Engagedly Inc.
Type 2 SOC 2
2020

REPORT ON ENGAGEDLY INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY AND CONFIDENTIALITY

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

October 1, 2019 to November 30, 2020

Table of Contents

SECTION 1 ASSERTION OF ENGAGEDLY INC. MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 3

SECTION 3 ENGAGEDLY INC.'S DESCRIPTION OF ITS REAL-TIME PERFORMANCE MANAGEMENT SAAS SERVICES SYSTEM THROUGHOUT THE PERIOD OCTOBER 1, 2019 TO NOVEMBER 30, 2020 7

OVERVIEW OF OPERATIONS 8
Company Background 8
Description of Services Provided 8
Principal Service Commitments and System Requirements 8
Components of the System 9
Boundaries of the System 13
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING 13
Control Environment 13
Risk Assessment Process 15
Information and Communications Systems 15
Monitoring Controls 16
Changes to the System Since the Last Review 16
Incidents Since the Last Review 16
Criteria Not Applicable to the System 16
Subservice Organization Controls 17
COMPLEMENTARY USER ENTITY CONTROLS 18
TRUST SERVICE CATEGORIES 18

SECTION 4 TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS 20

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS 21
CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION 22
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY 22
ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY 122

SECTION 1

ASSERTION OF ENGAGEDLY INC. MANAGEMENT

ASSERTION OF ENGAGEDLY INC. MANAGEMENT

December 5, 2020

We have prepared the accompanying description of Engagedly Inc.'s ('Engagedly' or 'the Company') Real-Time Performance Management SaaS Services System titled "Engagedly Inc.'s Description of Its Real-Time Performance Management SaaS Services System throughout the period October 1, 2019 to November 30, 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 Real-Time Performance Management SaaS Services System that may be useful when assessing the risks arising from interactions with Engagedly's system, particularly information about system controls that Engagedly has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (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*).

Engagedly uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Engagedly, to achieve Engagedly's service commitments and system requirements based on the applicable trust services criteria. The description presents Engagedly's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Engagedly'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 and operating effectively are necessary, along with controls at Engagedly, to achieve Engagedly's service commitments and system requirements based on the applicable trust services criteria. The description presents Engagedly's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Engagedly's controls.

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

a. the description presents Engagedly's Real-Time Performance Management SaaS Services System that was designed and implemented throughout the period October 1, 2019 to November 30, 2020, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2019 to November 30, 2020, to provide reasonable assurance that Engagedly'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 and user entities applied the complementary controls assumed in the design of Engagedly's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period October 1, 2019 to November 30, 2020, to provide reasonable assurance that Engagedly's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Engagedly's controls operated effectively throughout that period.

Sri Chellappa
President
Engagedly Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Engagedly Inc.

Scope

We have examined Engagedly's accompanying description of its Real-Time Performance Management SaaS Services System titled "Engagedly Inc.'s Description of Its Real-Time Performance Management SaaS Services System throughout the period October 1, 2019 to November 30, 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 and operating effectiveness of controls stated in the description throughout the period October 1, 2019 to November 30, 2020, to provide reasonable assurance that Engagedly's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality (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*).

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

Engagedly 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 Engagedly's service commitments and system requirements were achieved. Engagedly has provided the accompanying assertion titled "Assertion of Engagedly Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Engagedly 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
- 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 Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects:

a. the description presents Engagedly's Real-Time Performance Management SaaS Services System that was designed and implemented throughout the period October 1, 2019 to November 30, 2020, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2019 to November 30, 2020, to provide reasonable assurance that Engagedly'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 and user entities applied the complementary controls assumed in the design of Engagedly's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period October 1, 2019 to November 30, 2020, to provide reasonable assurance that Engagedly's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Engagedly'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 Engagedly, user entities of Engagedly's Real-Time Performance Management SaaS Services System during some or all of the period October 1, 2019 to November 30, 2020, business partners of Engagedly subject to risks arising from interactions with the Real-Time Performance Management SaaS Services 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 organization, 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
December 5, 2020

SECTION 3

ENGAGEDLY INC.'S DESCRIPTION OF ITS REAL-TIME PERFORMANCE MANAGEMENT SAAS SERVICES SYSTEM THROUGHOUT THE PERIOD OCTOBER 1, 2019 TO NOVEMBER 30, 2020

OVERVIEW OF OPERATIONS

Company Background

Engagedly was founded in February 2015 with its headquarters in St. Louis, Missouri. Engagedly's mission is to improve workplaces to better align employees' motivation to organizational objectives. Engagedly believes that as organizations become more digital and networked, the traditional performance and talent management system approaches fall short of optimizing their talent pool. Engagedly's unique approach to performance enablement using an engagement and employee first mentality has proven more effective in actively galvanizing the employees for a common purpose.

Industries served by Engagedly include Financial Services, Telecommunications, Legal Services, Advertising, Manufacturing, Healthcare, Retail, and Educational institutions.

