



SOC 2 REPORT

FOR

DRIVEWEALTH PLATFORM

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON
CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

APRIL 1, 2022, TO MARCH 31, 2023

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

This report is intended solely for use by the management of DriveWealth, LLC, user entities of DriveWealth, LLC's services, and other parties who have sufficient knowledge and understanding of DriveWealth, LLC's services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2 MANAGEMENT'S ASSERTION	5
SECTION 3 DESCRIPTION OF THE SYSTEM	7
SECTION 4 TESTING MATRICES	23
SECTION 5 OTHER INFORMATION PROVIDED BY DRIVEWEALTH	57

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To DriveWealth, LLC:

Scope

We have examined DriveWealth, LLC's ("DriveWealth" or the "service organization") accompanying description of its DriveWealth Platform system, in Section 3, throughout the period April 1, 2022, to March 31, 2023, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that DriveWealth's service commitments and system requirements were achieved based on the trust services criteria relevant to security, and availability ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

The information included in Section 5, "Other Information Provided by DriveWealth" is presented by DriveWealth management to provide additional information and is not a part of the description. Information about DriveWealth's management's responses to exceptions noted has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve DriveWealth's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

DriveWealth 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 DriveWealth's service commitments and system requirements were achieved. DriveWealth has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. DriveWealth 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 (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the 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; and
- Evaluating the overall presentation of the description.

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

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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 users may consider important to meet their informational needs.

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

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

Description of Test of Controls

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

Opinion

In our opinion, in all material respects,

- a. the description presents the DriveWealth Platform system that was designed and implemented throughout the period April 1, 2022, to March 31, 2023, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that DriveWealth's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of DriveWealth's controls throughout that period; and

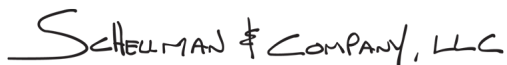
- c. the controls stated in the description operated effectively throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that DriveWealth's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of DriveWealth's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of DriveWealth; user entities of the DriveWealth Platform system during some or all of the period of April 1, 2022, to March 31, 2023, business partners of DriveWealth subject to risks arising from interactions with the DriveWealth Platform 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 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; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

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

 SCHEELMAN & COMPANY, LLC

Washington, District of Columbia
May 3, 2023

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of the DriveWealth Platform system, in Section 3, throughout the period April 1, 2022, to March 31, 2023, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, ("description criteria"). The description is intended to provide report users with information about the DriveWealth Platform system that may be useful when assessing the risks arising from interactions with DriveWealth's system, particularly information about system controls that DriveWealth 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 and availability ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

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

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

- a. the description presents the DriveWealth Platform system that was designed and implemented throughout the period April 1, 2022, to March 31, 2023, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that DriveWealth's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of DriveWealth's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that DriveWealth's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of DriveWealth's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

DriveWealth is an investing platform company that provides clearing services to registered counterparties, globally. Founded in 2012 and based out of Chatham, New Jersey, DriveWealth has clients in over 150 countries. DriveWealth clearing platform allows counterparty customers to make investments in U.S. securities. A key product feature is that DriveWealth allows its counterparty's customer to place dollar based and fractional share orders, removing the hurdle for retail customers to access many high share priced securities.

Through its clearing platform technology, DriveWealth delivers a full suite of APIs providing counterparties with a seamless integration. DriveWealth offers exchange listed securities and has developed a retail-focused surveillance system designed to provide full transparency and oversight to its counterparties, in addition to its own surveillance needs. The firm has further developed several micro-services which are designed to control various retail-related activities, to mitigate DriveWealth and the customer's risk in trading. By way of example, the firm has implemented a real-time margin trading system, which tracks customer margin debit to ensure that the risk of using margin is managed properly. Other system controls, alerting and reporting includes the monitoring and detection of Good Faith Violations, Pattern Day Trading violations and a series of other monitoring tools to ensure control around its system and activity on its platform.

Description of Services Provided

The DriveWealth Platform is an investing platform that provides retail investors the ability to invest in the U.S. stock market with fewer monetary requirements. The DriveWealth Platform has:

- Removed the requirement to purchase securities in share quantities, allowing for dollar-based investing.
- Lowered the cost of transacting in securities through the efficiencies of technology.
- No minimum account balance requirement.

The two main services that are provided by DriveWealth are broken into two difference divisions:

- **Wealth Management and Advisory Services:** DriveWealth offers a suite of digital investment productions to a global audience. DriveWealth enables their partners to onboard global customers and their assets, currently servicing over 100 countries.
- **Brokerage Solutions:** DriveWealth provides a digital brokerage platform which is open to the world's leading financial market to all investors. Through DriveWealth's application programming interface (API) driven process, customers have an onboarding experience which includes account setup, along with a variety of account types so that a full suite of services can be provided to customers.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

DriveWealth designs its processes and procedures to meet its objectives for the DriveWealth Platform. Those objectives are based on the service commitments that DriveWealth makes to its customers. Security and availability commitments to customers are documented and communicated in service level agreements (SLAs) and non-disclosure agreements.

The principal service commitments and system requirements related to the DriveWealth Platform system include the following:

Principal Service Commitments and System Requirements		
Trust Services Category	Service Commitments	System Requirements
Security	<ul style="list-style-type: none"> Limited access to systems, application, and the Amazon Web Services (AWS) environment Encryption in transit data Encryption of data in storage Application security requirements Perform risk assessments for both internal and external threats to the system and its information 	<ul style="list-style-type: none"> Logical access standards including employee provisioning and deprovisioning standards Encryption standards Incident handling standards Change management standards Risk management standards
Availability	<ul style="list-style-type: none"> Ability to recover and restore customer data Included Products and Services each available with a monthly uptime percentage of at least 99.95% 	<ul style="list-style-type: none"> System monitoring Backup and recovery standards Physical and environmental protections

In accordance with DriveWealth’s assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

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

Infrastructure and Software

The DriveWealth Platform is a cloud-based system available through a set of representational state transfer (REST) and financial information exchange (FIX) APIs which provides access to the US Markets. Through the various REST API sets, customers can onboard, fund, and manage their brokerage operations. DriveWealth also offers a front-end application, Zeppelin, which provides a user-interface into the APIs.

DriveWealth utilizes AWS for underlying infrastructure as a service (IaaS). AWS is responsible for providing physical safeguarding of IT infrastructure, to help ensure unauthorized access to the IT infrastructure does not occur. AWS is also responsible for providing environmental safeguards (e.g., power supply, temperature control, fire suppression, etc.) against certain environmental threats. DriveWealth uses AWS’s collection of pre-build services as a foundation for the platform which provides horizontal and vertical scalability, with the inherited security provided by AWS’s cloud-based infrastructure.

The production infrastructure resides within AWS US data centers. For high availability and infrastructure resilience, the AWS production infrastructure is distributed across availability zones within the region. Availability zones within AWS are isolated data center locations, which are physically separated from each other within the same geographic region. Since each zone is independent from the other, failures in one zone do not affect other zones; therefore, if one zone becomes unavailable, traffic can be routed to another zone to allow for continued uptime and availability of the running service.

DriveWealth’s system was designed using a message-based architecture, which uses a java message service (JMS) bus to facilitate communications between services. Plugging into the message bus, are a series of micro services, which are micro applications that manage the various functionality of the system, this reduces a variety of risks, including deployment risk and downtime exposures. The message bus, micro services, load balancer and databases all reside inside DriveWealth’s virtual private cloud (VPC) within AWS.

DriveWealth’s network architecture places externally accessible resources, such as the load balancers and FIX Servers, in a “public” subnet that has internet connectivity managed by AWS managed firewall (security groups). API Servers, micro-services, processing resources, databases, and internal systems reside in a “private” subnet with no inbound connectivity possible. The AWS security groups that segment traffic between types of services are restrict-by-default and allow only sourced traffic on specified protocols to pass between instances. Any connectivity to external services is managed by these security groups, which control the authorized access to DriveWealth’s system. The system was designed to control (implicitly) the external service communications with DriveWealth’s platform.

The production database is a managed no-SQL database provided by AWS. It is replicated real-time across availability zones within the region.

DriveWealth’s development and user acceptance testing (UAT) environments reside in separate and distinct environments on the AWS platform. The environments are logically and physically segmented from the production environment and make use of Amazon’s account boundaries to ensure the accounts remain distinct.

