Modern Hire

SOC 2 Report

For The

Recruiting and Hiring Solutions

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security, Availability, and Confidentiality

January 1, 2021, to December 31, 2021

Attestation and Compliance Services

schellman
Quality, above all.

This report is intended solely for use by the management of Modern Hire, Inc., user entities of Modern Hire, Inc.'s services, and other parties who have sufficient knowledge and understanding of Modern Hire, Inc.'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.

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Modern Hire, Inc.:

Scope

We have examined Modern Hire, Inc.'s ("Modern Hire" or the "service organization") accompanying description of its Recruiting and Hiring Solutions system, in Section 3, throughout the period January 1, 2021, to December 31, 2021, (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 January 1, 2021, to December 31, 2021, to provide reasonable assurance that Modern Hire's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Modern Hire 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 Modern Hire, to achieve Modern Hire's service commitments and system requirements based on the applicable trust services criteria. The description presents Modern Hire's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Modern Hire'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.

Service Organization's Responsibilities

Modern Hire 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 Modern Hire's service commitments and system requirements were achieved. Modern Hire has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Modern Hire is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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.

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 Modern Hire's Recruiting and Hiring Solutions system that was designed and implemented throughout the period January 1, 2021, to December 31, 2021, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Modern Hire'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 Modern Hire's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Modern Hire'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 Modern Hire'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 Modern Hire; user entities of Modern Hire's Recruiting and Hiring Solutions system during some or all of the period January 1, 2021, to December 31, 2021, business partners of Modern Hire subject to risks arising from interactions with the Recruiting and Hiring Solutions 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.

Schellman & Company, LLC

Tampa, Florida
January 10, 2022

Section 2

Management's Assertion

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Modern Hire's Recruiting and Hiring Solutions system, in Section 3, throughout the period January 1, 2021, to December 31, 2021, (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 Recruiting and Hiring Solutions system that may be useful when assessing the risks arising from interactions with Modern Hire's system, particularly information about system controls that Modern Hire has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Modern Hire 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 Modern Hire, to achieve Modern Hire's service commitments and system requirements based on the applicable trust services criteria. The description presents Modern Hire's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Modern Hire'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 Modern Hire's Recruiting and Hiring Solutions system that was designed and implemented throughout the period January 1, 2021, to December 31, 2021, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Modern Hire's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Modern Hire's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period January 1, 2021, to December 31, 2021, to provide reasonable assurance that Modern Hire'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 Modern Hire's controls operated effectively throughout that period.

Section 3

Description of the System

OVERVIEW OF OPERATIONS

Company Background

Modern Hire, Inc. or ("Modern Hire") is a privately-owned Software as a Service (SaaS) company that formed in 2019 as the result of the merger between Montage Talent, Inc. and Shaker International. Modern Hire expands on the traditional talent acquisition process by leveraging science-based technology to enable organizations the ability to improve their hiring experience and outcomes. The Modern Hire platform combines technologies such as artificial intelligence (AI), predictive analysis, workflow automation, and assessment to provide their clients an objective and unbiased tool to use during the talent acquisition process. Modern Hire has offices in Delafield, Wisconsin; Cleveland, OH; and Wexford, Ireland.

Description of Services Provided

Modern Hire's SaaS platform offering includes multiple solutions to make the talent acquisition process seamless. In addition to providing clients with a platform to enable an objective and unbiased hiring product, Modern Hire also provides services for client onboarding and ongoing support.

The services provided by Modern Hire include a virtual hiring platform that covers the entire talent acquisition process. By leveraging technologies such as AI, predictive analysis, and workflow automation, Modern Hire's platform captures the essence of the traditional hiring process while providing clients with objective and unbiased results to aid in decision-making.

Modern Hire's platform utilizes scientifically proven pre-hire assessments and virtual job simulations, along with interviewing technology solutions that all work together to provide both the candidate and user organization an enhanced interview experience. Modern Hire's platform offers users two different types of interviews – live or on-demand.

- Live Interviews – The live interviews can be between a candidate and one or more interviewers and can occur in-person, over a telephone system, or any web-enabled video device (i.e., laptops, smart phone, tablet).
- On-demand Interviews – The on-demand interview process differs from the live interview in that the on-demand interview allows candidates the opportunity to answer questions on their own time and schedule. The answers to these questions can be submitted either by smart phone, tablet, or desktop computer.

Upon completing the interview of choice, the Modern Hire platform then provides Automated Interview Scoring. Automated Interview Scoring analyzes candidate interview responses and recommends scores based on job-relevant data and core competencies that are linked to the candidate's job success. Recruiters then receive a rank-ordering of candidates based on an overall score, simplifying the selection of the most qualified candidate to move forward with. The AI analysis focuses on the content of the candidates' answers instead of the candidates' image, facial expressions, or audio qualities.

Further, Modern Hire provides a client success service that is included with its SaaS offering to assist clients through onboarding, change management, and to familiarize clients in using their product. Modern Hire employees configure the client's application, provide training, and usage recommendation to ensure smooth and successful adoption of the Modern Hire SaaS application. Lastly, Modern Hire's client support services are on-call and can be reached either via phone, e-mail, or chat on Modern Hire's website should any issues arise in the use of Modern Hire's platform.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Modern Hire designs its processes and procedures related to the system to meet its objectives for its Recruiting and Hiring Solutions services. These objectives are based on the service commitments that the organization makes to user entities, the laws and regulations that govern the provisioning of the Recruiting and Hiring Solutions services, and the financial, operational, and compliance requirements that the organization has established for the services. The Recruiting and Hiring Solutions services are subject to the relevant regulatory, industry, and data security requirements in which Modern Hire operates.

The security, availability, and confidentiality commitments to user entities are documented and communicated in customer contracts, non-disclosure agreements, company policies, and the company website. The principal security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

Security

- Restrict physical and logical access to authorized users.
- Maintain up-to-date software patches and antivirus software.
- Perform regular vulnerability scans and penetration testing.
- Identify and remediate security incidents/events.
- Perform risk assessments for both internal and external threats to the system and its information.

Availability

- Maintain system availability within the production environment with an uptime of 99%.
- Perform data backups on a periodic basis to support system recovery.

Confidentiality

- Retain and/or dispose of confidential information in accordance with guidelines and contractual requirements.
- Encrypt confidential information at rest and in transit.

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

In accordance with the 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 production information systems are maintained at third-party data centers operated by Amazon Web Services, Inc. (AWS) in the primary US East (Northern Virginia) and secondary US West (Oregon) regions. AWS provides Infrastructure as a Service (IaaS), which consists of virtual servers, databases, infrastructure management and maintenance, and security infrastructure.

The applications are housed on servers running Microsoft Windows operating systems. SQL server databases and AWS Simple Storage Service (S3) are also utilized to support the applications.

The in-scope infrastructure consists of multiple systems, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Location**
Identity and Access Management	Hosted access solutions used by internal personnel to access systems, infrastructure components, and various corporate resources.	Microsoft Azure Active Directory (AD)	N/A
Elastic Compute Cloud (EC2)	Used for virtual application delivery and support for the Recruiting and Hiring Solutions.	Windows	US East (N. Virginia) and US West (Oregon)
Databases	Used to store, retrieve, and manage data input into the system, as well as perform analytical transactions.	SQL Server	
Storage System	Used to store and retrieve file data, including files uploaded by customers.	AWS S3	
Firewall System	Virtual firewall system configured to protect the network perimeter and limit inbound and outbound access.	AWS EC2 Security Groups	
Web Application	Modern Hire's Recruiting and Hiring Solutions SaaS platform.	Windows	

People

The personnel supporting the Modern Enterprise Platform include, but are not limited to, the following:

- Executive management – responsible for developing and executing overall global business strategy including market approach, service and software provision to clients and customers, and recruiting and developing Modern Hire people.
- Corporate IT department – responsible for managing, monitoring, and supporting user entities' information and systems, and protecting systems from unauthorized access and use while maintaining integrity and availability.

- DevOps engineers – responsible for developing infrastructure automation code and serving as the liaison between development and operations; however, these members are independent of teams who develop application code.
- Finance – responsible for financial planning and reporting, accounts payable, and accounts receivable.
- Functional groups (software development, knowledge management, marketing, and communications, HR, and legal) – responsible for carrying out business strategy and company objectives.