Description of Services Provided

Engagedly is a cloud platform for progressive performance management and employee engagement built for organizations with visionary leadership. With Engagedly's gamification, engagement, and continuous improvement-based approach, organizations can alight, motivate, engage, and optimize employee performance.

As part of the platform, Engagedly provides holistic, employee first centric modules that include:

- Easy to use performance reviews
- Ongoing check-ins, facilitating employee-manager discussions
- Goals/Objectives/Key Results for agile goal alignment
- 360-degree feedback for employee development
- Agile learning
- Gamification based employee recognition
- Employee surveys
- Social collaboration tools

Principal Service Commitments and System Requirements

Engagedly designs its processes and procedures related to its cloud platform to meet its objectives for its services. Those objectives are based on the service commitments that Engagedly makes to user entities, and the financial, operational, and compliance requirements that Engagedly has established for the services.

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

- Open Web Application Security Project (OWASP) centric security principles within the fundamental designs of the cloud platform 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
- Single sign on centralized session and user authentication

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

Components of the System

Infrastructure

Primary infrastructure used to provide Engagedly's Real-Time Performance Management SaaS Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Elastic Cloud Compute (EC2)	Platform as a Service (PaaS)	Amazon elastic compute cloud virtual computer
Relational Database Service (RDS)		Relational Database
Route53		Domain Name System (DNS)
S3		File Storage System
Cloud Front		Content Delivery System

Software

Primary software used to provide Engagedly's Real-Time Performance Management SaaS Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Postgres	AWS Service	Database
Redis		Persistent Data Storage
ElasticSearch		Search and Aggregate Services
CLAM Antivirus (AV)	Linux	Antivirus
Nginx		Webserver
Wazuh		File Monitoring and Host-based Intrusion Detection System (HIDS)
Jumpcloud	Ubuntu	Directory as a service for managing access to systems

People

Engagedly has a staff of approximately 100 employees organized in the following functional areas:

- *Corporate*: Executives, operations staff, and company administrative support staff, such as legal, internal audit, accounting, finance, human resources (HR)
- *Information Technology (IT):* Help desk, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support
    - The help desk group provides technical assistance to the platform users
    - The software development staff develops and maintains the custom software for Engagedly
    - The information security staff supports the platform indirectly by monitoring internal and external security threats and maintaining current antivirus software
    - The information security staff maintains the inventory of IT assets

Data

Data, as defined by Engagedly, constitutes the following:

- Client's User data
- Transaction data
- Output reports
- System files
- Application files
- Error logs

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 Engagedly policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Engagedly team member.

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. Refer to the subservice organization table below for detailed controls.

Logical Access

Engagedly 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. In the event incompatible responsibilities cannot be segregated, Engagedly implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and approved vendor personnel sign on to the Engagedly network using a Jump Cloud user Identification (ID) and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Jump Cloud. Passwords must conform to defined password standards and are enforced through parameter settings in Jump Cloud. 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.

Authorized employees accessing the system from outside the Engagedly network are required to use the virtual private network (VPN) authentication system on their workstations. Vendor personnel are not permitted to access the system.

Customer employees' access Engagedly's Real-Time Performance Management SaaS services through the Internet using the Transport Layer Security (TLS) encryption functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the application using the application administration account.

Upon hire, employees are assigned to a position in the HR management system. On the day of the employees' start date, HR requests the IT Helpdesk create a user ID and access rules. Access rules are predefined based on 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 IT Help Desk and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the Chief Information Security Officer (CISO). As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

On a quarterly basis, HR creates a report of active and terminated employees. The IT Help Desk uses these reports to suspend user IDs and delete roles from IDs belonging to terminated employees.

On a quarterly basis, managers review roles assigned to their direct reports. Role lists are generated by the internal audit team. Managers review the lists and indicate the required changes in the change management system. The record is routed back to the internal audit team for processing. The internal audit team identifies any records not returned within two weeks and follows up with the manager. As part of this process, the CISO reviews employees with access to privileged roles and requests modifications through the change management system.

Computer Operations - Backups

Customer data is backed up and monitored by operations 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.

Backup infrastructure resides on private networks logically secured from other networks.

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.

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

- Disk storage
- Backup storage
- Network bandwidth

Engagedly 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 Engagedly system owners review proposed operating system patches to determine whether the patches are applied. Customers and Engagedly 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. Engagedly staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Engagedly 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.

Engagedly 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 Engagedly system owners review proposed operating system patches to determine whether the patches are applied. Customers and Engagedly 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. Engagedly 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 Engagedly. 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 Engagedly policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Engagedly. 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 Engagedly 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 through the use of leading VPN technology.

Boundaries of the System

The scope of this report includes the Real-Time Performance Management SaaS Services System performed in the St. Louis, Missouri and Bengaluru, India facilities.

This report does not include the cloud hosting services provided by AWS at the Northern Virginia Region 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 Engagedly's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Engagedly'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

Engagedly'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

Engagedly'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

Engagedly'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.