The in-scope infrastructure consists of multiple systems as shown in the table below:

Primary Infrastructure		
Production System	Business Function Description	Platform
Identity Provider (IdP)	Identity and access management cloud platform used for single sign-on.	Okta
AWS Cloud Environment	AWS – provides identity and access management (IAM), virtualized network, and processing infrastructure to host the DriveWealth platform.	Linux
	Security Groups – virtual firewalls used to configure, control, and restrict inbound and outbound network traffic into the production infrastructure within the AWS cloud environment.	
	Web Application Firewall (WAF) – provides packet filtering for web traffic from untrusted sources such as the public Internet.	
Production servers	Application, web, and API servers, supporting the platform and related services.	
Production databases	AWS DynamoDB databases used for storage of platform data, including restricted and confidential information.	Proprietary NoSQL
	Snowflake databases contains metadata and historical usage data, about the objects in the organization and accounts	Snowflake
VPN	Provides access control, endpoint security, and authentication and authorization services to production environments.	OpenVPN

Primary Infrastructure		
Production System	Business Function Description	Platform
DriveWealth Platform		
Front-office API set	REST-based API set designed for communication between an end-client device and the DriveWealth platform.	REST
Back-office API set	REST-based API set designed for communication between a partner server and the DriveWealth platform.	
FIX APIs	FIX-based APIs for trade execution.	FIX 4.2
Zeppelin	Brokerage administration user interface.	Linux and hypertext transfer protocol secure (HTTPS)

People

The personnel supporting the DriveWealth Platform includes, but is not limited to, the following:

- Executive Management – Responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Human Resources (HR) – Responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- Corporate Services – Responsible for finance, IT, renewals, and procurement, legal, and sales operations.
- Software Development – Responsible for risk management and identification, monitoring, and compliance of security issues and incidents throughout the service delivery infrastructure.
- Product Management – Responsible for product launches, responding to customer request for proposals, and user interface design.
- Customer Success – Responsible for customer service activities.

Procedures

Access, Authentication and Authorization

Documented information security policies and procedures are in place to govern information security standards. These policies and procedures are reviewed by senior management on at least an annual basis and are made available to employees via the corporate intranet.

Access to the production environment is restricted by the implementation of identification, authentication, and authorization mechanisms governed by backend IAM privileges within AWS. To access production systems, users must first login to the AWS management console, which enforces password parameters including password minimum length, password expiration intervals, password complexity and minimum history requirements. Production servers can also be reached by authenticating to the VPN and connecting via secure shell (SSH) to the server. The AWS database is restricted to users with authorized IAM AWS access. The Snowflake databases require a username, password, and two-factor authentication. An IdP is utilized to manage access to security support tools including the password vault which maintains the production server keys. Permissions are granted based on the user's job role. The application enforces password minimum length and complexity requirements.

Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel. In addition, predefined security groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.

Access Requests and Access Revocation

Prior to granting access to DriveWealth systems, including AWS, production server operating systems, VPN, databases, and application, a user's supervisor reviews the user access request. Requests for access to the DriveWealth systems are documented in a ticketing system. Once a request is created in the ticketing system, system owners are required to provide approval before access is granted.

Termination tickets are completed, and system access is revoked for employees as a component of the employee termination process on the date of termination. When an employee submits their resignation or is involuntarily terminated, a ticket is created with the employee's last day of employment. System owners are required to remove access prior to the last day of employment and track progress within the ticket. Logical access of AWS user accounts and administrators is reviewed and approved by management on at least an annual basis. In the event that inappropriate access is discovered, it is corrected and documented in the results of the review. Access to the application for DriveWealth personnel is managed by the IT team. Access provisioning and deprovisioning from the client side is the client's responsibility.

System Security, Operations, and Monitoring

Documented policies and procedures are in place to guide personnel in network security practices that include, but are not limited to, perimeter security, and access and authorization. These policies and procedures are reviewed by senior IT and operations personnel on at least an annual basis and are made available to employees via the corporate intranet. The network security policies provide details on the firewall system and how security groups are configured to deny any type of network connection that is not explicitly authorized by a firewall system. Furthermore, management personnel create an incident ticket to monitor and track the remediation of network issues identified through resolution.

Security groups are in place to restrict access to and from the network. The security groups are configured to deny any type of network connection that is not explicitly authorized by a rule. An intrusion prevention system (IPS) is in place to analyze network events and is configured to send e-mail notification alerts to IT personnel regarding possible or actual network security breaches. Management personnel create an incident ticket to monitor and track the remediation of issues identified through resolution.

Internal and external penetration assessments are conducted by a third-party on an annual basis to assess vulnerabilities of the infrastructure. Management personnel create an incident ticket to monitor and track the remediation of any vulnerabilities identified through resolution.

The cloud operations team maintains formally documented standard build procedures for the installation of new production systems and the maintenance of existing systems.

Logging and monitoring software are configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization and alert the information security team upon detection of unusual system activity or service requests. The following tools are used in the DriveWealth environment:

- Enterprise monitoring tools – monitors for metrics such as central processing unit (CPU) utilization, memory usage, and website uptime.
- WAF – monitors the cloud environment and alerts on potential suspicious activity or unsecure ports.
- Intrusion detection system (IDS) – monitors the environment using cloud machine learning and sensor machine learning and alerts on potential suspicious activity.

The software is configured to alert IT / operations personnel when predefined thresholds are exceeded. IT and operations personnel will investigate and resolve identified issues.

The technology team meets to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures. These meetings are held weekly and include various members of the cloud operations team. The intent of these meetings is to ensure that proper resolution steps are being taken for current incidents and that proper planning for new threats to the system are being considered.

Encryption

DriveWealth utilizes various forms of encryption within their environment to help ensure that end user communications with system are secure and that data held within the boundaries of the system is rendered unreadable at rest. Web servers utilize TLS encryption for web communication sessions and for DriveWealth personnel accessing systems. An encrypted VPN is required for remote access to servers to help ensure the security and integrity of the data passing over the public network. The VPN is configured with advanced encryption standard (AES-256) cipher configuration. Additionally, client data is stored in encrypted format in the database at rest. Access to cryptographic keys is restricted to authorized personnel.

Incident Response

Documented incident response procedures are in place to guide incident response process and include the assignment of roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program, containment of the incident and threat, mitigating the effects of ongoing security incidents, remediation of the incident, restoration of operations, communication protocols and timing to affected parties, and lessons learned. Additionally, the policy includes steps for identifying incidents and properly documenting them. Root cause analysis is required to help identify the issue and ensure that it does not occur again.

Management personnel utilize a ticketing system to manage system incidents, response, and resolution. Security incidents and impact of security events are discussed during security meetings which are held on a monthly basis to ensure that the incident response procedures were followed and that incidents were resolved. In addition, management personnel discuss the effect of identified security vulnerabilities on the ability to meet business objectives and identify corrective measures.

Change Management

Documented change management policies and procedures are in place to guide personnel in the system development and change management processes, including submitting change requests, change request prioritization, and approving change requests.

In order to keep track of each application and infrastructure change, a ticketing system is utilized. Within this ticketing system, development personnel are able to maintain, manage, and monitor enhancement, developments, and maintenance activities and to document change requests prior to implementation. Change management meetings are held on a weekly basis to review the status of new and pending changes to production. During these meetings there is a review of any high priority changes along with the status of production application and infrastructure changes for the week. Development and testing efforts take place in environments that are logically separated from the production environment to help ensure that changes made within the test environment do not affect changes in the production environment. The separate environments include development, testing, and production.

A development platform is utilized by development personnel to help ensure that the ability to change application and infrastructure source code is restricted to authorized personnel. The development platform allows personnel to check out different versions of the code for editing. Once users are ready to update the code repository, they check the code back in and request for their change to be merged with the main code branch. Changes to source code result in the creation of a new version of code. Prior versions of code are logged enabling a previous version to be restored in the event that an update needs to be made. Write access to the repositories containing application and infrastructure source is restricted to user accounts accessible by authorized personnel.

After development, engineering personnel perform testing and approval of application and infrastructure code changes which are documented within the change request. Depending on the nature of the change, application changes may require additional testing. If testing is unsuccessful, the change moves back to the development team to make amendments as needed before resubmitting to engineering personnel for a further round of testing. Once testing has passed and approval is documented within the change request, IT and operations management personnel are responsible for providing final approval prior to the application or infrastructure change implementation. The change request activity is integrated into the ticketing system where the change is reviewed, and final approvals are documented prior to implementation. The ability to implement application and infrastructure changes is restricted to authorized personnel through the use of elevated access rights on production systems. Furthermore, a file integrity monitoring tool is in place to track code changes.

Data Backup

DriveWealth utilizes AWS to perform scheduled system and database backups. Access to the backup data is restricted to user accounts accessible by authorized personnel in the AWS portal. AWS is responsible for maintaining infrastructure in a manner that allows DriveWealth to retrieve their data on demand.

Operations personnel perform backup restores at least annually to verify that system components can be recovered from system backups.

Infrastructure Redundancy and Disaster Recovery

Redundancy of infrastructure components is built into the architecture to help mitigate the risk of production availability issues. This is done through live replicating from two hot connections to the AWS US-east-1a and US-east-1b. Furthermore, there are configurations in place that if AWS fails, the backup availability zone is US-east-1b.

Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plan identifies vulnerabilities and recommends necessary measures to prevent extended service outages, encompassing all DriveWealth system sites and operations facilities. IT personnel perform disaster recovery testing in addition to the previous mentioned backup restores on an annual basis to ensure that operations can be successfully restored and update the plan as needed.

