Shortlist Project, Inc.
Type 1 SOC 2
2020

REPORT ON SHORTLIST PROJECT, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY

Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205

August 31, 2020

Table of Contents

SECTION 1

ASSERTION OF SHORTLIST PROJECT, INC. MANAGEMENT

ASSERTION OF SHORTLIST PROJECT, INC. MANAGEMENT

September 10, 2020

We have prepared the accompanying description of Shortlist Project, Inc.'s ('Shortlist' or 'the Company') Automated Workflow Management and Performance Monitoring Solutions System titled "Shortlist Project, Inc.'s Description of Its Automated Workflow Management and Performance Monitoring Solutions System as of August 31, 2020" (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 Automated Workflow Management and Performance Monitoring Solutions System that may be useful when assessing the risks arising from interactions with Shortlist's system, particularly information about system controls that Shortlist has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

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

a. the description presents Shortlist's Automated Workflow Management and Performance Monitoring Solutions System that was designed and implemented as of August 31, 2020, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of August 31, 2020, to provide reasonable assurance that Shortlist's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Shortlist's controls as of that date.

Martin Konrad

Martin Konrad
Chief Product Officer
Shortlist Project, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Shortlist Project, Inc.

Scope

We have examined Shortlist's accompanying description of its Automated Workflow Management and Performance Monitoring Solutions System titled "Shortlist Project, Inc.'s Description of Its Automated Workflow Management and Performance Monitoring Solutions System as of August 31, 2020" (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 of controls stated in the description as of August 31, 2020, to provide reasonable assurance that Shortlist's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

Service Organization's Responsibilities

Shortlist 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 Shortlist's service commitments and system requirements were achieved. Shortlist has provided the accompanying assertion titled "Assertion of Shortlist Project, Inc. Management" (assertion) about the description and the suitability of the design of controls stated therein. Shortlist 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 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 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 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
- 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 the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects:

a. the description presents Shortlist's Automated Workflow Management and Performance Monitoring Solutions System that was designed and implemented as of August 31, 2020, in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of August 31, 2020, to provide reasonable assurance that Shortlist's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Shortlist's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Shortlist, user entities of Shortlist's Automated Workflow Management and Performance Monitoring Solutions System as of August 31, 2020, business partners of Shortlist subject to risks arising from interactions with the Automated Workflow Management and Performance Monitoring 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 user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

A-LIGN ASSURANCE

Tampa, Florida
September 10, 2020

SECTION 3

SHORTLIST PROJECT, INC.'S DESCRIPTION OF ITS AUTOMATED WORKFLOW MANAGEMENT AND PERFORMANCE MONITORING SOLUTIONS SYSTEM AS OF AUGUST 31, 2020

OVERVIEW OF OPERATIONS

Company Background

Shortlist Project Inc. (Shortlist) was founded in June 2015 with the objective of building and selling a SaaS software that will help corporations manage external talent. The solution is delivered via modern multi-modular platform, that offers a simple interface and modern UI. The organization is based in San Francisco, California with a distributed workforce model of employees based in the US, Europe, and South East Asia.

Customers served by Shortlist include Fortune 500 companies such as Disney, Microsoft and Loreal.

Description of Services Provided

Shortlist's core application, Shortlist Freelancer Management System is a multiuser, multitenant application suite that enables hiring, onboarding, tracking, managing and paying external workers.

- Capturing data via automated workflow tools
- Tracking workers with a modern system of record tool
- Managing profiles
- Managing onboarding and offboarding
- Tracking tasks and contracts
- Processing contractor engagement
- Processing bidding process
- Managing talent suppliers
- Tracking invoices and processing payments
- Providing operational, management, and ad hoc reports via integrated BI tool

Principal Service Commitments and System Requirements

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Shortlist that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

Shortlist establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Shortlist's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained.

Components of the System

Infrastructure

Primary infrastructure used to provide Shortlist's Automated Workflow Management and Performance Monitoring Solutions System includes the following:

Primary Infrastructure	
Hardware	**Purpose**
API Gateway	Expose webhook Lambdas through HTTPS.