Engagedly'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

Engagedly'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. Engagedly'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

Engagedly's risk assessment process identifies and manages risks that could potentially affect Engagedly'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. Engagedly 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 Engagedly 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

Engagedly 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. Engagedly 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 Engagedly's Real-Time Performance Management SaaS system; as well as the nature of the components of the system result in risks that the criteria will not be met. Engagedly 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, Engagedly's 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 are an integral component of Engagedly'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 Engagedly 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. Additionally, meetings are held bi-annually in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues.

Specific information systems used to support Engagedly's Real-Time Performance Management SaaS Services 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. Engagedly'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

Engagedly'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 Engagedly'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 Engagedly'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 Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common/ Security and Confidentiality criterion were applicable to the Engagedly Real-Time Performance Management SaaS Services System.

Subservice Organization Controls

This report does not include the cloud hosting services provided by AWS at the Northern Virginia Region facilities.

Subservice Description of Services

AWS provides cloud hosting services to Engagedly by hosting, maintaining, and monitoring all critical entity data needed to support the in-scope system.

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

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, CC7.2	A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours.
		A badge access system controls access to and within the office facility.
		Personnel are assigned to predefined badge access security zones based on job responsibilities.
		The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.
		Privileged access to the badge access system was restricted to appropriate IT personnel.
		Access to the server room / data center is restricted to appropriate IT personnel.
		A video surveillance system is in place with footage retained for 30 days.
		Visitors to the facility and server room are required to be escorted by an authorized employee.
		Visitors to the facility and server room are required to sign a visitor log prior upon arrival.
		Physical access to systems is revoked as a component of the termination process.
		User access to the badge access system is reviewed at least quarterly.

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

- 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

Engagedly'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 Engagedly's services to be solely achieved by Engagedly control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Engagedly'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 Engagedly.
2. User entities are responsible for notifying Engagedly of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Engagedly 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 Engagedly services.
6. User entities are responsible for providing Engagedly with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Engagedly of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICE CATEGORIES

In-Scope Trust Services Criteria

Common Criteria (to the Security and Confidentiality Categories)
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.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control Activities Specified by the Service Organization

The applicable trust services criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Engagedly's description of the system. Any applicable trust services criteria that are not addressed by control activities at Engagedly are described within Section 4 and within the subservice organization and Criteria Not Applicable to the System sections above.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. 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.

SECTION 4

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

A-LIGN ASSURANCE's examination of the controls of Engagedly was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Engagedly and did not encompass all aspects of Engagedly'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.

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**	**Test Applied by the Service Auditor**	**Test Results**
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.	Inspected the employee handbook, information security policy and the entity's intranet to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, and the employee handbook.	No exceptions noted.
		An employee handbook is documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook was documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Upon hire, personnel are required to sign a non-disclosure agreement.	Inspected the signed non-disclosure agreement for a sample of new hires to determine that upon hire, personnel were required to sign a non-disclosure agreement.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Sanction procedures, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the employee handbook to determine that sanction procedures, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the anonymous hotline reporting section on the Engagedly website to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	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.	Executive management roles and responsibilities are documented and reviewed annually.	Inspected the executive management job descriptions including revision dates to determine that executive management roles and responsibilities were documented and reviewed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart and internal controls matrix to determine that executive management maintained independence from those that operate the key controls within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the ISMS Internal Control Review meeting minutes to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
			Inspected the ISMS Internal Control Review meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A third-party performs an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls within the environment.	Inspected the entity's completed attestation report to determine that a third-party performed an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls within the environment.	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.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.	Inspected the revision history of the organizational chart to determine that executive management reviewed the organizational chart annually and made updates to the organizational structure and lines of reporting, if necessary.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job roles to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	No exceptions noted.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, internal controls matrix, and job description for a sample of job roles to determine that executive management established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.	Inspected the job description for a sample of job roles to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the supplier security policy to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment and vendor review form for a sample of vendors to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
		Executive management considers the roles and responsibilities performed by third-parties when documenting the organizational chart and defining job descriptions.	Inspected the organizational chart and the job description for a sample of job roles to determine that executive management considered the roles and responsibilities performed by third-parties when documenting the organizational chart and defining job descriptions.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook and the security awareness training policy to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the interview cycle and interview feedback for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring.	Inspected the job description for a sample of job roles, and interview cycle and interview feedback for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring.	No exceptions noted.
		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.	Inspected the organizational chart and job opening postings to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the learning and development tracking sheet to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the training completion tracker for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the information security and awareness training materials to determine that executive management created a training program for its employees.	No exceptions noted.
		The entity assesses training needs on an annual basis.	Inspected the training survey to determine that the entity assessed the training needs on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
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.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook and the security awareness training policy to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job roles to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions annually and made updates, if necessary.	No exceptions noted.
		Sanction procedures, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the employee handbook to determine that sanction procedures, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 intranet.	Inspected the information security policy and the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inspected the input validation requirements to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
		Data flow diagram are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagram to determine that data flow diagram was documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the file integrity monitoring (FIM) configurations, intrusion detection system (IDS) configurations, encryption methods and configurations and virtual private network (VPN) authentication configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		The entity's policies and procedures, and employee handbook are made available to employees through the entity's intranet.	Inspected the entity's intranet to determine that the entity's policies and procedures, and employee handbook were made available to employees through the entity's intranet.	No exceptions noted.
		Upon hire, employees are required complete information security and awareness training.	Inspected the information security and awareness training completion tracker for a sample of new hires to determine that upon hire, employees were required complete information security and awareness training.	No exceptions noted.
		Current employees are required to complete information security and awareness training on an annual basis.	Inspected the information security and awareness training completion tracker for a sample of current employees to determine that current employees were required to complete information security and awareness training on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	No exceptions noted.
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the anonymous hotline reporting section on the Engagedly website to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's intranet.	Inspected the incident management process and procedures and the entity's intranet to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and made available to employees through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's organizational level meetings.	Inspected the organizational level meeting minutes to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's organizational level meetings.	No exceptions noted.
		Management tracks and monitors compliance with information security and awareness training requirements.	Inspected the information security and awareness training completion tracker to determine that management tracked and monitored compliance with information security and awareness training requirements.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.	Inspected the third-party agreement template to determine that the entity’s third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
			Inspected the third-party agreement for a sample of third-parties to determine that the entity’s third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		The entity's third-party agreement communicates the system commitments and requirements of third-parties.	Inspected the third-party agreement template to determine that the entity’s third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.
		The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third-parties.	Inspected the third-party agreement template to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third-parties.	No exceptions noted.
			Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third-parties.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the customer agreement template to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
			Inspected the agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via website notices.	Observed the entity's website to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users and customers via website notices.	No exceptions noted.
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the anonymous hotline reporting section on the Engagedly website to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		The entity communicates to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	Inspected the third-party agreement template to determine that the entity communicated to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	No exceptions noted.
		Changes to commitments and requirements relating to confidentiality are communicated to third-parties, external users, and customers via website notices.	Observed the entity's website to determine that changes to commitments and requirements relating to confidentiality were communicated to third-parties, external users and customers via website notices.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Inspected the organizational chart and organizational level meeting minutes to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk assessment and management policy and procedure to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
