System and Organization Controls 2 (SOC 2®) Type 2 Report

Description of RightCapital Inc.'s Financial Planning System Relevant to Security

For the Period July 1, 2023 to June 30, 2024

System and Organization Controls 2 (SOC 2®) Type 2 Report

Description of RightCapital Inc.'s Financial Planning System
Relevant to Security

For the Period July 1, 2023 to June 30, 2024

Table of Contents

Section I. 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

To the Management of RightCapital Inc.:

Scope

We have examined RightCapital Inc.'s (RightCapital) accompanying description of its financial planning system found in Section III titled "Description of RightCapital Inc.'s Financial Planning System" throughout the period July 1, 2023 to June 30, 2024 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* (AICPA, *Description Criteria* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that RightCapital's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (AICPA, *Trust Services Criteria*).

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

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

Service Organization's Responsibilities

RightCapital is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that RightCapital's service commitments and system requirements were achieved. In Section II, RightCapital has provided the accompanying assertion titled "RightCapital Inc.'s Management Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. RightCapital is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section IV, "Description of Criteria, Controls, Tests and Results of Tests" of this report.

Opinion

In our opinion, in all material respects—

a. the description presents RightCapital's financial planning system that was designed and implemented throughout the period July 1, 2023 to June 30, 2024 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period July 1, 2023 to June 30, 2024 to provide reasonable assurance that RightCapital's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of RightCapital's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period July 1, 2023 to June 30, 2024 to provide reasonable assurance that RightCapital's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of RightCapital's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of RightCapital, user entities of RightCapital's financial planning system during some or all of the period July 1, 2023 to June 30, 2024, business partners of RightCapital subject to risks arising from interactions with the financial planning system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Fiondella, Milone & LaSaracina LLP

Glastonbury, Connecticut
September 25, 2024

Section II. RightCapital Inc.'s Management Assertion

RightCapital Inc.'s Management Assertion

We have prepared the accompanying description of RightCapital Inc.'s (RightCapital) financial planning system titled "Description of RightCapital Inc.'s Financial Planning System" throughout the period July 1, 2023 to June 30, 2024 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the financial planning system that may be useful when assessing the risks arising from interactions with RightCapital's system, particularly information about system controls that RightCapital has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (AICPA, *Trust Services Criteria*).

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

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

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

1) The description presents RightCapital's financial planning system that was designed and implemented throughout the period July 1, 2023 to June 30, 2024 in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period July 1, 2023 to June 30, 2024 to provide reasonable assurance that RightCapital's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of RightCapital's controls throughout that period.
3) The controls stated in the description operated effectively throughout the period July 1, 2023 to June 30, 2024 to provide reasonable assurance that RightCapital's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of RightCapital's controls operated effectively throughout that period.

RightCapital Inc. Management

Section III. Description of RightCapital Inc.'s Financial Planning System

Description of RightCapital Inc.'s Financial Planning System

Services Provided

RightCapital Inc. ("the Company" or "RightCapital") was founded in 2015 to provide financial planning services to financial professionals.

The Company's core application, RightCapital, is a web-based Software as a Service (SaaS) application that enables financial professionals to provide financial planning services to their clients. The Company's SaaS offering provides financial professionals:

- The ability to enter financial information about their clients, including but not limited to income, saving, expense, goal, investment account, property, and insurance information.
- The ability for their clients to link bank, credit, investment, and loan accounts through account aggregation services provided by a third party.
- Monte Carlo simulations illustrate the probability that clients will not run out of money before the end of their lives.
- Detailed cash flow projections showing projected client inflows, outflows, account balances, and net worth over time.
- Detailed tax projections and tax planning tools.
- Tools to illustrate education, insurance, debt, and student loan projections and solutions.
- A document storage vault to share documents with clients.
- PDF reports illustrating all components to share with clients.
- The ability, for an additional charge, to assess clients fees for financial planning.

To facilitate the financial planning processes RightCapital integrates with a number of other software providers and asset custodians, allowing financial professionals the ability to easily retrieve client information and/or client investment account details from those other systems.