Media Handling and Disposal

A media handling and disposal policy is in place to guide personnel in requirements for the secure handling by data classification types as well as disposal of media when no longer required. This can include the physical destruction of non-electronic media, or the physical and data destruction related to electronic media such as of personal computers, network equipment, hard drives, and handheld devices. Only non-sensitive data may be disposed of without sanitization measures; data in other classifications must be disposed of when no longer necessary and sensitive data is cleared and purged to render it unrecoverable utilizing industry-accepted standards for secure deletion or physical destruction.

Vendor Management

In addition to monitoring the subservice organization, DriveWealth maintains policies and procedures to assist in onboarding, managing risks, and ongoing monitoring of vendors deemed to be critical to operations by management. Vendors are required to sign contracts when onboarded, including non-nondisclosure agreements, that help communicate security and information safeguarding requirements. In addition to monitoring performance as part of day-to-day operations, management performs a formal review of critical vendors on an annual basis. This usually entails a documented review of available attestation or other audit reports.

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Customer account information	Customer Account information can be viewed through the Zeppelin user interface (UI) or retrieved via the Back-Office API.	Confidential
Customer transactions	Customer transaction information can be viewed through the Zeppelin UI or retrieved via the Back-Office or Front-Office APIs.	
Market data	Market data is delivered through the Back-Office or Front-Office APIs.	Sensitive

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
System metrics and logs	Available via AWS Management Console or the centralized logging platform.	Sensitive
Referential Data (instruments, countries, etc.)	Can be viewed through the Zeppelin UI, retrieved via the Back-Office or Front-Office APIs, or available through the reporting services.	Public

Significant Changes During the Review Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The cloud hosting services provided by AWS were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at DriveWealth, and the types of controls expected to be implemented at AWS to achieve DriveWealth's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for managing and monitoring logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the DriveWealth systems reside.	CC6.1, CC6.2, CC6.3, CC6.5, CC6.6, CC7.2
AWS is responsible for restricting and monitoring physical access to data center facilities underlying network, virtualization management, and storage devices where the DriveWealth applications reside.	CC6.4, CC6.5, CC7.2
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where DriveWealth systems reside.	CC6.7
AWS is responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2
AWS is responsible for providing redundant underlying infrastructure components to help ensure that DriveWealth's systems are able to be restored.	A1.2

CONTROL ENVIRONMENT

The control environment at DriveWealth is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of DriveWealth control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of DriveWealth's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example. Specific control activities that the service organization has implemented in this area are described below.

- Background checks are performed for employees as a component of the hiring process.
- A code of conduct is in place to communicate established workplace conduct standards, acceptable use, and conduct enforcement procedures to internal users.
- Employees are required to sign an employment agreement form upon hire indicating that they understand their responsibility for adhering to company policies.
- Employees are required to sign a non-disclosure agreement (NDA) upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.
- Vendors are required to sign an agreement about their requirements to adhere to certain commitments and requirements as they pertain to security.

Board of Directors

DriveWealth's control consciousness is influenced significantly by its board of directors. Specific control activities that the service organization has implemented in this area are described below.

- The board of directors establishes and maintains a formal charter and set of bylaws which describe their responsibilities and oversight of management's system of internal control.
- The board of directors has members who are, by majority, independent from management and are objective in evaluations and decision making.
- Strategic plans are established by the board of directors to help guide management personnel in achieving organizational objectives and to establish performance measures for management personnel to be evaluated against on at least an annual basis.
- Management provides the results of control assessment reports to the board of directors on at least an annual basis.

Organizational Structure and Assignment of Authority and Responsibility

DriveWealth's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. DriveWealth management believes that establishing

a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. DriveWealth has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities.

This factor includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. Policies and communications are in place to help ensure that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. In addition to a formal charter and set of bylaws the board of directors has put in place to establish responsibilities, specific control activities that DriveWealth has implemented in this area are described below.

- Organizational charts are communicated to define key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system.
- Documented employment position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.

Commitment to Competence

DriveWealth management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. DriveWealth's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that the service organization has implemented in this area are described below.

- New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
- Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies.
- A formal training budget is available to new and existing employees to help maintain and advance the skill level of personnel.

Accountability

DriveWealth management establishes accountability by setting a strong tone at the top and holding those accountable for internal control responsibilities. Management communicates the internal control responsibilities and the criteria that employees will be measured against as well as incentives and other rewards. Management also provides the results of control assessment reports to the board of directors on at least an annual basis. In addition to documented position descriptions, DriveWealth maintains a code of conduct to communicate established workplace conduct standards, acceptable use, and conduct enforcement procedures to internal users. Additional policies are in place that address remedial actions for lack of compliance with policies and procedures.

RISK ASSESSMENT

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

Objective Setting

The risk assessment process involves a dynamic process that includes identification and analysis of risks that pose a threat to the organization's ability to perform the in-scope services. The process first starts with determining the organization's objectives as these objectives are key to understanding the risks and allow identification and analysis of those risks relative to the objectives. Management formally documents an organization strategy and performance policy and updates it on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives. An information security committee charter is in place to document company operations, reporting, and compliance objectives and establish governance over the risk management process. Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.

Risk Identification and Analysis

An information security committee is in place to establish governance over the risk management process. While identifying applicable risks to operations, DriveWealth uses a risk rating system based on probability and impact to determine the overall risk level, specifically considering threats that would result in financial loss, system disruption, and interruption of business activity.

DriveWealth risk management process is based on the following systematic principles which shall adapt to DriveWealth's fluctuating risk appetite and risk tolerance:

- Communication and context – Establish the criteria against which internal and external risks will be evaluated and defined.
- Identification – Identify how certain events could pose a risk to DriveWealth objectives.
- Documentation – Systematically document risks in a risk register.
- Analysis and evaluation – Determine consequences and likelihood of risk and compare risk levels (i) in accordance with an internationally recognized risk management framework, such as the NIST framework, and (ii) against the company's objectives.
- Monitor – Continuously monitor the effectiveness of the risk management process.

As part of the risk assessment process, management identifies business objective risks, assessing changes to the system, and developing risk management strategies. DriveWealth has also considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities. Key members of the security and operational teams meet on at least an annual basis to identify and review risks to the system. The risk assessment identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Risk assessment policies and procedures also prompt personnel to identify and assess changes that could significantly impact the system of internal control as a part of the risk assessment process. The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management. The annual risk assessment identifies and assesses changes that could significantly impact the system of internal control.

Risk Factors

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

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities

- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

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

Potential for Fraud

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial reporting and related to various other business processes including misappropriation of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. The risk assessment policies and procedures address the need for identifying the potential for fraud as part of the risk assessment process. The formal risk assessment that is performed on an annual basis considers the potential for fraud.

Risk Mitigation

Risk mitigation activities include the ability to identify, select, and develop activities that sufficiently meet the identified risks. As noted in the risk management policy, once a risk has been identified, the mitigation is handled through one of the four types of mitigation strategies: terminate, tolerate, treat, or transfer. From a risk transfer perspective, the risk can be transferred through contract, insurance, or other methods identified by the organization. Each risk is owned by a member from DriveWealth based on the type of risk that is identified. The owner of the risk would manage and be responsible for the overall mitigation of the risk and is tracked and identified within the overall risk assessment. The responses to risks are carried out by each individual responsible for the risk, with the oversight of the risk officer within their business unit.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

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

Selection and Development of Control Activities

Selecting control activities includes consideration of the relevant business processes and identified risks that require control activities. Additionally, both automated and manual controls are considered during the selection of control activities. Management also considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.

Documented policies and procedures are in place to guide personnel in selecting and developing control activities, including control activities over technology to support the achievement of objectives and that contribute to the mitigation of risks to the achievement of objectives to acceptable levels as a part of the risk assessment process. Assigned risk owners select and develop control activities, including control activities over technology to support the achievement of objectives, to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.

Control activities are deployed through the use of policies to establish what is expected and procedures that put policies into action. Management has documented information security policies and procedures are in place to govern information security standards and Documented policies and procedures to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems. These policies and procedures are communicated to internal personnel via the intranet. Additionally, a data classification policy is formally documented and reviewed on an annual basis that identifies information required to support the functioning of internal control and achievement of objectives and associated protection, access rights, and retention requirements. Employees are held accountable for complying with these policies. Employee sanction procedures are in place that outline the consequences for noncompliance.

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

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability categories are applicable to the DriveWealth Platform system.

INFORMATION AND COMMUNICATION SYSTEMS

Pertinent information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial, and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to inform business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across, and up the organization. Personnel must receive a clear message from top management that control responsibilities must be taken seriously. Personnel must understand their own role in the internal control system, as well as how individual activities relate to the work of others. Personnel must also have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

Internal Communications

DriveWealth has implemented various methods of communication to help provide assurance that all employees understand their individual roles and responsibilities and that significant events are communicated. These methods include documented information security policies and procedures, security awareness training on an annual basis, documented position descriptions, and documented escalation procedures for reporting security and availability incidents, which are provided to internal users to guide them in identifying and reporting failures, incidents,

concerns, and other complaints. Policies and procedures are published on the company intranet and are accessible to DriveWealth employees.