			Inspected the completed risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the documented key performance indicators to determine that the entity defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the documented key performance indicators and organizational level meeting minutes to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the organizational-level management meeting minutes and the entity`s sales and financial plan to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the organizational-level management meeting minutes and the entity`s sales and financial plan to determine that entity strategies, objectives and budgets were assessed on an annual basis.	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.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment and management policy and procedure to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.	Inspected the risk assessment and management policy and procedure to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's risk assessment process includes: • Identifying and assessing the impact of the threats to those information assets • 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	Inspected the risk assessment and management policy and procedure to determine that the entity's risk assessment process included: • Identifying and assessing the impact of the threats to those information assets • 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	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that the entity's risk assessment process included: • Identifying and assessing the impact of the threats to those information assets • 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	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment and management policy and procedure to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment and management policy and procedure to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.
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.	Inspected the completed risk assessment to determine that, on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		As part of management's assessment of fraud risks, management considers key fraud factors such as opportunity for unauthorized access or use of data.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considers key fraud factors such as opportunity for unauthorized access or use of data.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policy and procedure to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policy and procedure to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policy and procedure to determine that changes in vendor and third-party relationships were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the completed risk assessment to determine that changes in vendor and third-party relationships were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Inspected the CloudWatch configurations, the antivirus software dashboard console and scan configurations, IDS configurations, FIM configurations, and EC2 security group configurations to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the entity policies and procedures to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
			Inspected the ISMS Internal Control Review meeting minutes to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the ISMS Internal Control Review meeting minutes to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access reviews are performed on a quarterly basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of quarters to determine that logical access reviews were performed on a quarterly basis.	No exceptions noted.
		Backup restoration tests are performed on a quarterly basis.	Inspected the backup restoration test results for a sample of quarters to determine that backup restoration tests were performed on a quarterly basis.	No exceptions noted.
		External vulnerability scans are performed quarterly, and remedial actions are taken where necessary.	Inspected the vulnerability scan result for a sample of quarters to determine that external vulnerability scans were performed quarterly, and remedial actions were taken where necessary.	No exceptions noted.
		Evaluations of policies, controls, systems, tools, applications, and third-parties for effectiveness and compliance is required annually.	Inspected the revision history of entity policies and procedures to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required annually.	No exceptions noted.
			Inspected the ISMS Internal Control Review meeting minutes to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the entity's completed attestation report to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required annually.	No exceptions noted.
			Inspected the completed risk assessment to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required annually.	No exceptions noted.
			Inspected the security program charter to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required annually.	No exceptions noted.
		Management reviews the frequency of compliance evaluations annually and adjusts it based on changes to the environment and operational performance.	Inspected the ISMS Internal Control Review meeting minutes to determine that management reviewed the frequency of compliance evaluations annually and adjusted it based on changes to the environment and operational performance.	No exceptions noted.
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A third-party performs an independent assessment of the controls environment annually to assess the effectiveness of controls within the environment.	Inspected the entity's completed attestation report to determine that a third-party performed an independent assessment of the controls environment annually to assess the effectiveness of controls within the environment.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	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.	Vulnerabilities, deviations and control gaps identified from the compliance and risk assessments are communicated to those parties responsible for taking corrective actions.	Inspected the completed risk assessment to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of vulnerabilities identified from a vulnerability scan to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Vulnerabilities, deviations and control gaps identified from the compliance and risk assessments are documented, investigated, and addressed.	Inspected the completed compliance, control and risk assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of vulnerabilities identified from a vulnerability scan to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the ISMS Internal Control Review meeting minutes to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Inspected the completed risk assessment to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	No exceptions noted.
		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.	Inspected the completed risk to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of vulnerabilities identified from a vulnerability scan to determine controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Prior to the development and implementation of internal controls into the environment, management considers the complexity, nature, and scope of its operations.	Inspected the internal controls matrix to determine that prior to the development and implementation of internal controls into the environment, management considers the complexity, nature and scope of its operations.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the ISMS Internal Control Review meeting minutes to determine that prior to the development and implementation of internal controls into the environment, management considers the complexity, nature and scope of its operations.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Inspected the internal controls matrix to determine that management 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.	No exceptions noted.
		Organizational and information security policies and procedures are documented and made available to employee's through the entity's intranet.	Inspected the information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's intranet.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats	Inspected the internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
		Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	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.	Organizational and information security policies and procedures are documented and made available to employee's through the entity's intranet.	Inspected the information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the information security and incident response policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the information security policies, incident response and procedures and internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample of job roles and the entity's intranet website to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		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.	Inspected the organizational and information security policies and procedures and internal controls matrix to determine that process owners and management operated the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	No exceptions noted.
		Effectiveness of the internal controls implemented within the environment are evaluated annually.	Inspected management meeting minutes to determine that effectiveness of the internal controls implemented within the environment were evaluated annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Chief Information Security Officer regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
	JumpCloud			
		JumpCloud user access is restricted via role based security privileges defined within the access control system.	Inspected the JumpCloud user listing and access rights to determine that JumpCloud user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		JumpCloud administrative access is restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer • Junior Software Developer	Inquired of the Chief Information Security Officer regarding administrative access to determine that JumpCloud administrative access was restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer • Junior Software Developer	No exceptions noted.
			Inspected the JumpCloud administrator listing and access rights to determine that JumpCloud administrative access was restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer • Junior Software Developer	No exceptions noted.
		JumpCloud is configured to enforce password requirements that include: • Password history • Password length • Complexity	Inspected the JumpCloud password settings to determine that JumpCloud was configured to enforce password requirements that included: • Password history • Password length • Complexity	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		JumpCloud account lockout settings are in place that include: • Account lockout threshold	Inspected the JumpCloud account lockout settings to determine that JumpCloud account lockout settings were in place that included: • Account lockout threshold	No exceptions noted.