Primary Infrastructure	
Hardware	**Purpose**
CloudFront	Content delivery and web cache
CloudTrail	Operator actions audit
CloudWatch	System monitoring and alerting
CodePipeline	Code builds and continuous deployment
Config	Configuration management and monitoring
DynamoDB	Webhook invocation logging
EC2 Container Registry	Code builds storage
Elastic Compute Cloud	Virtual machines for app servers.
Elastic Container Service for Kubernetes	Virtual machines for app servers.
Elastic File System	File system sharing for app servers.
ElastiCache	Memory cache for app servers.
Elasticsearch Service	Search and application logs
Key Management Service	Data encryption
Lambda	Webhooks and infrastructure helpers
Relational Database Service	PostgreSQL hosting for application databases.
Route 53	DNS provider
Secrets Manager	Application configuration
Security Hub	Security monitoring and alerting
Simple Notification Service	Alerting
Simple Queue Service	Zapier integration, Slack alerting
Simple Storage Service	Document and backup storage, static asset hosting

Software

Primary software used to provide Shortlist’s Automated Workflow Management and Performance Monitoring Solutions System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Shortlist main app	Linux/Kubernetes	App servers
Nginx	Linux/Kubernetes	Traffic routing, static asset hosting
Sisense	Windows Server	Embedded Business Intelligence
ClamAV	Linux/Kubernetes	Antivirus

Primary Software		
Software	**Operating System**	**Purpose**
Kubernetes	Linux	Cluster management
Flower (Celery)	Linux/Kubernetes	Background task monitoring
Kibana	Amazon Web Services (AWS) hosted	Log search
Prometheus/Grafana	Linux/Kubernetes	System monitoring

People

Shortlist has a staff of approximately 25 employees organized in the following functional areas:

- Corporate. Company founders, executives, senior operations staff, and company administrative support staff
- Product development team. Staff that administers the software development cycle such as managing JIRA ticketing system, running meeting, and scrum sessions
- Quality Assurance engineers that test the software and administer the process of deployment
- Engineering team developing and maintaining the product/software
- DevOps in charge of maintaining servers and security
- Sales, in charge of selling the software to new customers
- Customer service in charge of account management and support

Data

Data, as defined by Shortlist, constitutes the following:

- Master customers data
- Transaction data
- Output reports
- System files
- Error logs

Transaction processing is initiated by the receipt of an approved invoice in the customer client account. This request typically comes directly from customer’s contractor or vendor. After the invoice is approved, the payments operations team schedules the invoice for payment processing. The log activity is information is available in the invoice interface within the Shortlist product.

Output reports are available in the BI tool and can be exported to electronic PDF or comma-delimited value file.

The availability of these reports is limited by job function/role in a system.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Shortlist’s policies and procedures that define how services should be delivered.

These are located on the Company’s policy portal that can be accessed by any team member, or 3rd party on as per needed basis.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope service. See the ‘Subservice Organizations’ section below for detailed controls owned by AWS.

Logical Access

Shortlist uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources.

Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users’ authorized roles in access control lists.

Employees, Customers and registered vendor personnel sign on to the Shortlist’s system using an SSO user ID and password or standard user/password if SSO isn’t enabled.

Passwords must conform to defined password standards and are enforced through parameter settings in the SSO and Shortlist system. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID’s ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the shortlist network are required to use a token-based two-factor authentication system. Employees are issued tokens upon employment and must return the token during their exit interview.

Customer employees’ access their Shortlist accounts through the Internet using the Secure Sockets Layer (SSL) functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources or use their SSO. Passwords must conform to password configuration requirements.

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees’ start date, the HR management system creates a report of employee user IDs to be created and access to be granted. The report is used by the security team member to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access.

On a quarterly basis, managers review roles assigned to their direct reports.

Computer Operations - Backups

Customer data is backed up and monitored by engineering personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

The backup infrastructure resides on private networks logically secured from other networks.

Contracted customer off-site tape rotations are logged and maintained within an enterprise ticket management system. A third-party provider that specializes in off-site tape rotation has been contracted to perform off-site tape rotation services for clients that select this as part of the backup service.

The ability to recall backup media from the third-party off-site storage facility is restricted to authorized operations personnel.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify, and respond to incidents on the network.

Shortlist monitors the capacity utilization of computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements.

Shortlist evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power and cooling
- Disk storage
- Tape storage
- Network bandwidth

Shortlist has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches.

Customers and Shortlist system owners review proposed operating system patches to determine whether the patches are applied.

Customers and Shortlist systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them.

Shortlist staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Shortlist maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Shortlist has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Shortlist system owners review proposed operating system patches to determine whether the patches are applied. Customers and Shortlist systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Shortlist staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Shortlist.

The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network.

Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications, and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with Shortlist policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Shortlist. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Shortlist system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through from the Internet. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the Automated Workflow Management and Performance Monitoring Solutions System performed in the San Francisco, California and London, England facilities.