External Communications

DriveWealth has also implemented various methods of external communication to help provide assurance that customers, vendors, and other external parties understand their roles and responsibilities and communication of significant events. Customer contracts are documented within service level agreements (SLAs), and NDAs are also in place to document the entity's security and availability commitments. In addition, vendor contracts are in place to document DriveWealth security and availability requirements and the associated system requirements. The DriveWealth website directs external users to links for communicating with support personnel should they need assistance, clarification, or to report a potential incident.

MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as customer complaints and regulatory comments that may indicate problems or highlight areas in need of improvement.

Ongoing Monitoring

By monitoring the risks and the effectiveness of control measures on a regular basis, DriveWealth can react dynamically to changing conditions. Logging and monitoring tools are configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization and alert the information security team upon detection of unusual system activity or service requests. In addition, an enterprise monitoring application is in place and configured to alert IT and operations personnel via e-mail when predefined thresholds are exceeded. Corrective actions are taken, as necessary.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and the importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often. A risk committee reviews internal controls on at least an annual basis to help ensure that controls and mitigating strategies selected are operating as intended. The risk committee meetings include discussions of enterprise-wide risks to the organization. During the meetings, the committee reviews various security metrics and reviews security controls to determine that they are functioning as intended. Functional heads of each department perform a department-level internal control self-assessment annually and the results of the self-assessments are reviewed as part of the risk assessment process which includes development of corrective action plans for control weaknesses identified. In addition, management personnel review critical vendors assessment reports on an annual basis and engage with a third-party vendor to perform a penetration test.

Subservice Organization Monitoring

Cloud hosting services provided by AWS are monitored on a regular basis as part of day-to-day business operations. DriveWealth management personnel obtain and review the applicable third-party attestation reports for AWS according to the established vendor management procedures.

Evaluating and Communicating Deficiencies

Management has developed protocols to help ensure findings of internal control deficiencies are reported to the individuals responsible for the function or activity involved and are in the position to take corrective action. This process enables responsible individuals to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Security committee meetings are held on a monthly basis to discuss ongoing objectives and their effect on the system. In addition, technology meetings are held on a weekly basis to discuss ongoing security initiatives and their effect on the system. The results of control assessments performed by external parties are provided to the board of directors on an annual basis.

System Incident Disclosures

No system incidents occurred during the period that were the result of controls that were not suitably designed or otherwise resulted in a significant failure of the achievement of one or more of the service commitments and systems requirements.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the DriveWealth Platform system provided by DriveWealth. The scope of the testing was restricted to the DriveWealth Platform system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period April 1, 2022, to March 31, 2023.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria, are presented in the “Subservice Organizations” section within Section 3.