The Company also provides a financial planning application programming interface (API) that allows financial institutions the ability to create their own planning tools leveraging the calculation engine that powers the Company's SaaS offering.

Principal Service Commitments and System Requirements

RightCapital designs its processes and procedures related to the Company's SaaS and API offerings to meet its objectives for its services. Those objectives are based on the service commitments that RightCapital makes to certain users, the laws and regulations that govern the provision of their services, and the financial, operational, and compliance requirements that RightCapital has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Documents reflecting the Terms of Service, Privacy Policy, Disclosure, and Security details can be found on our website (www.rightcapital.com).

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role. Internal users are required to utilize two-factor authentication to access company systems.

- Requirements for external users to log in to the system using a password, and options for two-factor authentication.

- Physical security provided through data center services provided by Amazon Web Services (AWS) and Microsoft Azure (MS Azure).

- Use of encryption technologies to protect customer data both at rest and in transit.

- Engineering team ensures security issues are factored into all system development.

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

Components of the system used to provide the services - Infrastructure

RightCapital runs on servers provided by AWS. All systems are accessed via the Internet and are accessible from any modern internet browser.

Employees access the application from an internet browser on company-supplied laptop computers.

Components of the system used to provide the services - Software

The Company's SaaS and API applications are web applications developed and maintained by in-house software engineering group. The software engineering group enhances and maintains solutions to provide service for the Company's subscribers. Software is not sold directly to consumers, only to financial professionals.

The Company's SaaS and API applications access RightCapital's calculation engine to process Monte Carlo and cash flow projections related to financial planning. The calculation engine is a separate application which takes in input files.

The Company's SaaS application website is a multiuser, web-based application that allows financial professionals and their clients to input data relevant to client's financial situation and review outputs, illustrate alternatives, store files, and generate reports.

The Company's API is an interface which allows external parties to supply input files and receive Monte Carlo or cash flow results.

Components of the system used to provide the services - People

The Company has a staff of approximately [redacted] employees organized in the following functional areas:

- *Product Support*. Staff that supports financial professionals who subscribe to the Company's services. Product Support representatives utilize RightCapital to answer customer questions and show customers how to use the services. Product support representatives take phone calls, answer online 'chat' questions, or respond to emails from financial advisors.

- *Customer Success.* Staff that helps financial professionals get started with RightCapital. Customer Success representatives utilize RightCapital to show advisors how to configure RightCapital, how to use the services, and how to help their clients use the services.

- *Sales*. Staff that facilitate the sale of the Company's SaaS and API offerings to financial professionals. Sales professionals utilize RightCapital to demonstrate the system's capabilities to potential customers and answer questions from potential customers.

- *Product*. Staff that designs and tests updates to RightCapital's services. Product staff uses RightCapital to design and test features, illustrate capabilities to potential customers, and train internal employees on the use of the services.

- *Marketing*. Staff focused on marketing the Company's offerings to financial professionals.

- *Engineering*. Staff responsible for development, testing, maintenance, security, and technology operations for our application and internal systems.

- *Training*. Staff focused on training customers and internal staff on RightCapital features and functionality.

- *Operations.* Staff focused on the subscription management operations, office operations, and financial operations.

- *Human Resource*. Staff responsible for recruiting, hiring, payroll, and people operations.

Components of the system used to provide the services – Data

Data, as defined by the Company, constitutes the following:

- Client data entered by financial professionals or clients.

- Client data brought in via integration with 3rd party software provider or asset custodian.

- Client data brought in via account aggregation provided by 3rd party provider.

- Financial professional data used to communicate with financial professionals and process subscription fees.
- Administrative data used to track and monitor subscriptions, capabilities, and other internal information.
- System files.
- Error logs.

Output reports are available in electronic PDF and/or comma-delimited value file exports. Access to certain data and reports is limited by job function.

Components of the system used to provide the services - Processes and procedures

Management has developed and communicated procedures to restrict logical access to RightCapital's platform. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output).
- Categorization of information.
- Assessment of the business impact resulting from proposed security approaches.
- Selection, documentation, and implementation of security controls.
- Performance of annual management self-assessments to assess 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 backup and offline storage.
- Incident response.
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

Relevant aspects of the control environment, risk assessment process, information and communication, and monitoring

The security category and applicable trust services criteria were used to evaluate the suitability of design of controls stated in the description. Security criteria and controls designed and implemented to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in Section IV of this report. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of the Company's description of the RightCapital SaaS and API application.

Relevant aspects of the control environment, risk assessment process, information and communication, and monitoring - Control environment

Management Philosophy

The Company's control environment reflects the philosophy of senior management concerning the importance of security of financial professional and client data and information. The importance of security is emphasized within RightCapital via the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. Security is highlighted in board meetings, quarterly employee meetings, one-on-one discussions with employees, and in public security and privacy policies listed on our website. In designing its controls, RightCapital has taken into consideration the relevance of controls to meet the relevant trust criteria.

Security Management

The Company has an information security team consisting of a security officer and engineers responsible for management of information security throughout the organization. They are responsible for developing, maintaining, and enforcing the Company's information security policies. The information security policy is reviewed annually by the CTO, CEO, and Sr. Management.

As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated to all relevant employees.

During annual security training and awareness programs, management ensures communication of the latest security policies.

Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

RightCapital uses two subservice organizations to perform certain functions that support the delivery of services. AWS provides data center and web hosting services and MS Azure provides data center services. Logical access security software, infrastructure, and architectures over protected information assets to protect them from security events (for example, standards for logical security tools and techniques restricting access to applications, access restricted to user with valid business needs, access to applications is reviewed on a periodic basis, system access to terminated users is removed upon notification and activities occurring through communication channels are restricted) are the responsibility of AWS and MS Azure and as such are not in scope for the criteria noted below:

- CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
  - The entity identifies, inventories, classifies, and manages information assets
  - Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets
  - Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely

- Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure and software
- New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use
- Processes are in place to protect encryption keys during generation, storage, use, and destruction.

- CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
  - The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.

Security Policies

The following security policies and related processes are in place for the RightCapital SaaS and API application:

- Data classification and business impact assessment.
- Selection, documentation, and implementation of security controls.
- Assessment of security controls.
- User access authorization and provisioning.
- Removal of user access.
- Monitoring of security controls.
- Security management.

Personnel Security

Background checks are performed on all new employees, who are also required to review and acknowledge their receipt of relevant security policies. The new positions are supported by job descriptions. Once employed, employees are subject to the Company's procedures for accessing systems and sanctions for violating the Company's information security policy. Employees are instructed to report potential security incidents to their manager immediately.

RightCapital's marketing services agreements instruct financial professionals to notify RightCapital if they become aware of a possible security breach.

Physical Security Controls

RightCapital uses two subservice organizations to perform certain functions that support the delivery of services. AWS to provide data center and web hosting services and MS Azure provides data center services. Physical access controls (for example, maintaining the electronic access control system, monitoring the grounds and facility, facilitating visitors, performing security inspections of the facility) are the responsibility of AWS and MS Azure and as such are not in scope for the criteria noted below:

- CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
  - Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner
  - Processes are in place to remove access to physical resources when an individual no longer requires access
  - Processes are in place to periodically review physical access to ensure consistency with job responsibilities.

Change Management

The Company has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure and software are developed and tested in a separate development or test environment. All changes are tested and reviewed in an integrated staging environment prior to release to production. Developers do not have the ability to migrate changes into production environments.

The Company has a formalized security and systems development methodology that includes planning, design, testing, implementation, and maintenance.

The Company uses a standardized server build checklist to help secure its servers, and it conducts quarterly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with the Company's patch management process.

System Monitoring

The security administration team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed daily by the security administration team using a security incident and event monitoring (SIEM) product. Additionally, the security administration team has developed and will review the following SIEM reports:

- Failed object level access.
- Daily IDS or IPS attacks.
- Critical IDS or IPS alerts.
- Devices not reporting in the past 24 hours.
- Failed login detail.
- Firewall configuration changes.