This report does not include the data center hosting services provided by AWS at the Virginia, California, and Canada facilities.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Shortlist's control environment, affecting the design, administration, and monitoring of other components.

Integrity and ethical behavior are the product of Shortlist'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. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed for employees as a component of the hiring process

Commitment to Competence

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

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Shortlist's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

Shortlist's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

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

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated to employees and updated as needed

Human Resources Policies and Practices

Shortlist's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Shortlist's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Shortlist's risk assessment process identifies and manages risks that could potentially affect Shortlist's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Shortlist identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Shortlist, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Shortlist has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Shortlist attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Shortlist's system; as well as the nature of the components of the system result in risks that the criteria will not be met.

Shortlist addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Shortlists management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of Shortlist's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Shortlist, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Shortlist personnel via e-mail and SLACK messages.

Specific information systems used to support Shortlist's system are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Shortlist's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Shortlist's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Shortlist's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Shortlist's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common/Security criterion was applicable to the Shortlist Automated Workflow Management and Performance Monitoring Solutions System.

Subservice Organizations

This report does not include the data center hosting services provided by AWS at the Virginia, California, and Canada facilities.

Subservice Description of Services

AWS is responsible for all physical security controls and data hosting services.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Shortlist management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant control objectives through written contracts, such as service level agreements. In addition, Shortlist performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and the subservice organization
- Reviewing attestation reports over services provided by vendors and the subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Shortlist's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Shortlist's services to be solely achieved by Shortlist control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Shortlist's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Shortlist.
2. User entities are responsible for notifying Shortlist of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.