Procedures

Access Authentication and Authorization

Modern Hire maintains information security policies that include information on security roles and responsibilities of various levels of management, Internet security, computer, and network security, use of corporate services, Internet/intranet usage, and consequences of security violations.

Modern Hire uses a multi-tiered approach to protecting resources and assets within their environment. This includes logical security from desktop through the network and server environments. To access system information, including confidential data, resources are protected by secure authentication and authorization mechanisms. The in-scope systems are configured to authenticate users with a unique username and enforce predefined user account and minimum password requirements including the following:

- Minimum password history
- Password expiration intervals
- Minimum password length
- Password complexity
- Invalid password account lockout threshold

The AD domain controller is utilized to manage access to the corporate and production networks. Access to system information, including confidential information, is controlled with role-based access groups. The AD servers are configured with predefined user groups to help restrict access based on roles and responsibilities and to enforce minimum password controls. Elevated access privileges (administrative access) within the AD network domain are restricted to authorized IT, security, and technical operations personnel.

Modern Hire has implemented single sign-on (SSO) for central authentication to applications and systems via employees' AD credentials (applications, servers, databases, and firewalls). These include access to the development and production environments in AWS. Additionally, users are required to authenticate to the VPN for remote access to the production environments.

Privileged access is restricted to administrator groups defined per system and application within AD. Privileged access to the AWS infrastructure is controlled with Identity and Access Management (IAM) security groups provisioned via AD. Provisioning users to AWS groups is performed by the IT team. The AWS management console is restricted to authorized personnel and centrally managed by the engineering and DevOps team.
Users are informed of their responsibilities regarding access and password management in the access control policy and password policy. Users are required to have a unique user account and authenticate into respective environments using a password that meets the system enforced criteria.

Access Requests and Access Revocation

A defined user access management process is in place. HR initiates the new employee access provisioning process by submitting an access request to the ticketing system and sends a follow up e-mail to the new hire's corresponding manager. Modern Hire corporate IT will create accounts on a least privilege basis as applicable to the role. Employees are assigned a unique network domain account, and user access requests are documented within the ticketing system and require manager approval. The Modern Hire development team is responsible for provisioning access rights to the production systems and environments. Once the user access request is initiated in the ticketing system, manager approval is required before access is granted. The Modern Hire production

environment is separate from the corporate network domain. Employees who require access to the production environment are authorized and assigned a separate distinct production user account to that environment.

Upon notification from HR of an employee termination, a termination ticket is created within the ticketing system and notification of the termination is communicated to the appropriate departments via e-mail (i.e., system owners, IT, etc.). Once the notification is sent, the departments that received the notification work together with corporate IT to ensure that the individual's access is not retained subsequent to their termination date. Depending on the sensitivity and/or urgency, the initial termination notice given to IT may be verbal. In either case, the stakeholder confirms via e-mail that the terminated employee's access has been revoked.

IT personnel perform a review of user access privileges on a quarterly basis to verify that network accounts are revoked for terminated employees, administrative access privileges are assigned to authorized personnel, and system access levels are commensurate with current job responsibilities. When a user is identified to no longer require access to the systems, their access is subsequently revoked.

Device and Network Security

AWS security groups are utilized to act as a virtual firewall to block unauthorized inbound network traffic from the internet. Further, access to production infrastructure and management systems, including the virtual firewall, is restricted via two-factor authentication. To ensure that data is transferred safely and securely to the intended party, encrypted VPNs are utilized for remote access for the security and integrity of the data passing over the public network. In addition, web servers utilize TLS encryption protocols for web communication sessions. Furthermore, confidential data is stored in an encrypted format. Access privileges to the cryptographic keys stored within the key management system are restricted to authorized personnel.

Modern Hire utilizes full disk encryption on employee workstations. Enterprise antivirus software is utilized to protect registered workstations that scan for updates to antivirus definitions and update registered clients in real time. The antivirus software is also configured to notify IT personnel via e-mail when malicious software is detected. Individuals from corporate IT and DevOps are notified in the event that malicious software is detected.

Change Management

Modern Hire has implemented both change management and software development lifecycle (SDLC) policies and procedures to guide personnel in application development, maintenance, and documentation activities. Change management meetings are held on both daily and weekly frequencies involving members of the DevOps team, infrastructure, corporate IT, and executive technology leadership to discuss and communicate on-going sprint activities, approval of changes ready to be released to production, and upcoming projects that affect Modern Hire's platform.

Modern Hire uses a ticketing system to document and track the various stages and lifecycle of each change to be made to the production environment. Changes are documented within a process workflow management ticket to capture the various change management tasks associated with each change. This includes procedures for the request, authorization, testing, configuration, quality assurance (QA), peer review, approval, and migration of changes to production. Details regarding the workflow stages through the completion of quality assurance activities are captured within the ticket for each change. Once a given change has been through each task of the change management cycle, the ticket is completed and evaluated as part of the weekly change management meeting. Management reviews the change details to ensure that the change process was followed, and segregation of duties was maintained between individuals involved in the authorization, development, and migration to production.

Upon receiving approval, a member of the DevOps team will migrate the change to production. Version control software is utilized to restrict access to source code and provide rollback capabilities. Administrative access to the version control software is restricted to user accounts accessible by authorized personnel. To increase security through isolation, the production environment is logically segmented from the development environment.

In addition to the change management and SDLC policies and procedures, documented patch management policies and procedures are in place to guide personnel in the monitoring, management, and application of patches to production systems. Vendor-supplied software, such as operating systems, database software, applications, etc., are patched with vendor-approved releases. The infrastructure team manually tracks critical releases by vendors supporting Modern Hire's environment. On a monthly basis, critical vendor releases are reviewed and applied.

Patches go through the same authorization, testing, and approval guidelines that are defined in Modern Hire's change management policy.

Data Backup and Disaster Recovery

Modern Hire employs an automated backup system that is utilized to backup production databases at predefined frequencies. The automated backup system is configured to perform full backups on a weekly basis, differential backups on a daily basis, and log backups every five minutes. The automated backup system is configured to notify IT personnel in the event of failure in processing backup jobs. IT personnel review the backup reports, investigate the cause for any failed backup jobs, and track the resolution of noted errors.

An automated replication system is used to replicate backups to a secondary AWS region on a continuous basis. Additionally, data restoration is completed manually by the infrastructure team on a monthly basis to help ensure that data can be restored from replicated backups.

Disaster recovery and business continuity plans are in place to address the framework in which a business disruption would be managed to minimize the loss of vital resources throughout the company. The primary objective of Modern Hire's disaster recovery and business continuity plans is to ensure that continued operation of identified business-critical processes in the event of a disaster can resume with a recovery time objective (RTO) of four hours and a recovery point objective (RPO) of one hour.

Modern Hire's disaster recovery plan details accountabilities, defines planning standards, and outlines the procedures and processes to be followed if an unplanned disaster occurs to Modern Hire or its clients. In the event of a disaster, Modern Hire's primary objective is to ensure that affected parties are safe and out of harm's way so that necessary resources can be employed to ensure timely resumption of critical processes. The disaster recovery plan is tested at least annually to ensure the continuity of operations and availability of critical resources in the event of a disaster.

Incident Response

Modern Hire has established a detailed incident policy that outlines the framework required to bring needed resources together in an organized manner to deal with adverse events related to the safety and security of the entity. Throughout the policy are standard operating procedures to guide personnel through the incident response process particularly over the evaluation, assessment, containment, eradication, recovery, notification, and remediation of any identified security incidents. If an incident occurs, employees contact the following individuals in order:

- Information security officer (ISO)
- CTO
- Vice president (VP) of engineering
- Director of DevOps
- Fourth tier support (i.e., QA lead, software architect)

Further, an incident will be categorized by the ISO as one of three severity levels. These severity levels are based on the impact to Modern Hire and can be expressed in terms of financial impact, impact to development, impact to sales, impact to Modern Hire's image or impact to trust by Modern Hire's clients.

The table below describes the severity levels and definition/description of each:

Severity Level	Description
Low (Security Event)	Incident where the impact is minimal. Examples are harmless isolated e-mail phishing attempts where the user acted, isolated virus infections, incidental client breaches (recruiter loads candidate information into a training environment), etc.