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Background checks are performed for employees as a component of the hiring process.	Inspected the completed background checks for a sample of employees hired during the period to determine that background checks were performed for employees as a component of the hiring process for each employee sampled.	No exceptions noted.
CC1.1.2	A code of conduct is in place to communicate established workplace conduct standards, acceptable use, and conduct enforcement procedures to internal users.	Inspected the code of conduct to determine that a code of conduct was in place to communicate established workplace conduct standards, acceptable use, and conduct enforcement procedures to internal users.	No exceptions noted.
CC1.1.3	Employees are required to sign an employment agreement form upon hire indicating that they understand their responsibility for adhering to company policies.	Inquired of the CISO regarding the employment agreement form process to determine that employees were required to sign an employment agreement form upon hire indicating that they understood their responsibility for adhering to company policies.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the signed employment agreement form for a sample of employees hired during the period to determine that an employment agreement form was signed for each employee sampled.	No exceptions noted.
CC1.1.4	Employees are required to sign an NDA upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inquired of the CISO regarding the NDA process to determine that employees were required to sign an NDA upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
		Inspected the signed NDA for a sample of employees hired during the period to determine that an NDA was signed for each employee sampled.	No exceptions noted.
CC1.1.5	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.	Inspected the compliance policies and employment agreement form to determine that policies were documented and maintained that addressed remedial actions for lack of compliance with policies and procedures.	No exceptions noted.
CC1.1.6	Vendors are required to sign an agreement about their requirements to adhere to certain commitments and requirements as they pertain to security.	Inspected the signed NDA for an example new vendor to determine that vendors were required to sign an agreement about their requirements to adhere to certain commitments and requirements as they pertained to security.	No exceptions noted.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The board of directors establishes and maintains a formal charter and set of bylaws which describe their responsibilities and oversight of management's system of internal control.	Inspected the board of directors' bylaws to determine that the board of directors established and maintained a formal charter and set of bylaws which described their responsibilities and oversight of management's system of internal control.	No exceptions noted.
CC1.2.2	The board of directors has members who are, by majority, independent from management and are objective in evaluations and decision making.	Inquired of the CISO regarding the board of directors to determine that the board of directors had members who were, by majority, independent from management and were objective in evaluations and decision making.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the board of directors' member list to determine that the board of directors had members who were, by majority, independent from management and were objective in evaluations and decision making.	No exceptions noted.
CC1.2.3	Strategic plans are established by the board of directors to help guide management personnel in achieving organizational objectives and to establish performance measures for management personnel to be evaluated against on at least an annual basis.	Inquired of the CISO regarding strategic plans to determine that strategic plans were established by the board of directors to help guide management personnel in achieving organizational objectives and to establish performance measures for management personnel to be evaluated against on at least an annual basis.	No exceptions noted.
		Inspected the most recent strategic plans to determine that strategic plans were established by the board of directors to help guide management personnel in achieving organizational objectives and established performance measures for management personnel to be evaluated against during the period.	No exceptions noted.
CC1.2.4	Management provides the results of control assessment reports to the board of directors on at least an annual basis.	Inquired of the CISO regarding external assessment reports to determine that management provided the results of control assessment reports to the board of directors on at least an annual basis.	No exceptions noted.
		Inspected the most recent control assessment report presentation to the board of directors to determine that management provided the results of control assessment reports to the board of directors during the period.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Organizational charts are communicated to define key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system.	Inquired of the CISO regarding the organizational structure to determine that organizational charts were communicated to define key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the organizational charts and the corporate intranet to determine that organizational charts were communicated to define key areas of authority, responsibility, and lines of reporting to personnel related to the design, development, implementation, operation, maintenance, and monitoring of the system.	No exceptions noted.
CC1.3.2	Documented employment position descriptions are in place to define the skills, responsibilities, and knowledge levels required for jobs.	Inspected the documented employment position descriptions for a sample of employment positions to determine that documented employment position descriptions were in place to define the skills, responsibilities, and knowledge levels required for jobs for each employment position sampled.	No exceptions noted.
CC1.3.3	The board of directors establishes and maintains a formal charter and set of bylaws which describe their responsibilities and oversight of management's system of internal control.	Inspected the board of directors' bylaws to determine that the board of directors established and maintained a formal charter and set of bylaws which described their responsibilities and oversight of management's system of internal control.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Onboarding procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the onboarding procedures to determine that onboarding procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
CC1.4.2	Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training documentation and evidence of security awareness training completion for a sample of employees hired during the period to determine that security awareness training was completed upon hire for each newly hired employee sampled.	No exceptions noted.
		Inspected the security awareness training documentation and evidence of security awareness training completion for a sample of current employees to determine that security awareness training was completed during the period for each current employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.3	Employee performance reviews are conducted by management personnel on an annual basis to evaluate the performance of employees against expected levels of performance and conduct.	Inspected the performance review documentation for a sample of current employees to determine that employee performance reviews were conducted by management personnel during the period to evaluate the performance of employees against expected levels of performance and conduct for each current employee sampled.	No exceptions noted.
CC1.4.4	A formal training budget is available to new and existing employees to help maintain and advance the skill level of personnel.	Inspected the professional development policy to determine that a formal training budget was available to new and existing employees to help maintain and advance the skill level of personnel.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Documented employment position descriptions are in place to define the skills, responsibilities, and knowledge levels required for jobs.	Inspected the documented employment position descriptions for a sample of employment positions to determine that documented employment position descriptions were in place to define the skills, responsibilities, and knowledge levels required for jobs for each employment position sampled.	No exceptions noted.
CC1.5.2	Employees are required to sign an employment agreement form upon hire indicating that they understand their responsibility for adhering to company policies.	Inquired of the CISO regarding the employment agreement form process to determine that employees were required to sign an employment agreement form upon hire indicating that they understood their responsibility for adhering to company policies.	No exceptions noted.
		Inspected the signed employment agreement form for a sample of employees hired during the period to determine that an employment agreement form was signed for each employee sampled.	No exceptions noted.
CC1.5.3	A code of conduct is in place to communicate established workplace conduct standards, acceptable use, and conduct enforcement procedures to internal users.	Inspected the code of conduct to determine that a code of conduct was in place to communicate established workplace conduct standards, acceptable use, and conduct enforcement procedures to internal users.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.4	Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training documentation and evidence of security awareness training completion for a sample of employees hired during the period to determine that security awareness training was completed upon hire for each newly hired employee sampled.	No exceptions noted.
		Inspected the security awareness training documentation and evidence of security awareness training completion for a sample of current employees to determine that security awareness training was completed during the period for each current employee sampled.	No exceptions noted.
CC1.5.5	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.	Inspected the compliance policies and employment agreement form to determine that policies were documented and maintained that addressed remedial actions for lack of compliance with policies and procedures.	No exceptions noted.
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Policies and procedures are documented and communicated to govern information security standards and identify information required to support the functioning of internal control.	Inspected the information security policies and procedures and evidence of communication to determine that policies and procedures were documented and communicated to govern information security standards and identify information required to support the functioning of internal control.	No exceptions noted.
CC2.1.2	Logging and monitoring software are configured to collect data from system infrastructure components to monitor system performance, potential security anomalies / vulnerabilities, and resource utilization and alert the IT team upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations, alert notification configurations, and an example alert generated during the period to determine that logging and monitoring software were configured to collect data from system infrastructure components to monitor system performance, potential security anomalies / vulnerabilities, and resource utilization and alert the IT team upon detection of unusual system activity or service requests.	No exceptions noted.
CC2.1.3	Internal vulnerability scans are configured to run daily.	Inquired of the CISO to determine that internal vulnerability scans were configured to run daily.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the internal vulnerability configuration and example vulnerability report to determine that internal vulnerability scans were configured to run daily.	No exceptions noted.
CC2.1.4	A third-party vendor is utilized to perform penetration tests on an annual basis. Any security vulnerabilities that are detected are reviewed by the vulnerability management team and monitored through resolution.	Inquired of the director of governance, risk & compliance regarding penetration testing to determine that a third-party vendor was utilized to perform penetration tests on an annual basis, and that any security vulnerabilities that were detected were triaged by the vulnerability management team and monitored through resolution.	No exceptions noted.
		Inspected the most recent penetration test performed and corresponding triaged tickets to determine that a third-party vendor was utilized to perform penetration tests and any security vulnerabilities that were detected were reviewed by the vulnerability management team and monitored through resolution during the period.	No exceptions noted.
CC2.1.5	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of the CISO regarding the monitoring of emerging technologies and the impact of changes to applicable laws or regulations to determine that the entity's IT security group monitored the security impact of emerging technologies and that the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected example security updates and notifications generated during the period to determine that the entity's IT security group monitored the security impact of emerging technologies.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Policies and procedures are documented and communicated to personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	Inspected the document repository and relevant policies and procedures to determine that policies and procedures were documented and communicated to personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.2	Employees are required to sign an employment agreement form upon hire indicating that they understand their responsibility for adhering to company policies.	Inquired of the CISO regarding the employment agreement form process to determine that employees were required to sign an employment agreement form upon hire indicating that they understood their responsibility for adhering to company policies.	No exceptions noted.
		Inspected the signed employment agreement form for a sample of employees hired during the period to determine that an employment agreement form was signed for each employee sampled.	No exceptions noted.
CC2.2.3	Documented employment position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the documented employment position descriptions for a sample of employment positions to determine that documented employment position descriptions were in place to define the skills, responsibilities, and knowledge levels required for jobs for each employment position sampled.	No exceptions noted.
CC2.2.4	Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training documentation and evidence of security awareness training completion for a sample of employees hired during the period to determine that security awareness training was completed upon hire for each newly hired employee sampled.	No exceptions noted.
		Inspected the security awareness training documentation and evidence of security awareness training completion for a sample of current employees to determine that security awareness training was completed during the period for each current employee sampled.	No exceptions noted.
CC2.2.5	Strategic plans are established by the board of directors to help guide management personnel in achieving organizational objectives and to establish performance measures for management personnel to be evaluated against on at least an annual basis.	Inquired of the CISO regarding strategic plans to determine that strategic plans were established by the board of directors to help guide management personnel in achieving organizational objectives and to establish performance measures for management personnel to be evaluated against on at least an annual basis.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent strategic plans to determine that strategic plans were established by the board of directors to help guide management personnel in achieving organizational objectives and established performance measures for management personnel to be evaluated against during the period.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Information regarding the design and operation of the system and its boundaries is communicated to external users via the company website.	Inspected the product description via the DriveWealth external website to determine that information regarding the design and operation of the system and its boundaries was communicated to external users via the company website.	No exceptions noted.