4. User entities are responsible for ensuring the supervision, management, and control of the use of Shortlist services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Shortlist services.
6. User entities are responsible for providing Shortlist with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Shortlist of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security Category)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines and the employee handbook. An employee handbook in addition to a code of conduct within the handbook are documented to communicate workforce conduct standards and enforcement procedures. Upon hire, personnel are required to acknowledge the employee handbook. Prior to employment, personnel are required to complete a background check. Performance evaluations are performed for personnel on an annual basis. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct and are documented within the employee handbook. Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management evaluates the skills and expertise of its members annually. Executive management meets at least annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment. Executive management evaluates the skills and competencies of those that operate the internal controls implemented within the environment annually. Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's website. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Executive management has established proper segregations of duties for key job functions and roles within the organization.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Performance evaluations are performed for personnel on an annual basis. The entity evaluates the competencies and experience of candidates prior to hiring. The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives. Executive management has created a training program for its employees. The entity assesses training needs on an annual basis. Prior to employment, personnel are required to complete a background check.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority. Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's website. Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities. Performance evaluations are performed for personnel on an annual basis. Executive management reviews the responsibilities assigned to operational personnel annually and makes updates, if necessary. Sanction policies, which include probation, suspension and termination, are in place for employee misconduct and are documented within the employee handbook.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's Shared drive. Edit checks are in place to prevent incomplete or incorrect data from being entered into the system. Data flow diagrams and procedures manuals are documented and maintained by management to identify the relevant internal and external information sources of the system. Data that entered into the system, processed by the system and output from the system is protected from unauthorized access. Data and information critical to the system is assessed annually for relevance and use. Data is only retained for as long as required to perform the required system functionality, service or use.
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.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's website. The entity's policies and procedures are made available to employees through the entity's Shared drive. Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security training. Current employees are required to read and acknowledge the information security policies and procedures and complete information security training on an annual basis. Upon hire, personnel are required to acknowledge the employee handbook. Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities. Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner. Changes to job roles and responsibilities are communicated to personnel through the entity's year in review meetings.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's Shared drive. The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's annual year in review meetings. Management tracks and monitors compliance with information security training requirements. The entity's third-party agreements delineate the boundaries of the system and describes relevant system components. The entity's third-party agreements communicate the system commitments and requirements of third parties. The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users as needed. The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third parties. Customer commitments, requirements and responsibilities are outlined and communicated through service agreements. Changes to commitments, requirements and responsibilities are communicated to third parties, external users, and customers via mass notifications. Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties. Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics. Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART). Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved. Executive management has established KPIs for operational and internal controls effectiveness, including the acceptable level of control operation and failure. Business plans and budgets align with the entity's strategies and objectives. Entity strategies, objectives and budgets are assessed on an annual basis.
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.	Documented policies and procedures are in place to guide personnel when performing a risk assessment. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. The entity's risk assessment process includes: • Identifying and assessing the impact of the threats to the entity • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability Identified risks are rated using a risk evaluation process and ratings are approved by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.
		As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.
		As part of management’s assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes to the regulatory, economic and physical environment in which the entity operates are considered and evaluated as part of the annual comprehensive risk assessment.
		Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.
		Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.
		Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses. Control self-assessments that include, but are not limited to, quarterly logical access reviews, and annual backup restoration tests are performed. Systems are configured to enable ongoing vulnerability scanning to identify control gaps and vulnerabilities and summary reports are generated on a monthly basis. Evaluations of policies, controls, systems, tools, applications, and third parties for effectiveness and compliance is required at least annually. A third-party performs a penetration testing biannually to identify and exploit vulnerabilities identified within the environment. Performance and conduct evaluations are performed for personnel on an annual basis. Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.
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.	Senior management assesses the results of the compliance, control and risk assessments performed on the environment. Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed. Vulnerabilities identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions. Vulnerabilities identified from the compliance, control and risk assessments are documented, investigated, and addressed.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management tracks whether vulnerabilities identified as part of the evaluations performed are addressed in a timely manner.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps. Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations (e.g. risk assessments, vulnerability scans) performed. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Prior to the development and implementation of internal controls into the environment, management considers the complexity, nature, and scope of its operations. Management has documented the relevant controls in place for each key business or operational process. Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls. Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes. Organizational and information security policies and procedures are documented and made available to employee's through the entity's shared drive. Management has documented the controls implemented around the entity's technology infrastructure. Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	As part of the risk assessment process, the use of technology in business processes is evaluated by management. The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure. Organizational and information security policies and procedures are documented and made available to employee's through the entity's shared drive. Job descriptions detail the day-to-day activities to be performed by personnel. Management has implemented controls that are built into the organizational and information security policies and procedures. Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment. Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities. Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Privileged access to sensitive resources is restricted to authorized personnel. Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network	
		Network user access is restricted via role based security privileges defined within the access control system. Network administrative access is restricted to user accounts accessible by authorized personnel. Networks are configured to enforce password requirements that include: • Password length (minimum and maximum) • Password reset • Multi-factor authentication (MFA) • Complexity Network users are authenticated via individually-assigned user accounts and passwords. Network audit logging settings are in place. Network audit logs are maintained and are reviewed as needed.
	Operating Systems (Application, Web, and Database Servers)	
		Operating system user access is restricted via role based security privileges defined within the access control system. Operating system administrative access is restricted to user accounts accessible by authorized personnel. Operating systems are configured to enforce password and lockout requirements. Operating system audit logging settings are in place. Operating system audit logs are maintained and are reviewed as needed.
	Databases	
		Database user access is restricted via role based security privileges defined within the access control system. Database administrative access is restricted to user accounts accessible by authorized personnel.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Databases are configured to enforce password requirements that include: • Password length (minimum and maximum) • Password reset • Multi-factor authentication (MFA) • Complexity Database audit logging settings are enabled. Database audit logs are maintained and are reviewed as needed.
	Application	