Severity Level	Description
Medium (Security Event)	Incident where the impact is significant. Examples are a delayed ability for users to access web services, delayed delivery of critical electronic mail, client breaches that may impact Modern Hire, successful phishing attack however isolated to a few users. Incident Response Team (IRT) involvement may not be necessary (determined by ISO or CTO).
High (Security Event)	Incident where the impact is severe. Examples are a disruption to web services, Modern Hire proprietary or confidential information has been compromised, a virus or worm has become widespread and is affecting over twenty percent of the employees, or Modern Hire executive management has reported it. IRT involvement is mandatory.

Once the severity level of an incident is determined, the IRT is engaged to protect Modern Hire's information assets, provide central organization to handle the incident, comply with (government or other) regulations, prevent the use of Modern Hire's systems in attacks against other systems, and minimize the potential for negative exposure. Modern Hire utilizes a ticketing system to manage and track issues for response and resolution. In addition, Modern Hire uses various tools to notify support personnel in a timely manner when suspicious activity and/or events occur. Further, the director of information systems and security and the chief technology officer meet at least annually to discuss any security events, updates to the incident response procedure, retention policy, and other pertinent topics to help ensure open issues are monitored and responded to in a timely manner. A root cause analysis is also performed for incidents that includes an impact analysis, resolution, lessons learned, and action items.

System Monitoring

Modern Hire leverages an enterprise monitoring application through a third-party vendor to monitor the capacity levels of IT systems and notify personnel via e-mail when predefined thresholds such as central processing unit (CPU) utilization, memory utilization, and partition disk utilization are exceeded. Additionally, management meets on a weekly basis to review capacity levels and availability trends in Modern Hire's environments.

An intrusion detection system (IDS) is utilized to analyze network traffic for potential or actual network security breaches. In the event that a potential or actual security breach is encountered, e-mail alerts are sent to Modern Hire corporate IT personnel, who work to identify the cause and remediate the breach as soon as possible.

Workstations are protected by antivirus software from malicious activities in real-time. Additionally, a vulnerability assessment of the network and web applications is performed by a third-party vendor, Veracode, at least annually. IT personnel monitor the results of the assessments and create remediation plans to remedy any potential vulnerabilities.

Finally, redundancy is built into the architecture to allow for failover to a secondary region in the event of a failure. This includes servers, databases, and firewalls. A monitoring application is used to monitor various security events including failed authentication attempts, unauthorized access to the systems, and brute force attacks. In the instance that a predefined event occurs, the monitoring application is configured to notify IT personnel via e-mail alerts. Significant issues reported are logged, escalated, and monitored through remediation.

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**
Modern Hire Employee Data	Employee data is used for logging into the Modern Hire Recruiting and Hiring Solutions platform.	Confidential

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Modern Hire data which may include, client information, such as client user data, background information, and other commercial details	Client data is used to generate metrics, reports, and viewable dashboards using the Recruiting and Hiring Solutions platform; the Recruiting and Hiring Solutions platform is used to assist talent acquisition in the hiring and recruiting process.	Confidential
Modern Hire source code and configuration data	N/A	Confidential and Proprietary

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 Modern Hire, and the types of controls expected to be implemented at AWS to achieve Modern Hire'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 implementing controls to manage logical access to the underlying network and virtualization management software for its cloud hosting services where production systems reside.	CC6.1 – CC6.3 CC6.6 – CC6.7
AWS is responsible for implementing controls to restrict physical access to facilities and protected information assets.	CC6.4
AWS is responsible for implementing controls to render data unreadable, when directed by Modern Hire, prior to the decommissioning of physical assets.	CC6.5
AWS is responsible for implementing controls to protect against environmental vulnerabilities and changing environmental conditions.	A1.2

CONTROL ENVIRONMENT

The control environment at Modern Hire 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 Modern Hire's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Modern Hire's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. Specific control activities that the service organization has implemented are described below.

- An employee handbook is in place and acknowledged by employees upon hire to communicate entity values and behavioral standards to personnel.
- Employees are required to sign a confidentiality statement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Background checks are performed for employees as a component of the hiring process.

Board of Directors and Executive Management Oversight

Modern Hire's control consciousness is influenced by its board of directors and executive management. The board of directors and executive management provide strategic direction and operational guidance, approves significant entity acquisitions, and reviews and approves corporate plans and policies. Attributes include the board of directors' independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors. Specific control activities that the service organization has implemented in this area are described below.

- A board of directors is in place to oversee management's system of internal control.
- The board of directors has members who are independent from internal control owners to provide independent oversight of company operations.
- The board of directors meets on an annual basis to measure the development and performance of internal control against documented objectives.

Organizational Structure and Assignment of Authority and Responsibility

Modern Hire's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Modern Hire's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. Modern Hire 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. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. The charts are updated as needed and communicated to employees via the company intranet. Additionally, documented position descriptions are in place to define the authorities and responsibilities required for employment positions.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Modern Hire'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.
- A skills assessment of employees is performed prior to employment to verify the required skillset based on the defined requirements within the job description.

- Documented position descriptions are in place to highlight company benefits and attract competent individuals.
- Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
- A performance review is conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct and provide opportunities for development as needed.
- An employee referral program is in place to attract new talent and retain competent individuals.

In addition, Modern Hire is committed to employee professional development by allocating training dollars for employees to attend conferences outside of the entity.

Accountability

Management establishes accountability by setting a strong tone at the top and holding personnel accountable for internal control responsibilities. Accountability encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitude toward information processing, accounting functions, and personnel. The organization analyzes business risks to ensure that the most informed decisions can be made with the information that is available.

Employees are required to complete security awareness training upon hire and annually thereafter to confirm their understanding regarding their internal control responsibilities in the pursuit of objectives. Management also conducts a performance review of employees on an annual basis to evaluate performance of employees against expected levels of performance and conduct and hold individuals accountable for their internal control responsibilities. Additionally, policies and procedures are in place that relate to company objectives, hiring, training, and disciplinary activities, including the consequences of noncompliance with organizational policies and procedures.

Risk Assessment

Modern Hire is susceptible to risks from both external and internal sources. As such, the entity has implemented a risk assessment program to identify and manage risks that could affect the organization's ability to provide reliable services for user entities. This process includes an internal review estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about actions to address them.

Objective Setting

The Modern Hire risk assessment program includes documented operations, reporting, and compliance objectives, along with associated risks, that are in line with the mission of the organization. Modern Hire has established documented policies for identifying, analyzing, and mitigating risk as it relates to the achievement of the organization's objectives. Modern Hire's objectives of the risk assessment program are to establish risk assessment requirements based on the following:

- Compliance with applicable laws and regulations;
- Applying commonly adopted industry standards and satisfying contractual obligations; and
- Maintaining confidentiality, integrity, and availability of Modern Hire's information assets.

These objectives are used to identify risk appetites which serve as the baseline for Modern Hire risk tolerances. Modern Hire then performs risk assessments to determine whether threats identified as part of their process pose a significant risk to the continuing operation of the business. The risk appetites are defined to determine if the identified risks deviate from the company's tolerance levels. In the event that a risk identified deviates from

management's risk tolerance, the risk is tracked and recorded using an online risk register. Risks are reviewed annually by the Executive Leadership Team (ELT).

Risk Identification and Analysis

Management is responsible for identifying the risks that threaten achievement of the criteria stated in management's description of the system. The scope of Modern Hire's risk assessment focuses on risks pertaining to critical technology, information records, personnel, and business processes. The culmination of each of these areas is referred to as Mission Essential Functions (MEFs). Modern Hire's implemented process for identifying relevant risks to MEFs is tracked and recorded using the risk register. This process includes estimating the magnitude of impact resulting from identified risks, assessing the likelihood of their occurrence, and determining appropriate actions to address them.

A risk assessment policy and framework for the evaluation of risks to the system is in place to identify and manage risks that could affect the company's ability to provide reliable services to its user entities. This process entails identification, assessment, notification, escalation, and resolution. Risks can be identified through management's internal knowledge of its operations. Identified risks are evaluated based on the magnitude of impact and likelihood. Upon performing the risk assessment, Modern Hire considers the process in the context of understanding what aspect(s) of the information system would cause the most business impact if it/they were to be compromised or destroyed. The determination of information systems to be considered for the risk assessment is based on the opinion of leadership, executive management, and stakeholders.