		JumpCloud automatically logs the user out of the account after 1 hour idle session.	Inspected the JumpCloud log out settings to determine that JumpCloud automatically logs the user out of the account after 1 hour idle session.	No exceptions noted.
		JumpCloud audit logging settings are in place that include: • Log streams • Last event time	Inspected the JumpCloud audit logging settings and example JumpCloud audit log extracts to determine that JumpCloud audit logging configurations were in place that included: • Log streams • Last event time	No exceptions noted.
		JumpCloud audit logs are maintained and reviewed as-needed.	Inquired of the Chief Information Security Officer regarding JumpCloud audit logs to determine that JumpCloud audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected example JumpCloud audit log extracts to determine that JumpCloud audit logs were maintained and reviewed as-needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	AWS			
		AWS user access is restricted via role based security privileges defined within the access control system.	Inspected the user listing to determine that AWS user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		AWS administrative access is restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer • Junior Software Developer	Inquired of the Chief Information Security Officer regarding administrative access to determine that AWS administrative access was restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer • Junior Software Developer	No exceptions noted.
			Inspected the administrator user listing and access rights to determine that AWS administrative access was restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer • Junior Software Developer	No exceptions noted.
		AWS is configured to use SSO authentication through Jumpcloud.	Inspected the JumpCloud authentication settings to determine that AWS was configured to use SSO authentication through Jumpcloud.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		AWS audit logs are maintained and reviewed as-needed.	Inquired of the Chief Information Security Officer regarding AWS audit logs to determine that AWS audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected example AWS audit log extracts to determine that AWS audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Operating System (Linux)			
		Operating system user access is restricted via role based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Operating system administrative access is restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer	Inquired of the Chief Information Security Officer regarding administrative access to determine that operating system administrative access was restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the operating system administrator user listing and access rights to determine that operating system administrative access was restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer	No exceptions noted.
		The operating system is configured to use SSO authentication through Jumpcloud.	Inspected the JumpCloud authentication settings to determine that the operating system was configured to use SSO authentication through Jumpcloud.	No exceptions noted.
		Operating system account lockout settings are in place that include: • LOGIN_RETRIES • LOGIN_TIMEOUT	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included: • LOGIN_RETRIES • LOGIN_TIMEOUT	No exceptions noted.
		Operating system audit logging settings are in place that include: • /Var/log/audit	Inspected the operating system audit logging settings and example operating system audit log extracts to determine that operating system audit logging configurations were in place that included: • /Var/log/audit	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Operating system audit logs are maintained and reviewed as-needed.	Inquired of the Chief Information Security Officer regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected example operating system audit log extracts to determine that operating system audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Database (Postgres)			
		Database user access is restricted via role based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Database administrative access is restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer	Inquired of the Chief Information Security Officer regarding administrative access to determine that database administrative access was restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the database administrator listing and access rights to determine that database administrative access was restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer	No exceptions noted.
		The database is configured to use SSO authentication through Jumpcloud.	Inspected the JumpCloud authentication settings to determine that the database was configured to use SSO authentication through Jumpcloud.	No exceptions noted.
		Database audit logs are maintained and reviewed as-needed.	Inquired of the Chief Information Security Officer regarding database audit logs to determine the database audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected example database audit log extracts to determine that database audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Application (Engagedly Platform)			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application administrative access is restricted to user accounts accessible by the following personnel: • Director of HR • VP of Professional Services • People Specialist • Chief Executive Officer • President • Chief Technology Officer	Inquired of the Chief Information Security Officer regarding administrative access to determine that application administrative access was restricted to user accounts accessible by the following personnel: • Director of HR • VP of Professional Services • People Specialist • Chief Executive Officer • President • Chief Technology Officer	No exceptions noted.
			Inspected the application administrator user listing and access rights to determine that application administrative access was restricted to user accounts accessible by the following personnel: • Director of HR • VP of Professional Services • People Specialist • Chief Executive Officer • President • Chief Technology Officer	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The application is configured to enforce password requirements that include: • Password history • Password length • Complexity	Inspected the application password settings to determine that application was configured to enforce password requirements that included: • Password history • Password length • Complexity	No exceptions noted.
		Application account lockout settings are in place that include: • Max Invalid password attempt • Lock user on invalid password attempt • Time-out session after	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: • Max Invalid password attempt • Lock user on invalid password attempt • Time-out session after	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Chief Information Security Officer regarding application audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example application audit log extracts to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Remote Access (AWS Client VPN)			
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		The ability to administer VPN access is restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer	Inquired of the Chief Information Security Officer regarding administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by the following personnel: • Full-Stack Developer • Chief Technology Officer	No exceptions noted.
		VPN users are authenticated via multi-factor authentication (username, password, and SSH Key) prior to being granted remote access to the system.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication (username, password, and SSH Key) prior to being granted remote access to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the demilitarized zone (DMZ) settings to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
		Data coming into the environment is secured and monitored through the use of firewalls and an IDS.	Inspected the network diagram, IDS configurations, and firewall rule sets to determine that data coming into the environment was secured and monitored through the use of firewalls and an IDS.	No exceptions noted.
		A DMZ is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Stored passwords are encrypted.	Inspected the encryption configurations for stored passwords to determine that stored passwords were encrypted.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the advanced encryption standards (AES)-256.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES-256.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Encryption keys are protected during generation, storage, use, and destruction.	Inspected the encryption policies and procedures to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		The entity restricts access to its environment using the following mechanisms: • Classifying data (e.g. Public, private, restricted, etc.) • Port restrictions (via firewall rule settings) • Access protocol restrictions (via firewall rule settings) • User identification • Digital certifications	Inspected the data classification policies and procedures, listings of users with access to the network, operating system, database and application, firewall rule sets and digital certificates to determine that the entity restricted access to its environment using the following mechanisms: • Classifying data • Port restrictions • Access protocol restrictions • User identification • Digital certifications	No exceptions noted.
		Logical access reviews are performed on a quarterly basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of quarters to determine that logical access reviews were performed on a quarterly basis.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Chief Information Security Officer regarding new hire access to systems to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Chief Information Security Officer regarding terminated employee revocation to systems to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