CC2.3.2	The entity's security and availability commitments and the associated system requirements are documented and communicated to external parties in SLAs and NDAs.	Inspected the SLA and NDA templates to determine that the entity's security and availability commitments and the associated system requirements were documented and communicated to external parties in SLAs and NDAs.	No exceptions noted.
CC2.3.3	Vendors are required to sign an agreement about their requirements to adhere to certain commitments and requirements as they pertain to security.	Inspected the signed NDA for an example new vendor to determine that vendors were required to sign an agreement about their requirements to adhere to certain commitments and requirements as they pertained to security.	No exceptions noted.
CC2.3.4	A support portal is accessible by external users to report security incidents, concerns, and complaints.	Inspected the external support portal to determine that a support portal was accessible by external users to report security incidents, concerns, and complaints.	No exceptions noted.
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Management formally documents an organization strategy and performance policy and updates it on an annual basis to align internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the most recently updated organization strategy and performance policy to determine that management formally documented an organization strategy and performance policy to align internal control responsibilities, performance measures, and incentives with company business objectives during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.2	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC3.2.2	Security stakeholders perform a risk assessment on an annual basis that identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. Identified risks are formally documented, along with mitigation strategies, for management review.	Inquired of the risk management director regarding the risk assessment process to determine that the risk assessment identified risks to the achievement of its objectives across the entity and analyzed risks as a basis for determining how the risks should be managed and that identified risks were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
		Inspected the results of the most recent risk assessment documentation to determine that security stakeholders performed a risk assessment that identified risks to the achievement of its objectives across the entity and analyzed risks as a basis for determining how the risks should be managed and that identified risks were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Documented policies and procedures are in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.3.2	Security stakeholders perform a risk assessment on an annual basis that considers the potential for fraud.	Inspected the results of the most recent risk assessment documentation to determine that security stakeholders performed a risk assessment that considered the potential for fraud during the period.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Documented policies and procedures are in place to guide personnel in identifying and assessing changes that could significantly impact the system of internal control as a part of the risk assessment process.	Inspected the risk management policy to determine that documented policies and procedures were in place to guide personnel in identifying and assessing changes that could significantly impact the system of internal control as a part of the risk assessment process.	No exceptions noted.
CC3.4.2	Security stakeholders perform a risk assessment on an annual basis that considers the impact of changes to the system. Risks that are identified are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the results of the most recent risk assessment documentation to determine that security stakeholders performed a risk assessment that considered the impact of changes to the system and risks that were identified were rated using a risk evaluation process that accounted for changes in risk from the prior year, and were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC3.4.3	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of the CISO regarding the monitoring of emerging technologies and the impact of changes to applicable laws or regulations to determine that the entity's IT security group monitored the security impact of emerging technologies and that the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected example security updates and notifications generated during the period to determine that the entity's IT security group monitored the security impact of emerging technologies.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The risk committee reviews internal controls on at least an annual basis to help ensure that controls and mitigation strategies selected are operating as intended.	Inquired of the CISO regarding an internal control review to determine that the risk committee reviewed internal controls on at least an annual basis to help ensure that controls and mitigation strategies selected were operating as intended.	No exceptions noted.
		Inspected the most recent risk committee meeting invite and meeting minutes to determine that the risk committee reviewed internal controls and that mitigation strategies selected were operating as intended during the period.	No exceptions noted.
CC4.1.2	Functional heads of each department perform an internal control self-assessment on an annual basis. The results of the self-assessments are reviewed as part of the risk assessment and require the development of corrective action plans for control weaknesses identified.	Inquired of the CISO regarding control self-assessments to determine that functional heads of each department performed an internal control self-assessment on an annual basis and the results of the self-assessments were reviewed as part of the risk assessment and require the development of corrective action plans for control weaknesses identified.	No exceptions noted.
		Inspected the results of the most recent annual self-assessments to determine that functional heads of each department performed an internal control self-assessment, and the results of the self-assessments were reviewed as part of the risk assessment and required the development of corrective action plans for control weaknesses identified during the period.	No exceptions noted.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	The risk committee reviews internal controls on at least an annual basis to help ensure that controls and mitigation strategies selected are operating as intended.	Inquired of the CISO regarding an internal control review to determine that the risk committee reviewed internal controls on at least an annual basis to help ensure that controls and mitigation strategies selected were operating as intended.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent risk committee meeting invite and meeting minutes to determine that the risk committee reviewed internal controls and that mitigation strategies selected were operating as intended during the period.	No exceptions noted.
CC4.2.2	Functional heads of each department perform an internal control self-assessment on an annual basis. The results of the self-assessments are reviewed as part of the risk assessment and require the development of corrective action plans for control weaknesses identified.	Inquired of the CISO regarding control self-assessments to determine that functional heads of each department performed an internal control self-assessment on an annual basis and the results of the self-assessments were reviewed as part of the risk assessment and require the development of corrective action plans for control weaknesses identified.	No exceptions noted.
		Inspected the results of the most recent annual self-assessments to determine that functional heads of each department performed an internal control self-assessment, and the results of the self-assessments were reviewed as part of the risk assessment and required the development of corrective action plans for control weaknesses identified during the period.	No exceptions noted.
CC4.2.3	Technology meetings are held on a weekly basis to discuss ongoing security initiatives and their effect on the system.	Inquired of the CISO regarding technology meetings to determine that technology meetings were held on a weekly basis to discuss ongoing security initiatives and their effect on the system.	No exceptions noted.
		Inspected the technology meeting standing invitation to determine that weekly technology meetings were scheduled to be held during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	Security stakeholders perform a risk assessment on an annual basis that includes an analysis of risk mitigation control activities. The analysis considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.	Inspected the results of the most recent risk assessment documentation to determine that security stakeholders performed a risk assessment that included an analysis of risk mitigation control activities and that the analysis considered how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affected the selection and development of control activities during the period.	No exceptions noted.
CC5.1.2	Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inquired of the CISO regarding control activities to determine that assigned risk owners selected and developed control activities to mitigate the risks identified during the annual risk assessment process and that control activities were documented within the mitigation plans that were created by risk owners above the tolerable threshold.	No exceptions noted.
		Inspected the most recently completed risk assessment documentation and risk mitigation plans to determine that assigned risk owners selected and developed control activities within the mitigation plans that were created by the risk owners for risks above the tolerable threshold during the period.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inquired of the CISO regarding control activities to determine that assigned risk owners selected and developed control activities to mitigate the risks identified during the annual risk assessment process and that control activities were documented within the mitigation plans that were created by risk owners above the tolerable threshold.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recently completed risk assessment and risk mitigation plans to determine that assigned risk owners selected and developed control activities within the mitigation plans that were created by the risk owners for risks above the tolerable threshold during the period.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Documented policies and procedures are in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of the in-scope systems.	Inspected the maintenance and operations procedures and the information security policy to determine that documented policies and procedures were in place to guide personnel in the design, development, implementation, operation, maintenance, and monitoring of in-scope systems.	No exceptions noted.
CC5.3.2	Policies are documented and maintained that address remedial actions for lack of compliance with policies and procedures.	Inspected the compliance policies and employment agreement form to determine that policies were documented and maintained that addressed remedial actions for lack of compliance with policies and procedures.	No exceptions noted.
Logical and Physical Access Controls			
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.			
CC6.1.1	The cloud operations team has formally documented standard build procedures for installation and maintenance of production servers.	Inspected the server build procedures to determine that the cloud operations team had formally documented standard build procedures for installation and maintenance of production servers.	No exceptions noted.
CC6.1.2	The in-scope systems are configured to require at least one of the following authentication mechanisms before granting users access to the systems: <ul style="list-style-type: none"> Authorized user account and password Two-factor authentication SSH authentication 	Inspected the authentication configurations for the IdP platform to determine that the IdP platform was configured to require an authorized user account and password and two-factor authentication before granting users access to the system.	No exceptions noted.
		Inspected the authentication configurations for the AWS management console to determine that AWS was configured to require an authorized user account and password and two-factor authentication before granting users access to the system.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the production server authentication configurations for a sample of production servers to determine that the servers were configured to require users to authenticate via an SSH private key before granting users access to the system for each server sampled.	No exceptions noted.
		Inspected the database authentication configurations for a sample of production databases to determine that the database was configured to require an authorized user account and password before granting users access to the system for each database sampled.	No exceptions noted.
		Inspected the DriveWealth application authentication configurations to determine that the application was configured to require an authorized user account and password before granting users access to the system.	No exceptions noted.
		Inspected the VPN authentication configurations to determine that the VPN was configured to require users to authenticate to the production environment via a unique user account and password before granting users access to the system.	No exceptions noted.
CC6.1.3	Administrative and privileged access to the in-scope systems is restricted to user accounts accessible by authorized personnel.	Inspected the IdP platform administrator access listing with the assistance of the head of technology to determine that administrative and privileged access to the IdP platform was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the AWS administrator access listing with the assistance of the head of technology to determine that administrative and privileged access to AWS was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the production server administrator access listings for a sample of production servers with the assistance of the head of technology to determine that administrative and privileged access to the server was restricted to user accounts accessible by authorized personnel for each server sampled.	No exceptions noted.
		Inspected the database administrator access listings for a sample of databases with the assistance of the head of technology to determine that administrative and privileged access to the database was restricted to user accounts accessible by authorized personnel for each database sampled.	No exceptions noted.
		Inspected the application administrator access listing with the assistance of the CISO to determine that administrative and privileged access to the application was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the VPN administrator access listing with the assistance of the head of technology to determine that administrative and privileged access to the VPN was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
	AWS is responsible for managing and monitoring logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the DriveWealth systems reside.		
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Employee access requests are documented in the ticketing system and require department manager approval prior to access being granted.	Inquired of the head of technology regarding access provisioning to determine that employee access requests were documented in the ticketing system and required department manager approval prior to access being granted.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the access request tickets for a sample of user access requests during the period to determine that employee access requests were documented in the ticketing system and department manager approval was obtained for each access request sampled.	No exceptions noted.
CC6.2.2	Termination tickets are completed, and system access is revoked for employees as a component of the employee termination process on the date of termination.	Inquired of the CISO regarding the termination process to determine that termination tickets were completed, and system access was revoked for employees as a component of the employee termination process on the date of termination.	No exceptions noted.