The magnitude of impact and likelihood of occurrence determines whether a risk is tolerable or intolerable based on management's risk appetite and assistance in prioritizing the response. Upon determining both of these factors, consideration is given towards mitigating activities and controls that work to limit the likelihood and impact. Management is responsible for implementing appropriate measures to monitor and resolve significant risks (e.g., implementing/revising control procedures, conducting specific internal audit projects, etc.). The remaining residual risk is then evaluated against management's risk appetite, at which point management determines if the risk falls within the acceptable boundaries or if they fall outside of those boundaries. If it is determined that the risk falls within management's acceptable boundaries, the risk assessment is complete, and it is up to the risk owner whether or not to include the risk in the risk register. If the risk identified falls outside of management's risk appetite, it is logged in the risk register and a treatment plan is established.

Given that threats to Modern Hire's business operations are ever-evolving, different approaches are used to evaluate MEFs and the impact that exploitation of assets could have on their business. Assets are analyzed considering the threats that could impact the confidentiality, integrity, and availability of Modern Hire's systems. Once threats are identified and understood, the impact is denoted within the risk register.

Once the impact that a particular risk may have against the business is interpreted and logged, Modern Hire assesses the likelihood of the exploitation of that same risk actually occurring through normal business operation. Likelihood determination is the rating that indicates the probability of a particular risk being exploited in the threat environment. To determine the overall likelihood that a potential vulnerability may be exercised, the following factors are considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls

When assessing the threat likelihood, any historical record of an event is also taken into consideration by management and risk owners. As defined in Modern Hire's risk assessment program, below are the likelihood ratings defined:

Likelihood	Definition
Negligible	Highly improbable to occur.
Very Low	1 - 3 times every 5 years

Likelihood	Definition
Low	<= once per year
Medium	<= once every 6 months
High	<= once per month
Very High	> once per month
Extreme	=> once per day
Unknown	Insufficient insight to determine likelihood

The magnitude of impact is evaluated both quantitatively and qualitatively. Quantitative impacts correlate to a loss in revenue, cost of repairing the system, and cost in restoring brand reputation. Qualitative impacts have more to do with the loss of credibility to the business. Magnitude of impact levels are defined as follows:

Magnitude of Impact	Impact Definition
Insignificant	No impact
Minor	No extra effort required to repair
Significant	Tangible harm, extra effort required to repair
Damaging	Significant expenditure of resources required; damage to reputation and
Serious	Extended outage and / or loss of connectivity; compromise of large amounts of data or services
Grave	Permanent shutdown; complete compromise

In making the risk determination, the particular threat/vulnerability pair can be expressed as a function of the following:

- The likelihood of a given threat source's attempt to exercise a given vulnerability
- The magnitude of the impact should a threat-source successfully exploit the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk

To measure the risk, the following risk-level matrix is used to assist in the analysis:

Threat Likelihood	Impact					
	Insignificant	Minor	Significant	Damaging	Serious	Grave
Negligible	Low	Low	Low	Low	Low	Low
Very Low	Low	Low	Low	Low	Low	Medium
Low	Low	Low	Low	Low	Medium	Medium
Medium	Low	Low	Medium	Medium	High	High
High	Low	Low	Medium	High	High	High
Very High	Low	Low	High	High	High	High
Extreme	Low	Low	High	High	High	High
Unknown	Low	Medium	High	High	High	High

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

Modern Hire's risk assessment considers the potential for fraud. Risks related to fraud are rated using a risk evaluation process and are documented, along with mitigation strategies, for management review. Fraudulent activities are those that impede the achievement of strategic goals and exacerbate risks in other risk categories. Management has noted that the company has zero appetite for activities that threaten the integrity, confidentiality, and availability of their business or systems.

Risk Mitigation

Management's review of risks and potential action plans, to mitigate identified risks, is an on-going process that occurs at various times throughout the year. On an annual basis, objectives and risks are reviewed by the ELT during the information security management system (ISMS) management review meeting. Appropriate control activities are discussed that would have the potential to contribute to the mitigation of information security risks to an acceptable level. In addition, the ELT meets to discuss the risk appetite to determine the risk acceptance criteria for each MEF. The table below demonstrates the risk appetites levels defined by Modern Hire:

Risk Appetite Rating	Description of Appetite
Zero Appetite	The company is unwilling to accept risks, threats, or opportunities within this category under any circumstances. Risk avoidance or elimination are the only treatment options.
Low Appetite	The associated risk is only acceptable if cost- justified controls and mitigations can be adopted to substantially minimize the potential harm to the company.
Moderate Appetite	The company can accept a degree of uncertainty to achieve an intended outcome given that effective measures are in place to monitor the risk and limit potential harm to the company.

Risk Appetite Rating	Description of Appetite
High Appetite	The company is willing to undertake these risks in order to attain high-value objectives.

The risk register is utilized to document the risk assessment and mitigation activities. The identification of threats, vulnerabilities, and assessment of consequences and likelihood is performed by management. Discussed risks are evaluated for likelihood of occurrence and impact to Modern Hire and its clients' business operations to the extent necessary, to provide reasonable assurances around integrity, confidentiality, and availability. Treatment of risks is defined in the table below:

Treatment Option	Description
Tolerate the risk	Where the risk is already below the company's risk appetite and further treatment is not proportionate.
Treat the risk	Where the risk exceeds the company's risk appetite, but treatment is available and reasonable; or where the treatment is so simple and cost effective that it is justifiable to treat the risk even though it falls below the company's risk appetite.
Transfer the risk	Where the risk cannot be brought below the company's risk appetite with proportionate treatment, but a cost-effective option is available to transfer the risk to a third party.
Terminate the risk source	Where the risk cannot be brought below the company's risk appetite with proportionate effort/resource and no cost-effective transfer is available, so the source of the risk is eliminated from the company.

The risk assessment considers risks associated with vendors and business partners. Confidentiality agreements are required to be in place with third parties prior to sharing information designated as confidential. Management reviews documentation provided by critical third-party service providers on an annual basis to help ensure that third-party providers are in compliance with integrity, availability, and confidentiality requirements. Various levels of cyber risk insurance are in place to offset the financial impact of a cyber-attack event.

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, availability, and confidentiality categories.

Selection and Development of Control Activities

The applicable trust services 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 services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Modern Hire's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Recruiting and Hiring Solutions system.

INFORMATION AND COMMUNICATION SYSTEMS

Documented policies and procedures are in place that identify the information required to support the functioning of internal control and achievement of objectives. Information is necessary for Modern Hire to carry out internal control responsibilities to support the achievement of its objectives related to the services. Management uses relevant and quality information from both internal and external sources to support the functioning of internal control. 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. The entity monitors the security impact of emerging technologies and the impact of applicable laws or regulations.

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. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must 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.

Communication takes such forms as policy manuals, procedures, e-mail, intranet postings and memoranda. Communication also can be made electronically, verbally, and through the actions of management.

Internal Communications

Modern Hire has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation and training for new employees, continuous and periodic training for employees, and the use of e-mail messages to communicate time-sensitive information. Escalation procedures for reporting incidents are in place to guide internal users in identifying and reporting failures, incidents, concerns, and other complaints. The policies and procedures are communicated to internal personnel via the company intranet and verbally from leadership. Upon hire and annually thereafter, employees are required to complete security awareness training to understand their obligations and responsibilities to comply with corporate and business unit security policies.

A newsletter is sent once a month, directly to the mailboxes of internal personnel, to communicate company objectives and changes to objectives. In addition, the monthly newsletter communicates information related to system outages, updates, alerts, and other information that employees should be aware of. The firm advocates an open-door policy and creates avenues for access for employees to express concerns to management as described in the whistleblower policy. The whistleblower channel on the company intranet is available for employees to report security incidents, concerns, and complaints. A user manual is also available to internal users to describe system functionality and security mechanisms.

External Communications

Modern Hire has implemented various methods of communication to help provide assurance that customers understand their roles and responsibilities in utilizing the services and communication of significant events. These methods include documenting customer contracts, nondisclosure agreements, and company policies to describe Modern Hire's commitments and the associated system requirements. The master software license, hosting and related services agreement includes appropriate contact information for customers. Additionally, marketing collateral and planned system outages are posted to the company intranet and within the monthly newsletter communicated to Modern Hire's customers so that customer facing teams may be able to communicate information to their customers. A help portal is available on Modern Hire's external facing customer website which allows individuals the opportunity to reach out, ask questions, provide feedback, or file complaints. The help portal automatically generates tickets and routes them to the Modern Hire IT help desk.

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 user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement.

Ongoing Monitoring

Modern Hire leverages several technologies and procedures to monitor and evaluate the operational effectiveness of internal controls around the services they provide. Documentation is in place to facilitate the monitoring of both Modern Hire systems and client systems hosted by Modern Hire. Further, Modern Hire has also deployed an IDS to log events, which are inventoried and addressed based upon severity.