			Inspected the termination procedures, user access listings and termination checklist for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Chief Information Security Officer regarding new hire access to systems to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Chief Information Security Officer regarding terminated employee revocation to systems to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, user access listings and termination checklist for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Logical access reviews are performed on a quarterly basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of quarters to determine that logical access reviews were performed on a quarterly basis.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Chief Information Security Officer regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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, considering 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.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Chief Information Security Officer regarding new hire access to systems to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Chief Information Security Officer regarding terminated employee revocation to systems to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, user access listings and termination checklist for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Chief Information Security Officer regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed on a quarterly basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review for a sample of quarters to determine that logical access reviews were performed on a quarterly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	JumpCloud			
		JumpCloud user access is restricted via role based security privileges defined within the access control system.	Inspected the JumpCloud user listing and access rights to determine that JumpCloud user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
	AWS			
		AWS user access is restricted via role based security privileges defined within the access control system.	Inspected the user listing and access rights to determine that AWS user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
	Operating System (Linux)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Database (Postgres)			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Application (Engagedly Platform)			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
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 criterion is the responsibility of the subservice organization. Refer to the subservice organization section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
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.	Inspected the hardware sanitation policy to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		Data that is no longer required for business purposes is rendered unreadable.	Inquired of the Chief Information Security Officer regarding data disposal requests to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the data disposal and destruction policies and procedures to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the service ticket for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that data that was no longer required for business purposes was rendered unreadable.	Testing of this control activity disclosed that there were no requests to dispose of data, purge a system, or physically destroy a system during the review period.
		Policies and procedures are in place for removal of media storing critical data or software.	Inspected the removable media policies and procedures to determine policies and procedures were in place for removal of media storing critical data or software.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		VPN and TLS encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN and TLS encryption technologies were used for defined points of connectivity.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication (username, password, and SSH Key) prior to being granted remote access to the system.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication (username, password, and SSH Key) prior to being granted remote access to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Chief Information Security Officer regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
			Inspected the firewall rule sets for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IDS is configured to notify personnel upon intrusion detection.	Inspected an IDS log alert notification to determine that the IDS is configured to notify personnel upon intrusion detection.	No exceptions noted.
		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.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations daily for active scans and weekly for full scans.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations daily for active scans and weekly for full scans.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the AES-256.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES-256.	No exceptions noted.
		A DMZ is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
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.	Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Chief Information Security Officer regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		The ability to recall backed up data is restricted to authorized personnel.	Inquired of the Chief Information Security Officer regarding the ability to recall backed up data to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
			Inspected the list of users with the ability to recall backup media from the third-party storage facility to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity secures its environment a using multi-layered defense approach that includes firewalls, an IDS, antivirus software and a DMZ**.**	Inspected the network diagram, IDS configurations, firewall rule sets, antivirus settings and DMZ settings to determine that the entity secured its environment a using multi-layered defense approach that included firewalls, an IDS, antivirus software and a DMZ.	No exceptions noted.
		VPN, TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inspected the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the firewall rule sets for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IDS is configured to notify personnel upon intrusion detection.	Inspected an example IDS alert notification to determine that the IDS is configured to notify personnel upon intrusion detection.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the AES-256.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES-256.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the encryption configurations for an example backup media to determine that backup media was stored in an encrypted format.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**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.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Chief Information Security Officer regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		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.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations daily for active scans and weekly for full scans.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations daily for active scans and weekly for full scans.	No exceptions noted.
		Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment.	Inspected the vulnerability scan process policies and procedures to determine that information assets, software, hardware, tools, and applications introduced into the environment were scanned for vulnerabilities and malware prior to implementation into the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Management has defined configuration standards in the information security policies and procedures.	Inspected the information security policy to determine that management had defined configuration standards in the information security policies and procedures.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software, an example log extract from the IDS and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IDS is configured to notify personnel upon intrusion detection.	Inspected an example IDS log alert notification to determine that the IDS is configured to notify personnel upon intrusion detection.	No exceptions noted.
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the firewall rule sets for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		External vulnerability scans are performed quarterly, and remedial actions are taken where necessary.	Inspected the vulnerability scan result for a sample of quarters to determine that external vulnerability scans were performed quarterly, and remedial actions were taken where necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Penetration tests are performed on an annual basis and remedial actions are taken where necessary.	Inspected the completed penetration test results to determine that penetration tests were performed on an annual basis and remedial actions were taken where necessary.	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.	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.	Inspected the incident management policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software, an example log extract from the IDS and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected an example IDS alert notification to determine that the IDS is configured to notify personnel upon intrusion detection**.**	No exceptions noted.
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
			Inspected the firewall rule sets for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
			Inspected the antivirus settings for a sample of workstations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations daily for active scans and weekly for full scans.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations daily for active scans and weekly for full scans.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Jumpcloud			
		JumpCloud account lockout settings are in place that include: • Account lockout threshold	Inspected the JumpCloud account lockout settings to determine that JumpCloud account lockout settings were in place that included: • Account lockout threshold	No exceptions noted.
		JumpCloud audit logging settings are in place that include: • Log streams • Last event time	Inspected the JumpCloud audit logging settings and example JumpCloud audit log extracts to determine that JumpCloud audit logging configurations were in place that included: • Log streams • Last event time	No exceptions noted.