- Windows policy changes.
- Windows system shutdowns and restarts.
- Security events requiring further investigation are tracked using a help desk ticket and monitored until resolved.

RightCapital uses a subservice organization, AWS to provide data center and web hosting services. System operations monitoring and detection controls for system data and software located with the AWS data center are the responsibility of AWS and as such are not in scope for the criteria noted below:

- CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
  - The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives
  - The IT system includes a change- detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files
  - Procedures are in place to detect the introduction of unknown or unauthorized components.
- CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
  - The entity obtains, reviews and evaluates attestation reports to ensure controls are designed and operate effectively.

Subservice Organization Monitoring

RightCapital monitors its subservice organizations according to compliance procedures by identifying and ranking the subservice organizations based on business-critical functions. AWS and MS Azure are the only subservice organizations currently used by RightCapital. RightCapital reviews AWS and MS Azure audit reports (e.g. SOC reports) to identify any potential issues. If any security concerns are found, RightCapital will reassess the relationship with the subservice organizations and put a plan in action to mitigate the risks to RightCapital users and/or terminate the relationship.

Complementary Subservice Organization Controls (CSOCs)

RightCapital uses two subservice organizations (AWS and MS Azure) to provide data center and web hosting services which are not included in the scope of this report. Complementary Subservice Organization Controls (CSOCs) that are necessary to achieve the commitments and system requirements related to Common Criteria 6.1, 6.4, 6.6, 7.1 and 7.4 are: subservice organizations should have general information technology logical and physical access controls and system operations monitoring and detection controls in place to protect the physical assets, data and software within the data center and hosted environment.

Complementary User Entity Controls

Certain trust services criteria identified in this report can only be achieved if complementary user entity controls, related to RightCapital service commitments and system requirements, are suitably designed and operating effectively, along with related controls at RightCapital. The user entity controls presented below should not be regarded as a comprehensive list of all of the controls that should be employed by user entities.

Complementary User Entity Controls	Common Criteria
Report security related issues to the product support team in a timely manner. Monitor for and respond to product support team on actions required to support issue resolution.	CC2.5
Protect their passwords to ensure security works as designed; do not write down or email passwords to others.	CC6.2
Read and understand communications from RightCapital about any changes to the system	CC2.2
Do not input private or confidential information in the system in an area not intended for such information.	CC8.1
Do not manipulate any data outputs generated out of RightCapital.	CC2.3

Problem Management

Security incidents and other IT-related problems are reported to management and the engineering team. Issues are tracked using a service desk ticket and monitored until resolved.

Data Backup and Recovery

The Company uses data replication to back up its data files and software. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized personnel.

System Account Management

The Company has implemented role-based security to limit and control access within RightCapital's systems. Employees are granted logical and physical access to in-scope systems based on documented approvals by appropriate management personnel. The ability to create or modify accounts and privileges is limited to authorized personnel. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

Administrative access to Active Directory, Unix, and RightCapital servers and databases is restricted to authorized employees.

Unique user names and passwords are required to authenticate all users to RightCapital's services, as well as to the facility services, transportation provider, member services, and client reporting websites. Password parameters consist of the following:

- Passwords contain a minimum of eight characters, including one numeric character.
- Log-on sessions are terminated after three failed log-on attempts.
- Users cannot reuse the last ten passwords.

Relevant aspects of the control environment, risk assessment process, information and communication, and monitoring - Risk assessment process

The Company regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security based on the applicable trust services criteria set forth in TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy* (AICPA, *Trust Services Criteria*).

The information security team assesses security risks on an ongoing basis. This is done through reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment.

An IT strategic plan is developed annually by the CTO and is communicated to and approved by senior management. As part of this plan, strategic IT risks affecting the organization and recommended courses of action are identified and discussed.

Senior management, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on RightCapital's security policies.

Changes in security threats and risks are reviewed by RightCapital, and updates to existing control activities and information security policies are performed as necessary.

Relevant aspects of the control environment, risk assessment process, information and communication, and monitoring - Information and communication systems

The Company has an information security policy 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 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.