Controls are updated as needed based on client needs, if any, and according to internal changes in control structure from time to time.

Modern Hire utilizes both manual and automated monitoring tools to monitor control activities, including the following:

- In carrying out its regular management activities, operations management obtains evidence that the system of internal control continues to function, including error and performance reports.
- Organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- A monitoring application is configured to identify security events, potential breaches, and privileged user activity. The application is configured to send alerts to administrators and security personnel in the event of a failure on the monitored component of the production environment. For alerts identified as critical, a member of the operations team creates a ticket to track and resolve the issue.

Separate Evaluations

Management has implemented an internal audit program to evaluate the performance of specific control activities and processes over time and confirm that the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. The Internal Audit (IA) department performs a variety of audits during throughout the year, including but not limited to:

- Information technology
- Information security
- Asset management
- Human resource compliance
- Vendor management compliance

Remediation plans are reviewed and tracked to closure with parties responsible for taking corrective action, to help ensure identified internal control deficiencies are remediated in a timely manner. The IA department prepares a report at the conclusion of each audit performed and provides to the responsible parties details on the conclusion of their results. Additionally, a third-party vendor is contracted to perform external vulnerability scans and a penetration test of the applications annually.

Subservice Organization Monitoring

The services provided by AWS are monitored on a regular basis as part of the day-to-day business operations. In addition, Modern Hire receives and reviews the subservice organization attestation reports on an annual basis to

help ensure that the security practices conform to management's expectations, that any relevant findings are sufficiently mitigated, and that any applicable complimentary user entity controls are assessed.

Evaluating and Communicating Deficiencies

Deficiencies in an entity's internal control system surface from many sources. Management has developed protocols to ensure that findings of internal control deficiencies are reported to the individual directly responsible for the function or activity involved and who is in the position to take corrective action. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and make the decision for addressing deficiencies based on whether the incident was isolated or requires a change in procedures or personnel.

System Incident Disclosures

No system incidents occurred 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 Recruiting and Hiring Solutions system provided by Modern Hire. The scope of the testing was restricted to the Recruiting and Hiring Solutions system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period January 1, 2021, to December 31, 2021.