		Application user access is restricted via role based security privileges defined within the access control system. Application administrative access is restricted to user accounts accessible by authorized personnel. The application is configured to enforce password requirements that include: • Password length (minimum and maximum) • Password reset • Multi-factor authentication (MFA) • Complexity Application audit logging settings are in place. Application audit policy settings are in place. Application audit logs are maintained and reviewed as-needed. The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel. Data coming into the environment is secured and monitored through the use of firewalls. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. Critical data is stored in encrypted format using software supporting the AES, SHA, RSA, DES, and ECC. Encryption keys are protected during generation, storage, use, and destruction. Control self-assessments that include, but are not limited to, quarterly logical access reviews, and annual backup restoration tests are performed. Logical access to systems is approved and granted to an employee as a component of the hiring process.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Logical access to systems is revoked as a component of the termination process.
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.
		Logical access to systems is revoked as a component of the termination process.
		Control self-assessments that include, but are not limited to, quarterly logical access reviews, and annual backup restoration tests are performed.
		Privileged access to sensitive resources is restricted to authorized personnel.
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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.
		Logical access to systems is revoked as a component of the termination process.
		Privileged access to sensitive resources is restricted to authorized personnel.
		Control self-assessments that include, but are not limited to, quarterly logical access reviews, and annual backup restoration tests are performed.
		Control self-assessments that include, but are not limited to, quarterly logical access reviews, and annual backup restoration tests are performed.
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.	This criteria is managed by the subservice organization. Please refer to the ‘Subservice Organizations’ section above for the controls managed by the subservice organization.
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.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.
		Policies and procedures are in place for removal of media storing critical data or software.
		Logical access to systems is revoked as a component of the termination process.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Data coming into the environment is secured and monitored through the use of firewalls.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	SSL and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. Transmission of digital output beyond the boundary of the system is encrypted. Logical access to stored data is restricted to authorized personnel. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new signatures are available. The antivirus software is configured to scan workstations on an ongoing basis. Critical data is stored in encrypted format using software supporting the AES, SHA, RSA, DES, and ECC. Policies and procedures are in place for removal of media storing critical data or software. Logical access to stored data is restricted to authorized personnel. The ability to recall backed up data is restricted to authorized personnel. The entity secures its environment a using multi-layered defense approach that includes firewalls, an IDS, and antivirus software. SSL and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches. Critical data is stored in encrypted format using software supporting the AES, SHA, RSA, DES, and ECC. Backup media is stored in an encrypted format. Transmission of digital output beyond the boundary of the system is encrypted. Use of removable media is prohibited by policy except when authorized by management. The ability to migrate changes into the production environment is restricted to authorized and appropriate users. File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment. Documented change control policies and procedures are in place to guide personnel in the change management process. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new signatures are available. The antivirus software is configured to scan workstations on an ongoing basis.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches. File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment. Use of removable media is prohibited by policy except when authorized by management. A firewall is in place to filter unauthorized inbound network traffic from the internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Ongoing internal vulnerability scans are performed and monthly summary reports are generated. Penetration tests are performed on at least an annual basis and remedial actions are taken where necessary.
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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches. File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment. A firewall is in place to filter unauthorized inbound network traffic from the internet.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new signatures are available. The antivirus software is configured to scan workstations on an ongoing basis. Use of removable media is prohibited by policy except when authorized by management.
	Network	
		Network audit logging settings are in place. Network audit logs are maintained and are reviewed as needed.
	Operating System (Application, Web, and Database Servers)	
		Operating systems are configured to enforce lockout requirements. Operating system audit logging settings are in place. Operating system audit logs are maintained and are reviewed as needed.
	Database	
		Database audit logging settings are enabled. Database audit logs are maintained and are reviewed as needed.
	Application	
		Application audit policy settings are in place. Application audit logs are maintained and reviewed as-needed. Management reviews reports on an annual basis summarizing incident, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes. Management monitors the effectiveness of detection tools and controls implemented within the environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. The incident response and escalation procedures are reviewed at least annually for effectiveness. The incident response policies and procedures define the classification of incidents based on its severity. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. Identified incidents are reviewed, monitored and investigated by the computer security incident response team. Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.
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.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented. Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. The actions taken to address identified security incidents are documented and communicated to affected parties. Documented response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Critical security incidents that result in a service/business operation disruption are communicated to those affected. Resolution of incidents are documented within the ticket and communicated to affected users. Remediation actions taken for security incidents are documented within the ticket and communicated to affected users. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. The risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Transfer the risk • Accept the risk The incident response and escalation procedures are reviewed at least annually for effectiveness. Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Updating software • Installing patches • Removing unauthorized access • Changing configurations Data backup and restore procedures are in place to guide personnel in performing backup activities. Control self-assessments that include, but are not limited to, quarterly logical access reviews, and annual backup restoration tests are performed. Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution. After critical incidents are investigated and addressed, lessons learned are documented and analyzed, and incident response plans and recovery procedures are updated based on the lessons learned. A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. The disaster recovery plan is tested on an annual basis. The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Change Management		
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	Documented change control policies and procedures are in place to guide personnel in the change management process. System changes are communicated to both affected internal and external users. Access to implement changes in the production environment is restricted to authorized IT personnel. System changes are authorized and approved by management prior to implementation. Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed. Development and test environments are physically and logically separated from the production environment. System change requests are documented and tracked in a ticketing system. Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation. System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. System changes implemented for remediating incidents follow the standard change management process. Information security policies and procedures document the baseline requirements for configuration of IT systems and tools. Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Identified risks are rated using a risk evaluation process and ratings are approved by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process. The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process. Identified third-party risks are rated using a risk evaluation process and ratings are approved by management. The entity's third-party agreement outlines and communicates: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment. A formal risk assessment is performed on an annual basis to identify threats from third parties that could impair system commitments and requirements.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE’s examination of the controls of September 10, 2020 was limited to the Trust Services Criteria, related criteria and control activities specified by the management of September 10, 2020 and did not encompass all aspects of September 10, 2020’s operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client’s knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity’s internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization’s controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity’s assertions; and
- Determine whether the service organization’s controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria.