG maintains an Information Classification Policy that classifies information entrusted to RCG from a third-party to its level of confidentiality and protection.	Inquired of the CIO to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
		Inspected the Information Classification Policy to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
C1.1.2	A Data Custody Chain Responsibilities policy defines procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	Inquired of the CIO to verify that the Data Custody Chain Responsibilities policy defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.
		Inspected the Data Custody Chain Responsibilities policy to verify that it defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.
C1.2 Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.			
C1.2.1	RCG maintains an Information Classification Policy that classifies information entrusted to RCG from a third-party to its level of confidentiality and protection.	Inquired of the CIO to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Information Classification Policy to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
C1.2.2	A Data Custody Chain Responsibilities policy defines procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	Inquired of the CIO to verify that the Data Custody Chain Responsibilities policy defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.
		Inspected the Data Custody Chain Responsibilities policy to verify that it defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.
C1.2.3	A ticketing system is utilized to prioritize, track, and monitor client change requests.	Inquired of the CIO to verify that a ticketing system was utilized to prioritize, track, and monitor client change requests.	No relevant exceptions noted.
		Inspected the ticketing system to verify that a ticketing system was utilized to prioritize, track, and monitor client change requests.	No relevant exceptions noted.
C1.2.4	Development meetings are held on a weekly basis to assess and prioritize changes prior to performing development work.	Inquired of the CIO to verify that development meetings were held on a weekly basis to assess and prioritize changes prior to performing development work.	No relevant exceptions noted.
		Inspected the meeting invitation for a sample of weeks during the examination period to verify that development meetings were held on a weekly basis to assess and prioritize changes prior to performing development work.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
C1.2.5	Development changes and enhancements to the production environment are required to be reviewed and approved by the COB, CEO, or Client Services Manager before the changes are migrated to production.	Inquired of the CIO to verify that development changes and enhancements to the production environment were required to be reviewed and approved by the COB, CEO, or Client Services Manager before the changes were migrated to production.	No relevant exceptions noted.
		Inspected the JIRA tickets and Release Notes for a sample of releases during the examination period to verify that development changes and enhancements to the production environment were required to be reviewed and approved by the COB, CEO, or Client Services Manager before the changes were migrated to production.	No relevant exceptions noted.
C1.2.6	Version control software is used to manage version control of developed code.	Inquired of the CIO to verify that version control software was used to manage version control of developed code.	No relevant exceptions noted.
		Inspected the configuration settings of the version control software to verify that version control software was used to manage version control of developed code.	No relevant exceptions noted.
C1.2.7	Audit logs are used to track changes made to the production environment and are available for review as needed.	Inquired of the CIO to verify that audit logs were used to track all changes made to the production environment and were available for review as needed.	No relevant exceptions noted.
		Inspected an example Operations Log to verify that audit logs were used to track changes made to the production environment and were available for review as needed.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
C1.2.8	Administrative access to Microsoft Azure Portal is restricted to the following personnel: ➢ CIO ➢ Director of Technology	Inquired of the CIO to verify that administrative access to Microsoft Azure Portal was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
		Inspected the Azure Administrators listing to verify that administrative access to Microsoft Azure Portal was restricted to the following personnel: ➢ CIO ➢ Director of Technology	No relevant exceptions noted.
C1.2.9	Internal IT access requests are administered using a new employee on-boarding checklist and are required to be approved by the Director of Technology prior to granting access to systems.	Inquired of the CIO to verify that internal IT access requests were administered using a new employee on-boarding checklist and were required to be approved by the Director of Technology prior to granting access to systems.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A
C1.2.10	System accounts assigned to terminated employees are deactivated upon notification of termination.	Inquired of the CIO to verify that system accounts assigned to terminated employees were deactivated upon notification of termination.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warrant the operation of the control did not occur during the examination period.	N/A
C1.2.11	Termination of client access is approved by the Project Manager, COB, or CEO prior to removing access to client environment.	Inquired of the CIO to verify that termination of client access was approved by the Project Manager, COB, or CEO prior to removing access to client environment.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Termination Procedures and Termination Notifications for the population of clients terminated during the examination period to verify that termination of client access was approved by the Project Manager, COB, or CEO prior to removing access to client environment.	No relevant exceptions noted.
C1.3 Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.			
C1.3.1	RCG maintains an Information Classification Policy that classifies information entrusted to RCG from a third-party to its level of confidentiality and protection.	Inquired of the CIO to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
		Inspected the Information Classification Policy to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
C1.3.2	A Data Custody Chain Responsibilities policy defines procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	Inquired of the CIO to verify that the Data Custody Chain Responsibilities policy defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.
		Inspected the Data Custody Chain Responsibilities policy to verify that it defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.
C1.3.3	Data transfers to and from the RCG environment hosted in Microsoft Windows Azure are encrypted using SSL over HTTPS.	Inquired of the CIO to verify that data transfers to and from the RCG environment hosted in Microsoft Windows Azure were encrypted using SSL over HTTPS.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the configuration of the PaySound[SM] session to verify that data transfers to and from the RCG environment hosted in Microsoft Windows Azure were encrypted using SSL over HTTPS.	No relevant exceptions noted.
C1.3.4	Remote access to the Azure environment is granted through an encrypted VPN connection that requires a certificate for authentication.	Inquired of the CIO to verify that remote access to the Azure environment was granted through an encrypted VPN connection that requires a certificate for authentication.	No relevant exceptions noted.
		Inspected the VPN configuration to verify that remote access to the Azure environment was granted through an encrypted VPN connection that requires a certificate for authentication.	No relevant exceptions noted.
C1.4 The entity obtains confidentiality commitments that are consistent with the entity's confidentiality requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.			
C1.4.1	RCG maintains an Information Classification Policy that classifies information entrusted to RCG from a third-party to its level of confidentiality and protection.	Inquired of the CIO to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
		Inspected the Information Classification Policy to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
C1.4.2	A Data Custody Chain Responsibilities policy defines procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	Inquired of the CIO to verify that the Data Custody Chain Responsibilities policy defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Data Custody Chain Responsibilities policy to verify that it defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.
C1.4.3	RCG performs vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments.	Inquired of the CIO to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments	No relevant exceptions noted.
		Inspected the vendor risk evaluations for current vendors and due diligence evaluations for “high risk” vendors to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors within the past 12 months.	No relevant exceptions noted.
C1.4.4	The process for clients to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents is outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy.	Inquired of the CIO to verify that the process for client to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents was outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy.	No relevant exceptions noted.
		Inspected the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy to verify that the process for client to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents was outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
C1.4.5	A Digital Lending Technology and Deposit Services Agreement is executed between the client and RCG prior to receipt of services.	Inquired of the CIO to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
		Inspected the executed Digital Lending Technology and Deposit Services Agreement for the population of clients on-boarded during the examination period to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
C1.5 Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.			
C1.5.1	RCG maintains an Information Classification Policy that classifies information entrusted to RCG from a third-party to its level of confidentiality and protection.	Inquired of the CIO to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
		Inspected the Information Classification Policy to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
C1.5.2	A Data Custody Chain Responsibilities policy defines procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	Inquired of the CIO to verify that the Data Custody Chain Responsibilities policy defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.
		Inspected the Data Custody Chain Responsibilities policy to verify that it defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
C1.5.3	RCG performs vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments.	Inquired of the CIO to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors in order to assess risks related to its vendors and their environments	No relevant exceptions noted.
		Inspected the vendor risk evaluations for current vendors and due diligence evaluations for “high risk” vendors to verify that RCG performed vendor risk evaluations and due diligence evaluations, if applicable, on new vendors and annual risk evaluations on existing vendors within the past 12 months.	No relevant exceptions noted.
C1.6 Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.			
C1.6.1	RCG maintains an Information Classification Policy that classifies information entrusted to RCG from a third-party to its level of confidentiality and protection.	Inquired of the CIO to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
		Inspected the Information Classification Policy to verify that RCG maintained an Information Classification Policy that classified information entrusted to RCG from a third-party to its level of confidentiality and protection.	No relevant exceptions noted.
C1.6.2	A Data Custody Chain Responsibilities policy defines procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	Inquired of the CIO to verify that the Data Custody Chain Responsibilities policy defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Data Custody Chain Responsibilities policy to verify that it defined procedures and requirements related to confidentiality of inputs, data processing, outputs, and disclosure of confidential information to third parties.	No relevant exceptions noted.
C1.6.3	The process for clients to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents is outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy.	Inquired of the CIO to verify that the process for client to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents was outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy.	No relevant exceptions noted.
		Inspected the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy to verify that the process for client to inform RCG of possible system security breaches, data confidentiality, availability, and other incidents was outlined in the Digital Lending Technology and Deposit Services Agreement and the Client Services Policy	No relevant exceptions noted.
C1.6.4	A Digital Lending Technology and Deposit Services Agreement is executed between the client and RCG prior to receipt of services.	Inquired of the CIO to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.
		Inspected the executed Digital Lending Technology and Deposit Services Agreement for the population of clients on-boarded during the examination period to verify that a Digital Lending Technology and Deposit Services Agreement was executed between the client and RCG prior to receipt of services.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
C1.7 The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.			
C1.7.1	Data retention and destruction policies and procedures are incorporated into the Security Awareness Training Guide and the Digital Lending Technology and Deposit Services Agreement.	Inquired of the CIO to verify that data retention and destruction policies and procedures were incorporated into the Security Awareness Training Guide and the Digital Lending Technology and Deposit Services Agreement.	No relevant exceptions noted.
		Inspected the Security Awareness Training Guide and the Digital Lending Technology and Deposit Services Agreement to verify that data retention and destruction policies and procedures were incorporated into the Security Awareness Training Guide and the Digital Lending Technology and Deposit Services Agreement.	No relevant exceptions noted.
C1.8 The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.			
C1.8.1	Data retention and destruction policies and procedures are incorporated into the Security Awareness Training Guide and the Digital Lending Technology and Deposit Services Agreement.	Inquired of the CIO to verify that data retention and destruction policies and procedures were incorporated into the Security Awareness Training Guide and the Digital Lending Technology and Deposit Services Agreement.	No relevant exceptions noted.
		Inspected the Security Awareness Training Guide and the Digital Lending Technology and Deposit Services Agreement to verify that data retention and destruction policies and procedures were incorporated into the Security Awareness Training Guide and the Digital Lending Technology and Deposit Services Agreement.	No relevant exceptions noted.