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	An employee handbook is in place and acknowledged by employees upon hire to communicate entity values and behavioral standards to personnel.	Inspected the employee handbook and the acknowledgment form for a sample of employees hired during the period to determine that an employee handbook was in place and acknowledged by each employee sampled upon hire to communicate entity values and behavioral standards to personnel.	No exceptions noted.
CC1.1.2	Employees are required to sign a confidentiality statement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality agreement for a sample of employees hired during the period to determine that each employee sampled signed a confidentiality statement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	Background checks are performed for employees as a component of the hiring process.	Inspected the completed background check documentation for a sample of employees hired during the period to determine that background checks were performed for each employee sampled as a component of the hiring process.	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	A board of directors is in place to oversee management's system of internal control.	Inspected the board of directors' biographies and meeting minutes to determine that a board of directors was in place to oversee management's system of internal control.	No exceptions noted.
CC1.2.2	The board of directors has members who are independent from internal control owners to provide independent oversight of company operations.	Inspected the board of directors' listing to determine that the board had members who were independent from control owners to provide independent oversight of company operations.	No exceptions noted.
CC1.2.3	The board of directors meets on an annual basis to measure the development and performance of internal control against documented objectives.	Inspected the meeting invite and minutes for the most recent board of directors meeting to determine that the board of directors met during the period to measure the development and performance of internal control against documented objectives.	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 in place that define the organizational structure, reporting lines, and authorities. These charts are communicated to employees and updated as needed.	Inspected the organizational charts posted on the company intranet to determine that organizational charts were in place that defined the organizational structure, reporting lines, and authorities and were communicated to employees and updated as needed.	No exceptions noted.
CC1.3.2	Documented position descriptions are in place to define the authorities and responsibilities required for employment positions.	Inspected the documented position description for a sample of employment positions to determine that documented position descriptions were in place to define the authorities and responsibilities required for each employment position sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	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.	Inspected the human resources policy and procedures to determine that new employee hiring 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	A skills assessment of employees is performed prior to employment to verify the required skillset based on the defined requirements within the job description.	Inspected the completed skills assessment for a sample of employees hired during the period to determine that a skills assessment of technical candidates was performed for each employee sampled prior to employment to verify the required skillset based on the defined requirements within the job description.	No exceptions noted.
CC1.4.3	Documented position descriptions are in place to highlight company benefits and attract competent individuals.	Inspected the position descriptions for a sample of employment positions to determine that documented position descriptions were in place to highlight company benefits and attract competent individuals for each employment position sampled.	No exceptions noted.
CC1.4.4	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.	Inspected the training course listing to determine that training courses were available to new and existing employees to maintain and advance the skill level of personnel.	No exceptions noted.
CC1.4.5	A performance review is conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct and provide opportunities for development as needed.	Inspected the performance review for a sample of current employees to determine that a performance review was conducted for each employee sampled during the period to evaluate the performance of employees against expected levels of performance and conduct and provide opportunities for development as needed.	No exceptions noted.
CC1.4.6	An employee referral program is in place to attract new talent and retain competent individuals.	Inspected the employee handbook to determine that an employee referral program was in place to attract new talent and retain competent individuals.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	An employee sanction procedure is in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	Inspected the employee handbook to determine that an employee sanction procedure was in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with a policy and/or procedure.	No exceptions noted.
CC1.5.2	A performance review is conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct and hold them accountable for their internal control responsibilities.	Inspected the performance review for a sample of current employees to determine that a performance review was conducted for each employee sampled during the period to evaluate the performance of employees against expected levels of performance and conduct and hold them accountable for their internal control responsibilities.	No exceptions noted.
CC1.5.3	Employees are required to complete security awareness training upon hire and annually thereafter to confirm their understanding regarding their internal control responsibilities.	Inspected the security awareness training materials and the training completion documentation for a sample of current employees and new employees hired during the period to determine that each employee sampled completed security awareness training upon hire or during the period to confirm their understanding regarding their internal control responsibilities.	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	Documented policies and procedures are in place that identify, define, and classify relevant and quality information required to support the functioning of internal control and achievement of objectives.	Inspected the data management policies to determine that documented policies and procedures were in place that identified, defined, and classified relevant and quality information required to support the functioning of internal control and achievement of objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.2	Relevant and quality internal and external data sources are used to support the functioning of internal control that include, but are not limited to, the following: • Service monitoring dashboards • Industry publications and security updates • Security reviews and vulnerability assessments	Inspected example internal and external data source updates that occurred during the period to determine that relevant and quality internal and external data sources were used to support the functioning of internal control that included the following: • Service monitoring dashboards • Industry publications and security updates • Security reviews and vulnerability assessments	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	Documented policies and procedures are in place to guide personnel in the entity's commitments, objectives, and the associated system requirements to support the functioning of internal control. These policies and procedures are communicated to employees via the company intranet.	Inspected the information security policies and procedures posted on the company intranet to determine that documented policies and procedures were in place to guide personnel in the entity's commitments, objectives, and the associated system requirements to support the functioning of internal control and were communicated to employees via the company intranet.	No exceptions noted.
CC2.2.2	Documented position descriptions are in place to define the responsibilities for internal control.	Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place for each employment position sampled to define the responsibilities for internal control.	No exceptions noted.
CC.2.2.3	Documented escalation procedures are in place to guide internal personnel in identifying and reporting failures, incidents, concerns, and other complaints.	Inspected the incident response plan to determine that documented escalation procedures were in place to guide internal personnel in identifying and reporting failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.2.4	Employees are required to complete security awareness training upon hire to confirm their understanding regarding their internal control responsibilities in the pursuit of objectives.	Inspected the security awareness training materials and the training completion documentation for a sample of current employees and new employees hired during the period to determine that each employee sampled completed security awareness training upon hire or during the period to confirm their understanding regarding their internal control responsibilities in the pursuit of objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.5	A whistleblower channel is available to internal users to report security incidents, concerns, and complaints.	Inspected the whistleblower page on the company intranet to determine that a whistleblower channel was available to internal users to report security incidents, concerns, and complaints.	No exceptions noted.
CC2.2.6	A user manual is made available to internal users to describe system functionality and security mechanisms.	Inspected the user manual available on the company website to determine that a user manual was made available to internal users to describe system functionality and security mechanisms.	No exception noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The entity's commitments and the associated system requirements, including the security, contractual, and regulatory requirements, are documented in service agreements.	Inspected the master service agreement to determine that the entity's commitments and the associated system requirements, including the security, contractual, and regulatory requirements, were documented in service agreements.	No exceptions noted.
CC2.3.2	Release notes are documented and communicated to internal and external parties via e-mail.	Inspected example internal and external communications to determine that release notes were documented and communicated to external parties via e-mail.	No exceptions noted.
CC2.3.3	System alerts, including planned changes to system components, planned outages, and known issues, are communicated to external parties via the company newsletter on a monthly basis.	Inspected the company newsletter for a sample of months during the period to determine that system alerts, including planned changes to system components, planned outages, and known issues were communicated to external parties via the company newsletter for each month sampled.	No exceptions noted.
CC2.3.4	A help portal is available to external parties to report security incidents, concerns, and complaints.	Inspected the help portal on the company website to determine that a help portal was available to external parties 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	The entity’s objectives are documented to align with the company mission and enable the identification and assessment of risks.	Inspected the objectives documentation to determine that the entity’s objectives were documented to align with the company mission and enable the identification and assessment of risks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.2	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to documented objectives.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the documented objectives.	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	A documented risk assessment methodology is in place to guide personnel in identifying and analyzing risks relating to the documented objectives.	Inspected the risk assessment policies and procedures to determine that a documented risk assessment methodology was in place to guide personnel in identifying and analyzing risks relating to the documented objectives.	No exceptions noted.
CC3.2.2	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to the documented objectives. Identified risks are rated using a risk evaluation process and are documented for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the documented objectives and that identified risks were rated using a risk evaluation process and were documented for management review.	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	A documented risk assessment methodology is in place to guide personnel in assessing risks including the potential for fraud.	Inspected the risk assessment policies and procedures to determine that a documented risk assessment methodology was in place to guide personnel in assessing risks including the potential for fraud.	No exceptions noted.
CC3.3.2	A risk assessment is performed on an annual basis that considers the potential for fraud. Identified risks are rated using a risk evaluation process and are documented for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the potential for fraud and that identified risks were rated using a risk evaluation process and were documented for management review.	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	A documented risk assessment methodology is in place to guide personnel in identifying and assessing changes that could significantly impact the system of internal control.	Inspected the risk assessment policies and procedures to determine that a documented risk assessment methodology was in place to guide personnel in identifying and assessing changes that could significantly impact the system of internal control.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.2	A risk assessment is performed on an annual basis that identifies and assesses changes that could significantly impact the system of internal control. Identified risks are rated using a risk evaluation process and are documented for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that identified and assessed changes that could significantly impact the system of internal control and that identified risks were rated using a risk evaluation process and were documented for management review.	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 through subscriptions to periodic industry publications.	Inspected example security updates and notifications received during the period to determine that the entity's IT security group monitored the security impact of emerging technologies and the impact of applicable laws or regulations through subscriptions to periodic industry publications.	No exceptions noted.
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	Security reviews and vulnerability assessments are performed on a periodic basis which include, but are not limited to, the following: • Application vulnerability scan annually • Application penetration test annually	Inspected the most recent vulnerability scan and penetration test reports to determine that security reviews and vulnerability assessments were performed which included the following: • Application vulnerability scan during the period • Application penetration test during the period	No exceptions noted.
CC4.1.2	An internal audit is conducted on an annual basis to ascertain whether the components of internal control are present and functioning.	Inspected the most recent internal audit documentation to determine that an internal audit was conducted during the period to ascertain whether the components of internal control were present and functioning.	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	Security reviews and vulnerability assessments are performed on a periodic basis which include, but are not limited to, the following: • Application vulnerability scan annually • Application penetration test annually Issues that are identified are communicated to relevant parties, tracked, and monitored through resolution.	Inspected the most recent vulnerability scan and penetration test reports to determine that security reviews and vulnerability assessments were performed which included the following: • Application vulnerability scan during the period • Application penetration test during the period	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the remediation tracking documentation to determine that issues that were identified were communicated to relevant parties, tracked, and monitored through resolution.	No exceptions noted.
CC4.2.2	An internal audit is conducted on an annual basis to ascertain whether the components of internal control are present and functioning. Issues that are identified are tracked and monitored through resolution.	Inspected the most recent internal audit documentation to determine that an internal audit was conducted during the period to ascertain whether the components of internal control were present and functioning and that issues identified were tracked and monitored through resolution.	No exceptions noted.
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	A documented risk assessment methodology is in place to guide personnel in selecting and developing control activities that contribute to the mitigation of risks.	Inspected the risk assessment policies and procedures to determine that a documented risk assessment methodology was in place to guide personnel in selecting and developing control activities that contribute to the mitigation of risks.	No exceptions noted.
CC5.1.2	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to the documented objectives. Mitigation strategies that include the development of control activities are documented for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to the documented objectives and that mitigation strategies that included the development of control activities were documented for management review.	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	A documented risk assessment methodology is in place to guide personnel in selecting and developing general control activities over technology to support the achievement of objectives.	Inspected the risk assessment policies and procedures to determine that a documented risk assessment methodology was in place to guide personnel in selecting and developing general control activities over technology to support the achievement of objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.2	A risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to technology. Mitigation strategies that include the development of general control activities over technology are documented to support the achievement of objectives.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered the identification and assessment of risks relating to technology and that mitigation strategies that included the development of control activities over technology were documented to support the achievement of objectives.	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 entity's commitments, objectives, and the associated system requirements to support the functioning of internal control. These policies and procedures are communicated to employees via the company intranet.	Inspected the information security policies and procedures posted on the company intranet to determine that documented policies and procedures were in place to guide personnel in the entity's commitments, objectives, and the associated system requirements to support the functioning of internal control and were communicated to employees via the company intranet.	No exceptions noted.
CC5.3.2	Employees are required to complete security awareness training upon hire and annually thereafter to confirm their understanding regarding their internal control responsibilities.	Inspected the security awareness training materials and the training completion documentation for a sample of current employees and new employees hired during the period to determine that each employee sampled completed security awareness training upon hire or during the period to confirm their understanding regarding their internal control responsibilities.	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	Documented policies and procedures are in place to guide personnel in logical security requirements that include, but are not limited to, the following: • Access management • Authentication requirements • Password management	Inspected the password policy to determine that documented policies and procedures were in place to guide personnel in logical security requirements that included the following: • Access management • Authentication requirements • Password management	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.2	The in-scope systems are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	Inspected the in-scope system user account listings and authentication configurations to determine that the in-scope systems were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	No exceptions noted.
CC6.1.3	Two-factor authentication is utilized for access to production systems.	Inspected the authentication configurations to determine that two-factor authentication was utilized for access to production systems.	No exceptions noted.
CC6.1.4	Predefined user groups are utilized to assign role-based access privileges and segregate access to data within the in-scope systems.	Inspected the in-scope system user listings to determine that predefined user groups were utilized to assign role-based access privileges and segregate access to data within the in-scope systems.	No exceptions noted.