		Inspected the termination ticket for a sample of employees terminated during the period to determine that termination tickets were completed as a component of the employee termination process for each employee sampled.	The test of the control activity disclosed that termination tickets were not completed for 10 of 25 terminated employees sampled.
		Inspected the system access listings for a sample of employees terminated during the period and for a sample of in-scope systems to determine that system access was revoked as a component of the employee termination process for each employee and system sampled.	No exceptions noted.
CC6.2.3	IT personnel perform a user access review of AWS user accounts, including administrative and privileged users, on an annual basis.	Inspected evidence of the most recent cloud network user account access review to determine that IT personnel performed a user access review of AWS user accounts, including administrative and privileged users, during the period.	No exceptions noted.
AWS is responsible for managing and monitoring logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the DriveWealth systems reside.			
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	Employee access requests are documented in the ticketing system and require department manager approval prior to access being granted.	Inquired of the head of technology regarding access provisioning to determine that employee access requests were documented in the ticketing system and required department manager approval prior to access being granted.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the access request tickets for a sample of user access requests during the period to determine that employee access requests were documented in the ticketing system and department manager approval was obtained for each access request sampled.	No exceptions noted.
CC6.3.2	Termination tickets are completed, and system access is revoked for employees as a component of the employee termination process on the date of termination.	Inquired of the CISO regarding the termination process to determine that termination tickets were completed, and system access was revoked for employees as a component of the employee termination process on the date of termination.	No exceptions noted.
		Inspected the termination ticket for a sample of employees terminated during the period to determine that termination tickets were completed as a component of the employee termination process for each employee sampled.	Refer to the test results for control activity CC6.2.2.
		Inspected the system access listings for a sample of employees terminated during the period and for a sample of in-scope systems to determine that system access was revoked as a component of the employee termination process for each employee and system sampled.	No exceptions noted.
CC6.3.3	IT personnel perform a user access review of AWS user accounts, including administrative and privileged users, on an annual basis.	Inspected evidence of the most recent cloud network user account access review to determine that IT personnel performed a user access review of AWS user accounts, including administrative and privileged users, during the period.	No exceptions noted.
CC6.3.4	Administrative and privileged access to the in-scope systems is restricted to user accounts accessible by authorized personnel.	Inspected the IdP platform administrator access listing with the assistance of the head of technology to determine that administrative and privileged access to the IdP platform was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the AWS administrator access listing with the assistance of the head of technology to determine that administrative and privileged access to AWS was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the production server administrator access listings for a sample of production servers with the assistance of the head of technology to determine that administrative and privileged access to the server was restricted to user accounts accessible by authorized personnel for each server sampled.	No exceptions noted.
		Inspected the database administrator access listings for a sample of databases with the assistance of the head of technology to determine that administrative and privileged access to the database was restricted to user accounts accessible by authorized personnel for each database sampled.	No exceptions noted.
		Inspected the application administrator access listing with the assistance of the CISO to determine that administrative and privileged access to the application was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Inspected the VPN administrator access listing with the assistance of the head of technology to determine that administrative and privileged access to the VPN was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.3.5	Predefined security groups are utilized to assign role-based access privileges and segregate access to data on the production environment.	Inspected the security group configurations to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data on the production environment.	No exceptions noted.
	AWS is responsible for managing and monitoring logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the DriveWealth systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
	AWS is responsible for restricting and monitoring physical access to data center facilities underlying network, virtualization management, and storage devices where the DriveWealth applications reside.		
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Documented policies and procedures are in place that require the destruction of confidential data and disposal of assets.	Inspected the media handling and disposal procedures to determine that documented policies and procedures were in place that required the destruction of confidential data and disposal of assets.	No exceptions noted.
	AWS is responsible for managing and monitoring logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the DriveWealth systems reside.		
	AWS is responsible for restricting and monitoring physical access to data center facilities underlying network, virtualization management, and storage devices where the DriveWealth applications reside.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Security groups are in place to filter unauthorized inbound network traffic from the internet and configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Inquired of the CISO regarding firewall rulesets to determine that security groups were in place to filter unauthorized inbound network traffic from the internet and configured to deny any type of network connection that was not explicitly authorized by a firewall rule.	No exceptions noted.
		Inspected the security group configurations and rulesets to determine that security groups were in place to filter unauthorized inbound network traffic from the internet and configured to deny any type of network connection that was not explicitly authorized by a firewall rule.	No exceptions noted.
CC6.6.2	A WAF is in place to block and monitor web requests and prevent web attacks.	Inspected the WAF configurations to determine that a WAF was in place to block and monitor web requests and prevent web attacks.	No exceptions noted.
CC6.6.3	Logging and monitoring software are configured to collect data from system infrastructure components to monitor system performance, potential security anomalies / vulnerabilities, and resource utilization and alert the IT team upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations, alert notification configurations, and an example alert generated during the period to determine that logging and monitoring software were configured to collect data from system infrastructure components to monitor system performance, potential security anomalies / vulnerabilities, and resource utilization and alert the IT team upon detection of unusual system activity or service requests.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.4	Web communication sessions are secured via TLS encryption.	Inspected the web server TLS certificate to determine that web communication sessions were secured via TLS encryption.	No exceptions noted.
AWS is responsible for managing and monitoring logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the DriveWealth systems reside.			
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Client data is stored in an encrypted format in the database at rest.	Inspected evidence of database encryption at rest for an example database to determine that client data was stored in an encrypted format in the database at rest.	No exceptions noted.
CC6.7.2	Access to the cryptographic keys for client data is restricted to authorized personnel.	Inspected the listing of users with access to cryptographic keys with the assistance of the head of technology to determine that access to the cryptographic keys was restricted to authorized personnel.	No exceptions noted.
CC6.7.3	Web communication sessions are secured via TLS encryption.	Inspected the web server TLS certificate to determine that web communication sessions were secured via TLS encryption.	No exceptions noted.
CC6.7.4	An encrypted VPN is required for remote access to the production systems to help ensure the security and integrity of the data passing over the public network.	Inspected the VPN tunneling encryption configurations to determine that an encrypted VPN was required for remote access to the production systems to help ensure the security and integrity of the data passing over the public network.	No exceptions noted.
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where DriveWealth systems reside.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Employees are required to complete security awareness training upon hire, and on an annual basis thereafter, to understand their obligations and responsibilities to comply with the corporate and business unit security policies.	Inspected the security awareness training documentation and evidence of security awareness training completion for a sample of employees hired during the period to determine that security awareness training was completed upon hire for each newly hired employee sampled.	No exceptions noted.
		Inspected the security awareness training documentation and evidence of security awareness training completion for a sample of current employees to determine that security awareness training was completed during the period for each current employee sampled.	No exceptions noted.
CC6.8.2	The ability to implement application and infrastructure changes is restricted to user accounts accessible by authorized personnel.	Inspected the deployment management tool user access listings with the assistance of the head of technology to determine that the ability to implement application and infrastructure changes was restricted to user accounts accessibly by authorized personnel.	No exceptions noted.
CC6.8.3	A file integrity monitoring tool is in place to monitor for production system changes.	Inquired of the CISO regarding file integrity monitoring to determine that a file integrity monitoring tool was in place to monitor for production system changes.	No exceptions noted.
		Inspected the file integrity monitoring configurations to determine that a file integrity monitoring tool was in place to monitor for production system changes.	No exceptions noted.
CC6.8.4	A cloud native tool is utilized to continuously monitor for malicious activity and unauthorized behavior in the production environment and alert management regarding potential malicious activity.	Inspected the cloud native monitoring tool dashboard, alerting configurations, and example alert to determine that a cloud native tool was utilized to continuously monitor for malicious activity and unauthorized behavior in the production environment and alert management regarding potential malicious activity.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
System Operations			
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.			
CC7.1.1	The cloud operations team has formally documented standard build procedures for installation and maintenance of production servers.	Inspected the server build to determine that the cloud operations team had formally documented standard build procedures for installation and maintenance of production servers.	No exceptions noted.
CC7.1.2	Logging and monitoring software are configured to collect data from system infrastructure components to monitor system performance, potential security anomalies / vulnerabilities, and resource utilization and alert the IT team upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations, alert notification configurations, and an example alert generated during the period to determine that logging and monitoring software were configured to collect data from system infrastructure components to monitor system performance, potential security anomalies / vulnerabilities, and resource utilization and alert the IT team upon detection of unusual system activity or service requests.	No exceptions noted.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Documented logging and monitoring policies are in place to guide personnel in security monitoring practices.	Inspected the logging and monitoring policies to determine that documented logging and monitoring policies were in place to guide personnel in security monitoring practices.	No exceptions noted.
CC7.2.2	Logging and monitoring software are configured to collect data from system infrastructure components to monitor system performance, potential security anomalies / vulnerabilities, and resource utilization and alert the IT team upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations, alert notification configurations, and an example alert generated during the period to determine that logging and monitoring software were configured to collect data from system infrastructure components to monitor system performance, potential security anomalies / vulnerabilities, and resource utilization and alert the IT team upon detection of unusual system activity or service requests.	No exceptions noted.
AWS is responsible for managing and monitoring logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the DriveWealth systems reside.			
AWS is responsible for restricting and monitoring physical access to data center facilities underlying network, virtualization management, and storage devices where the DriveWealth applications reside.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Incident response plan and escalation policies outline the response to security events and includes lessons learned to evaluate the effectiveness of the policies.	Inspected the incident response plan and escalation policies to determine that incident response policies outlined the response to security events and included lessons learned to evaluate the effectiveness of the policies.	No exceptions noted.
CC7.3.2	A ticketing system is utilized to document system incidents, response, and resolution.	Inspected an example security and availability incident resolved during the period to determine that a ticketing system was utilized to manage system incidents, response, and resolution.	No exceptions noted.
CC7.3.3	Technology meetings are held on a weekly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.	Inquired of the CISO regarding technology meetings to determine that technology meetings were held on a weekly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.	No exceptions noted.
		Inspected the technology meeting standing invitation to determine that weekly technology meetings were scheduled to be held on a weekly basis during the period.	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Incident response policies outline the process for responding to security events which includes steps on how to understand, contain, remediate, and communicate security incidents and includes lessons learned to evaluate the effectiveness of the policies.	Inspected the incident response plan and escalation policies to determine that incident response policies outlined the process for responding to security events which included steps on how to understand, contain, remediate, and communicate security incidents including the lessons learned to evaluate the effectiveness of the policies.	No exceptions noted.