CC6.1.5	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope systems administrator listings with the assistance of director of information systems and security to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
	AWS is responsible for implementing controls to manage logical access to the underlying network and virtualization management software for its cloud hosting services where production 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	New user access requests are documented within a checklist or ticket.	Inspected the access request documentation for a sample of employees hired during the period to determine that the new user access request was documented within a checklist or ticket for each employee sampled.	No exceptions noted.
CC6.2.2	A termination ticket is completed, and system access is revoked for employees as a component of the employee termination process.	Inspected the termination tickets and the in-scope user listings for a sample of employees terminated during the period to determine that a termination ticket was completed, and system access was revoked for each employee sampled as a component of the employee termination process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.3	User access reviews are performed on a quarterly basis to verify that access to the in-scope systems and data is restricted to authorized personnel.	Inspected the completed user access review for a sample of quarters during the period to determine that user access reviews were performed during each quarter sampled that verified that access to the in-scope systems and data was restricted to authorized personnel.	No exceptions noted.
	AWS is responsible for implementing controls to manage logical access to the underlying network and virtualization management software for its cloud hosting services where production 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	New user access requests are documented within a checklist or ticket.	Inspected the access request documentation for a sample of employees hired during the period to determine that the new user access request was documented within a checklist or ticket for each employee sampled.	No exceptions noted.
CC6.3.2	A termination ticket is completed, and system access is revoked for employees as a component of the employee termination process.	Inspected the termination tickets and the in-scope user listings for a sample of employees terminated during the period to determine that a termination ticket was completed, and system access was revoked for each employee sampled as a component of the employee termination process.	No exceptions noted.
CC6.3.3	User access reviews are performed on a quarterly basis to verify that access to the in-scope systems and data is restricted to authorized personnel.	Inspected the completed user access review for a sample of quarters during the period to determine that user access reviews were performed during each quarter sampled that verified that access to the in-scope systems and data was restricted to authorized personnel.	No exceptions noted.
CC6.3.4	Predefined user groups are utilized to assign role-based access privileges and segregate access to data within the in-scope systems.	Inspected the in-scope system user listings to determine that predefined user groups were utilized to assign role-based access privileges and segregate access to data within the in-scope systems.	No exceptions noted.
CC6.3.5	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope systems administrator listings with the assistance of the director of information systems and security to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
	AWS is responsible for implementing controls to manage logical access to the underlying network and virtualization management software for its cloud hosting services where production 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 implementing controls to restrict physical access to facilities and protected information assets.		
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	Asset removal and disposal policies are in place to guide personnel in the disposal of assets to ensure data and software is unrecoverable prior to decommissioning the physical asset.	Inspected the asset handling policies and procedures to determine that asset removal and disposal policies were in place to guide the disposal of assets and that data and software was required to be unrecoverable prior to decommissioning the physical asset.	No exceptions noted.
CC6.5.2	Assets are securely destroyed or erased prior to decommissioning to help ensure that data and software is unrecoverable.	Inspected the data sanitization receipts for a sample of assets decommissioned during the period to determine that each asset sampled was securely destroyed or erased prior to decommissioning.	No exceptions noted.
	AWS is responsible for implementing controls to render data unreadable, when directed by Modern Hire, prior to the decommissioning of physical assets.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	AWS security groups are utilized to act as a virtual firewall to block unauthorized inbound network traffic from the Internet.	Inspected the AWS security groups to determine that AWS security groups were utilized to act as a virtual firewall to block unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC6.6.2	Web servers utilize the TLS encryption protocol for web communication sessions.	Inspected the web certificate to determine that web servers utilized the TLS encryption protocol for web communication sessions.	No exceptions noted.
CC6.6.3	Encrypted VPNs are utilized for remote access for the security and integrity of the data passing over the public network.	Inspected the VPN encryption configurations to determine that encrypted VPNs were utilized for remote access for the security and integrity of the data passing over the public network.	No exceptions noted.
CC6.6.4	Two-factor authentication is utilized for access to production systems.	Inspected the authentication configurations to determine that two-factor authentication was utilized for access to production systems.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.5	Confidential data is stored in encrypted format. Access privileges to the cryptographic keys stored within the key management system are restricted to authorized personnel.	Inspected the database configurations and encryption key user access listings with the assistance of the director of information systems and security to determine that confidential data was stored in encrypted format and that access privileges to the cryptographic keys stored within the key management system were restricted to authorized personnel.	No exceptions noted.
	AWS is responsible for implementing controls to manage logical access to the underlying network and virtualization management software for its cloud hosting services where production 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	Documented policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the data management and cryptography policies to determine that documented policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
CC6.7.2	Web servers utilize the TLS encryption protocol for web communication sessions.	Inspected the web certificate to determine that web servers utilized the TLS encryption protocol for web communication sessions.	No exceptions noted.
CC6.7.3	Encrypted VPNs are utilized for remote access for the security and integrity of the data passing over the public network.	Inspected the VPN encryption configurations to determine that encrypted VPNs were utilized for remote access for the security and integrity of the data passing over the public network.	No exceptions noted.
CC6.7.4	Two-factor authentication is utilized for access to production systems.	Inspected the authentication configurations to determine that two-factor authentication was utilized for access to production systems.	No exceptions noted.
CC6.7.5	Employee workstations are configured with full disk encryption.	Inspected the encryption configurations for a sample of workstations belonging to current employees to determine that each employee workstation sampled was configured with full disk encryption.	No exceptions noted.
	AWS is responsible for implementing controls to manage logical access to the underlying network and virtualization management software for its cloud hosting services where production 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	Enterprise antivirus software is utilized to protect registered workstations with the following configurations: • Scan for updates to antivirus definitions and update registered clients in real time • Scan registered clients in real time	Inspected the enterprise antivirus software configurations to determine that enterprise antivirus software was utilized to protect registered workstations with the following configurations: • Scan for updates to antivirus definitions and update registered clients in real time • Scan registered clients in real time	No exceptions noted.
CC6.8.2	The enterprise antivirus software is configured to notify IT personnel via e-mail when malicious software is detected.	Inspected the enterprise antivirus alert configurations and an example alert generated during the period to determine that the enterprise antivirus software was configured to notify IT personnel via e-mail when malicious software was detected.	No exceptions noted.
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	Security reviews and vulnerability assessments are performed on a periodic basis to identify new vulnerabilities and susceptibilities to new vulnerabilities which include, but are not limited to, the following: • Application vulnerability scan annually • Application penetration test annually	Inspected the most recent vulnerability scan and penetration test reports to determine that security reviews and vulnerability assessments were performed which included the following: • Application vulnerability scan during the period • Application penetration test during the period	No exceptions noted.
CC7.1.2	An IDS is utilized to analyze and report network events.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was utilized to analyze and report network events.	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	Security reviews and vulnerability assessments are performed on a periodic basis to identify anomalies that are indicative of malicious acts and errors which include, but are not limited to, the following: • Application vulnerability scan annually • Application penetration test annually	Inspected the most recent vulnerability scan and penetration test reports to determine that security reviews and vulnerability assessments were performed which included the following: • Application vulnerability scan during the period • Application penetration test during the period	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC.7.2.2	Issues that are identified as part of the application vulnerability assessments are communicated to relevant parties, tracked, and monitored through resolution.	Inspected the remediation tracking documentation to determine that issues that were identified were communicated to relevant parties, tracked, and monitored through resolution.	No exceptions noted.
CC7.2.3	A log monitoring system is utilized to monitor and log events for the in-scope systems that include, but are not limited to, the following: • Failed logins • High volume requests • Administrative login and role assumption • Increased application requests	Inspected the log monitoring system configurations and example logs generated during the period to determine that a log monitoring system was utilized to monitor and log events for the in-scope systems that included the following: • Failed logins • High volume requests • Administrative login and role assumption • Increased application requests	No exceptions noted.
CC7.2.4	Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization, and alert engineering personnel upon detection of unusual system activity.	Inspected the logging and monitoring software configurations and an example alert generated during the period to determine that logging and monitoring software was configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization, and alert engineering personnel upon detection of unusual system activity.	No exceptions noted.
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Documented incident response and escalation procedures are in place to guide personnel in evaluating security events.	Inspected the incident response policy to determine that documented incident response and escalation procedures were in place to guide personnel in evaluating security events.	No exceptions noted.
CC7.3.2	IT management meetings are held on an annual basis to discuss and evaluate security incidents and actions to prevent or address them.	Inspected the meeting agenda and minutes for the most recent meeting to determine that IT management meetings were held during the period to discuss and evaluate security incidents and actions to prevent or address them.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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	Documented incident response and escalation procedures are in place to guide personnel in understanding, containing, remediating, and communicating security incidents.	Inspected the incident response policy and incident response form to determine that documented incident response and escalation procedures were in place to guide personnel in understanding, containing, remediating, and communicating security incidents.	No exceptions noted.
CC7.4.2	A tracking system is utilized to document security violations, responses, and resolution.	Inspected the security incident log to determine that a tracking system was utilized to document the security violation, response, and resolution.	No exceptions noted.
CC7.4.3	A root cause analysis is performed for incidents that includes an impact analysis, resolution, lessons learned, and action items.	Inspected the incident response policy to determine that a root cause analysis was performed for incidents that included an impact analysis, resolution, lessons learned, and action items.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented incident response and escalation procedures are in place to guide personnel in the identification, development, and implementation of activities to recover from identified security incidents.	Inspected the incident response policy to determine that documented incident response and escalation procedures were in place to guide personnel in the identification, development, and implementation of activities to recover from identified security incidents.	No exceptions noted.
CC7.5.2	A root cause analysis is performed for incidents that includes an impact analysis, resolution, lessons learned, and action items.	Inspected the incident response policy to determine that a root cause analysis was performed for incidents that included an impact analysis, resolution, lessons learned, and action items.	No exceptions noted.
CC7.5.3	IT management meetings are held on an annual basis to discuss and evaluate security incidents and actions to prevent or address them.	Inspected the meeting agenda and minutes for the most recent meeting to determine that IT management meetings were held during the period to discuss and evaluate security incidents and actions to prevent or address them.	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	Change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of changes.	Inspected the change management policy to determine that change management policies and procedures were in place to guide personnel in the request, documentation, testing, and approval of changes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.2	Changes made to in-scope systems are authorized, tested when applicable, and approved prior to implementation.	Inspected the change tickets for a sample of changes implemented during the period to determine that each change sampled was authorized, tested when applicable, and approved prior to implementation.	No exceptions noted.
CC8.1.3	Changes are tested when applicable and approved prior to implementation.	Inspected the change management system dashboard and workflow for a sample of changes implemented during the period to determine that each change sampled was tested when applicable and approved prior to implementation.	No exceptions noted.
CC8.1.4	The production environment is logically segmented from the development environment.	Inspected the environment configurations to determine that the production environment was logically segmented from the development environment.	No exceptions noted.
CC8.1.5	Version control software is utilized to restrict access to source code and provide rollback capabilities.	Inspected the version control software configurations to determine that version control software was utilized to restrict access to source code and provide rollback capabilities.	No exceptions noted.
CC8.1.6	Administrative access to the version control software is restricted to user accounts accessible by authorized personnel.	Inspected the version control software configurations and administrator listing with the assistance of the director of information systems and security to determine that administrative access to the version control software was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.7	The ability to implement changes is restricted to user accounts accessible by authorized personnel.	Inspected the change deployment user listing with assistance of the director of information systems and security to determine that the ability to implement changes was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC.8.1.8	Change management meetings are held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the system, and review and approve changes prior to implementation.	Inspected the recurring meeting invitation and meeting minutes to determine that change management meetings were scheduled to be held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affected the system, and review and approve changes prior to implementation.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.9	Documented patch management policies and procedures are in place to guide personnel in the monitoring, management, and application of patches to production systems.	Inspected the information security policy to determine that documented patch management policies and procedures were in place to guide personnel in the monitoring, management, and application of patches to production systems.	No exceptions noted.
CC.8.1.10	IT personnel review the availability of patches on production systems on a monthly basis to ensure patch updates are installed.	Inspected the patch tracker for a sample of months during the period to determine that IT personnel reviewed the availability of patches on production systems for each month sampled.	No exceptions noted.
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	A documented risk assessment methodology is in place to guide personnel in identifying, selecting, and developing risk management activities for risks arising from potential business disruptions.	Inspected the risk assessment policies and procedures to determine that a documented risk assessment methodology was in place to guide personnel in identifying, selecting, and developing risk management activities for risks arising from potential business disruptions.	No exceptions noted.
CC9.1.2	A risk assessment is performed on an annual basis that considers risks arising from potential business disruptions. Identified risks are rated using a risk evaluation process and are documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered risks arising from potential business disruptions and that identified risks were rated using a risk evaluation process and were documented, along with mitigation strategies, for management review.	No exceptions noted.
CC9.1.3	A cyber insurance policy is in place to offset the financial impact of materializing risk.	Inspected the cyber insurance policy to determine that a cyber insurance policy was in place to offset the financial impact of materializing risk.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	A vendor management policy is in place that addresses risks associated with vendors and business partners that includes, but is not limited to, the following: • Vendor classification and vetting • Vendor review • Exception handling • Termination of contract	Inspected the vendor management policy and standard to determine that a vendor management policy was in place that addressed risks associated with vendors and business partners that included the following: • Vendor classification and vetting • Vendor review • Exception handling • Termination of contract	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.2	A risk assessment is performed on an annual basis that considers risks associated with vendors and business partners. Identified risks are rated using a risk evaluation process and are documented, along with mitigation strategies, for management review.	Inspected the most recent risk assessment to determine that a risk assessment was performed during the period that considered risks associated with vendors and business partners and that identified risks were rated using a risk evaluation process and were documented, along with mitigation strategies, for management review.	No exceptions noted.
CC9.2.3	A signed nondisclosure agreement regarding confidentiality and the protection of data is required before sharing information designated as confidential with third parties.	Inspected the nondisclosure agreement for a sample of third parties onboarded during the period to determine that a signed nondisclosure agreement regarding confidentiality and the protection of data was required before sharing information designated as confidential with each third party sampled.	No exceptions noted.
CC9.2.4	Management reviews vendor audit reports and/or security questionnaires on an annual basis to help ensure that third-party vendors are in compliance with the organization's system requirements.	Inspected the most recent vendor assessment documentation to determine that management reviewed vendor audit reports and/or security questionnaires during the period.	No exceptions noted.