CC7.4.2	A ticketing system is utilized to document system incidents, response, and resolution.	Inspected an example security and availability incident resolved during the period to determine that a ticketing system was utilized to manage system incidents, response, and resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Incident response policies outline the procedures for responding to security events and includes lessons learned to evaluate the effectiveness of the procedures and discusses activities to recover from identified security incidents.	Inspected the incident response plan and escalation policies to determine that incident response policies outlined the procedures for responding to security events including the lessons learned to evaluate the effectiveness of the procedures and discussed activities to recover from identified security incidents.	No exceptions noted.
CC7.5.2	A ticketing system is utilized to document system incidents, response, and resolution.	Inspected an example security and availability incident resolved during the period to determine that a ticketing system was utilized to manage system incidents, response, and resolution.	No exceptions noted.
CC7.5.3	Technology meetings are held on a weekly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.	Inquired of the CISO regarding technology meetings to determine that technology meetings were held on a weekly basis to discuss the effect of identified security vulnerabilities on the ability to meet business objectives and to identify corrective measures.	No exceptions noted.
		Inspected the technology meeting standing invitation to determine that weekly technology meetings were scheduled to be held for each week sampled.	No exceptions noted.
Change Management			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Documented change management policies and procedures are in place to guide personnel in the systems development and infrastructure change management process.	Inspected the change management policies and procedures to determine that documented change management policies and procedures were in place to guide personnel in the systems development and infrastructure change management processes.	No exceptions noted.
CC8.1.2	A ticketing system is utilized to centrally maintain, manage, and monitor enhancement, development, and maintenance activities.	Inspected the ticketing system dashboard and change request tickets for a sample of application and infrastructure changes implemented during the period to determine that a ticketing system was utilized to centrally maintain, manage, and monitor enhancement, development and maintenance activities for each change sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.3	Change management meetings are held on a weekly basis to review the status of new and pending production application and infrastructure changes.	Inquired of the head of technology regarding the change management process to determine that change management meetings were held on a weekly basis to review the status of new and pending production application and infrastructure changes.	No exceptions noted.
		Inspected the change management meeting invite from during the period to determine that change management meetings were scheduled to be held on a weekly basis during the period.	No exceptions noted.
CC8.1.4	Development personnel perform development and testing efforts in environments that are logically separate from the production environment.	Inspected the URLs for the development, test, and production environments to determine that development personnel performed development and testing efforts in environments that were logically separate from the production environment.	No exceptions noted.
CC8.1.5	A development platform is in place to control access to source code libraries and programs.	Inspected the development platform configurations and example activity logs generated during the period to determine that a development platform was in place to control access to source code libraries and programs.	No exceptions noted.
CC8.1.6	Changes to source code result in the creation of a new version of code. The development platform provides rollback capabilities in the event code needs to be restored to a previous version.	Inquired of the head of technology regarding the development platform to determine that changes to source code resulted in the creation of a new version of code and that the development platform provided rollback capabilities in the event code needed to be restored to a previous version.	No exceptions noted.
		Inspected the development platform configurations and example logs generated during the period to determine that changes to source code resulted in the creation of a new version of code and that the development platform provided rollback capabilities in the event code needed to be restored to a previous version.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.7	Write access to application and infrastructure source code is restricted to user accounts accessible by authorized personnel.	Inspected the development platform user access listing with the assistance of the head of technology to determine that write access to application and infrastructure source code was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.8	Administrator access to the development platform is restricted to user accounts accessible by authorized personnel.	Inspected the development platform administrator access listing with the assistance of the head of technology to determine that administrator access to the development platform was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.9	Engineering personnel review, test, and approve application and infrastructure changes prior to implementation.	Inquired of the head of technology regarding the change management process to determine that engineering personnel reviewed, tested, and approved application and infrastructure changes prior to implementation.	No exceptions noted.
		Inspected the testing and approval documentation for a sample of application and infrastructure changes implemented during the period to determine that engineering personnel reviewed, tested, and approved each application and infrastructure change sampled.	No exceptions noted.
CC8.1.10	The ability to implement application and infrastructure changes is restricted to user accounts accessible by authorized personnel.	Inspected the deployment management tool user access listings with the assistance of the head of technology to determine that the ability to implement application and infrastructure changes was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.11	A file integrity monitoring tool is in place to monitor for production system changes.	Inquired of the CISO regarding file integrity monitoring to determine that a file integrity monitoring tool was in place to monitor for production system changes.	No exceptions noted.
		Inspected the file integrity monitoring configurations to determine that a file integrity monitoring tool was in place to monitor for production system changes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented policies and procedures are in place to guide personnel in identifying, selecting, and developing risk management strategies to address the risks arising from potential business disruptions as a part of the risk assessment process.	Inspected the information security risk management policy to determine that documented policies and procedures were in place to guide personnel in identifying, selecting, and developing risk management strategies to address the risks arising from potential business disruptions as a part of the risk assessment process.	No exceptions noted.
CC9.1.2	Security stakeholders perform a risk assessment on an annual basis that identifies risks related to potential business disruptions across the entity and analyzes risks as a basis for determining how the risks should be managed. Identified risks are formally documented, along with mitigation strategies, for management review.	Inspected the results of the most recent risk assessment documentation to determine that security stakeholders performed a risk assessment that identified risks related to potential business disruptions across the entity and analyzed risks as a basis for determining how the risks should be managed and identified risks were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.
CC9.1.3	A business continuity plan is in place to guide personnel in procedures to restore critical operations following an unplanned business disruption.	Inspected the business continuity plan to determine that a business continuity plan was in place to guide personnel in procedures to restore critical operations following an unplanned business disruption.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Vendor management policies and procedures are in place to guide personnel in assessing and managing risks associated with third parties.	Inspected the vendor management policies and procedures to determine that vendor management policies and procedures were in place to guide personnel in assessing and managing risks associated with third parties.	No exceptions noted.
CC9.2.2	Vendors are required to sign an agreement about their requirements to adhere to certain commitments and requirements as they pertain to security.	Inspected the signed NDA for an example new vendor to determine that vendors were required to sign an agreement about their requirements to adhere to certain commitments and requirements as they pertained to security.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.3	Critical vendors are monitored and reviewed on at least an annual basis to help ensure that third-party vendors follow the organization's requirements.	Inspected evidence of vendor reviews for a sample of critical vendors to determine that critical vendors were monitored and reviewed to help ensure that third-party vendors followed the organization's requirements during the period for each critical vendor sampled.	No exceptions noted.
CC9.2.4	Security stakeholders perform a risk assessment on an annual basis that identifies, selects, and develops risk mitigation activities for risks associated with vendors and business partners. Identified risks are formally documented, along with mitigation strategies, for management review.	Inspected the results of the most recent risk assessment documentation to determine that security stakeholders performed a risk assessment that identified, selected, and developed risk mitigation activities for risks associated with vendors and business partners and identified risks were formally documented, along with mitigation strategies, for management review during the period.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Documented policies and procedures are in place to guide personnel in performing production system availability and monitoring activities.	Inspected the technology operating procedures to determine that documented policies and procedures were in place to guide personnel in performing production system availability and monitoring activities.	No exceptions noted.
A1.1.2	Logging and monitoring software are configured to collect data from system infrastructure components to monitor system performance, potential security anomalies / vulnerabilities, and resource utilization and alert the IT team upon detection of unusual system activity or service requests.	Inspected the logging and monitoring software configurations, alert notification configurations, and an example alert generated during the period to determine that logging and monitoring software were configured to collect data from system infrastructure components to monitor system performance, potential security anomalies / vulnerabilities, and resource utilization and alert the IT team upon detection of unusual system activity or service requests.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1.3	Redundancy of infrastructure components is built into the architecture to help mitigate the risk of production system availability issues.	Inspected the failover and redundancy configurations to determine that redundancy of infrastructure components was built into the architecture to help mitigate the risk of production system availability issues.	No exceptions noted.
A1.1.4	A ticketing system is utilized to document and manage system incidents, response, and resolution.	Inspected an example security and availability incident resolved during the period to determine that a ticketing system was utilized to document and manage system incidents, response, and resolution.	No exceptions noted.
A1.1.5	Operations team meetings are held on a weekly basis to discuss availability incidents and review availability trends and forecasts as compared to system commitments.	Inquired of the CISO regarding availability meetings to determine that operations team meetings were held to discuss availability incidents and review availability trends and forecasts as compared to system commitments.	No exceptions noted.
		Inspected the operations team meeting standing invitations and meeting agenda for a sample of weeks to determine that weekly operations team meetings were scheduled to be held during the period for each week sampled.	No exceptions noted.
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Documented policies and procedures are in place to guide cloud operations personnel in backup and recovery activities.	Inspected the backup and recovery policies and procedures to determine that documented policies and procedures were in place to guide cloud operations personnel in backup and recovery activities.	No exceptions noted.
A1.2.2	An automated backup system is utilized to perform daily system and database backups.	Inspected the automated backup system configurations to determine that an automated backup system was utilized to perform daily system and database backups.	No exceptions noted.
A1.2.3	The ability to access backup data is restricted to user accounts accessible by authorized personnel.	Inspected the listing of users with access to backup data to determine that the ability to access backup data was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
A1.2.4	Redundancy of infrastructure components is built into the architecture to help mitigate the risk of production equipment failures.	Inspected the failover and redundancy configurations to determine that redundancy of infrastructure components was built into the architecture to help mitigate the risk of production equipment failures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2.5	Disaster recovery plans are in place to guide personnel in procedures to respond to disruptions caused by an unexpected event.	Inspected the disaster recovery plans to determine that disaster recovery plans were in place to guide personnel in procedures to respond to disruptions caused by an unexpected event.	No exceptions noted.
	AWS is responsible for ensuring the data center facilities are equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.		
	AWS is responsible for providing redundant underlying infrastructure components to help ensure that DriveWealth's systems are able to be restored.		
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Operations personnel perform backup restores at least annually to verify that system components can be recovered from system backups.	Inspected evidence of the most recently completed backup restore documentation to determine that operations personnel performed backup restores to verify that system components can be recovered from the systems backups during the period.	No exceptions noted.
A1.3.2	The disaster recovery plan is tested on at least an annual basis.	Inspected the results of the most recent disaster recovery test to determine that the disaster recovery plan was tested during the period.	No exceptions noted.

SECTION 5

**OTHER INFORMATION
PROVIDED BY
DRIVEWEALTH**

MANAGEMENT’S RESPONSE TO TESTING EXCEPTIONS

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<p>CC6.2.2 CC6.3.2</p>	<p>Termination tickets are completed, and system access is revoked for employees as a component of the employee termination process on the date of termination.</p>	<p>Inspected the termination ticket for a sample of employees terminated during the period to determine that termination tickets were completed as a component of the employee termination process for each employee sampled.</p>	<p>The test of the control activity disclosed that termination tickets were not completed for 10 of 25 terminated employees sampled.</p>
<p>Management's Response:</p>	<p>DriveWealth underwent a reduction in force (RIF) that did not create a termination ticket for the individuals that were sampled. During the process an exception was made for tracking the off boarding of all individuals that were impacted. This exception included tracking each individual through a spreadsheet that contained every application and system that was disabled.</p> <p>To prevent this result in the future an updated process has been created to handle this type of activity. A ticket will be made to track the entirety of the removal of any terminations that are in bulk satisfying the internal requirements for tracking off-boarding of employees.</p>		