Additional Criteria for Availability Category

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	An enterprise monitoring application is configured to monitor the in-scope system capacity levels and notify IT personnel via e-mail when predefined thresholds are met.	Inspected the enterprise monitoring application configurations and example e-mail notifications generated during the period to determine that an enterprise monitoring application was configured to monitor the in-scope system capacity levels and notify IT personnel via e-mail when predefined thresholds were met.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1.2	IT management meetings are held at least weekly to review availability trends and forecasts as compared to system commitments.	Inspected the recurring meeting invite and the most recent meeting minutes to determine that IT management meetings were scheduled to be held at least weekly to review availability trends and forecasts as compared to system commitments.	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	An automated backup system is configured to perform scheduled backups of production data at predefined frequencies.	Inspected the backup system configurations to determine that an automated backup system was configured to perform scheduled backups of production data at predefined frequencies.	No exceptions noted.
A1.2.2	The automated backup system is configured to notify IT personnel via e-mail regarding backup job failures.	Inspected the backup system notification configurations and an example e-mail notification generated during the period to determine that the automated backup system was configured to notify IT personnel via e-mail regarding backup job failures.	No exceptions noted.
A1.2.3	Backup data is replicated to a geographically diverse secondary region on a continuous basis.	Inspected the replication configurations to determine that backup data was replicated to a geographically diverse secondary region on a continuous basis.	No exceptions noted.
A1.2.4	Disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the disaster recovery and business continuity plans to determine that disaster recovery and business continuity plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
	AWS is responsible for implementing controls to protect against environmental vulnerabilities and changing environmental conditions.		
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Data restoration is performed from replicated backups on a monthly basis to help ensure data can be recovered.	Inspected the data restoration documentation for a sample of months during the period to determine that data restoration testing was performed from replicated backups for each month sampled.	No exceptions noted.
A1.3.2	The disaster recovery plan is tested at least annually to help ensure the recoverability of operations in the event of a disaster.	Inspected the most recent disaster recovery test results to determine that the disaster recovery plan was tested during the period.	No exceptions noted.

Additional Criteria for Confidentiality Category

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Documented data retention policies and procedures are in place to guide personnel in the retention of confidential information.	Inspected the data retention policy to determine that documented data retention policies and procedures were in place to guide personnel in the retention of confidential information.	No exceptions noted.
C1.1.2	Confidential information is retained for the duration of an active contract and for a predefined period specified in the customer contract post termination.	Inspected the system data retention configurations to determine that confidential information was retained for the duration of an active contract and for a predefined period specified in the customer contract post termination.	No exceptions noted.
C1.1.3	Confidential information is stored in encrypted format. Access privileges to the cryptographic keys stored within the key management system are restricted to authorized personnel.	Inspected the database encryption configurations and encryption key user access listings with the assistance of the director of information systems and security to determine that confidential information was stored in encrypted format and that access privileges to the cryptographic keys stored within the key management system were restricted to authorized personnel.	No exceptions noted.
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	Documented data disposal policies and procedures are in place to guide personnel in the disposal of confidential information.	Inspected the data disposal policies and procedures to determine that documented data disposal policies and procedures were in place to guide personnel in the disposal of confidential information.	No exceptions noted.
C1.2.2	Confidential information is automatically purged based on parameters defined within the data disposal policies after retention commitments are met.	Inspected the automated data disposal configurations to determine that confidential information was automatically purged based on parameters defined within the data disposal policies after retention commitments were met.	No exceptions noted.