		JumpCloud audit logs are maintained and reviewed as needed.	Inquired of the Chief Information Security Officer regarding JumpCloud audit logs to determine that JumpCloud audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example JumpCloud audit log extracts to determine that JumpCloud audit logs were maintained and reviewed as needed.	No exceptions noted.
	AWS			
		AWS audit logs are maintained and reviewed as needed.	Inquired of the Chief Information Security Officer regarding AWS audit logs to determine that AWS audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected example AWS audit log extracts to determine that AWS audit logs were maintained and reviewed as needed.	No exceptions noted.
	Operating System (Linux)			
		Operating system account lockout settings are in place that include: • LOGIN_RETRIES • LOGIN_TIMEOUT	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included: • LOGIN_RETRIES • LOGIN_TIMEOUT	No exceptions noted.
		Operating system audit logging settings are in place that include: • /Var/log/audit	Inspected the operating system audit logging settings and example operating system audit log extracts to determine that operating system audit logging configurations were in place that included: • /Var/log/audit	No exceptions noted.
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Chief Information Security Officer regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example operating system audit log extracts to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database (Postgres)			
		Database audit logs are maintained and reviewed as needed.	Inquired of the Chief Information Security Officer regarding database audit logs to determine that the database audit logs were maintained and reviewed as needed. Inspected example database audit log extracts to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted. No exceptions noted.
	Application (Engagedly Platform)			
		Application account lockout settings are in place that include: • Max Invalid password attempt • Lock user on invalid password attempt • Time-out session after Application audit logs are maintained and reviewed as needed.	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: • Max Invalid password attempt • Lock user on invalid password attempt • Time-out session after Inquired of the Chief Information Security Officer regarding application audit logs to determine that application audit logs were maintained and reviewed as needed. Inspected example application audit log extracts to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted. No exceptions noted. No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management monitors the effectiveness of detection tools and controls implemented within the environment.	Inspected management meeting minutes to determine that management monitors the effectiveness of detection tools and controls implemented within the environment.	No exceptions noted.
		Additional controls are implemented by the subservice organization. Refer to the subservice organization section above for additional details.	Not applicable.	Not applicable.
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.	Inspected the incident management policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response and escalation procedures are reviewed annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Chief Information Security Officer regarding incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	Testing of this control activity disclosed that no incidents occurred during the review period.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Chief Information Security Officer regarding incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of this control activity disclosed that no incidents occurred during the review period.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inquired of the Chief Information Security Officer regarding incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	Testing of this control activity disclosed that no incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.	Inquired of the Chief Information Security Officer regarding incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine that the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that identified incidents were 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.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were 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.	Testing of this control activity disclosed that no incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**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.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.
		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.	Inspected the incident management policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Chief Information Security Officer regarding incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of this control activity disclosed that no incidents occurred during the review period.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inquired of the Chief Information Security Officer regarding incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	Testing of this control activity disclosed that no incidents occurred during the review period.
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Chief Information Security Officer regarding incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	Testing of this control activity disclosed that no incidents occurred during the review period.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inquired of the Chief Information Security Officer regarding incidents to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of incidents to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	Testing of this control activity disclosed that no incidents occurred during the review period.
		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.	Inquired of the Chief Information Security Officer regarding incidents to determine that identified incidents were 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.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that identified incidents were 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.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were 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.	Testing of this control activity disclosed that no incidents occurred during the review period.
		The incident response and escalation procedures are reviewed annually for effectiveness.	Inspected the revision history of the incident management policies and procedures to determine that the incident response and escalation procedures were reviewed annually for effectiveness.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes.	Inspected the change management policies and procedures to determine that change management requests were required to be opened for incidents that required permanent fixes.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security, incident, and change management policies and procedures to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Backup restoration tests are performed on a quarterly basis.	Inspected the backup restoration test results for a sample of quarters to determine that backup restoration tests were performed on a quarterly basis.	No exceptions noted.
		On an annual basis, preventative and detective controls are evaluated and updated, as necessary.	Inspected the Information Security Management Systems (ISMS) Internal Control Review meeting minutes to determine that on an annual basis, preventative and detective controls were evaluated and updated, as necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the entity's completed attestation report to determine that on an annual basis, preventative and detective controls were evaluated and updated, as necessary.	No exceptions noted.
		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.	Inspected the business continuity and disaster recovery plans to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No exceptions noted.
		The disaster recovery plan is tested on an annual basis.	Inspected the completed disaster recovery test results to determine that the disaster recovery plan was tested on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests- CAB Members • Development-Change Implementor • Testing-Change Implementor • Implementation software change management group	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests- CAB Members • Development-Change Implementor • Testing-Change Implementor • Implementation software change management group	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Observed the change notification on the Engagedly website to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Chief Information Security Officer regarding access to implement changes in the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
			Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		Code change review meetings occur prior to deployment.	Inspected the Pre Development code change review meeting minutes to determine that code change review meetings occurred prior to deployment.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of infrastructure changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
			Inspected the supporting change ticket for a population of system patch changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting change ticket for a sample of application changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
		Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the change control software settings to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, QA and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
		Changes implemented into the production environment trigger an alert to affected users.	Inspected the change control software settings and an example alert to determine that changes implemented into the production environment triggered an alert to affected users.	No exceptions noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of infrastructure changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting change ticket for a population of system patch changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
			Inspected the supporting change ticket for a sample of application changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation.	Inspected the supporting change ticket for a sample of infrastructure changes to determine that back out procedures were documented within each change implementation to allow for rollback of changes when changes impair system operation.	No exceptions noted.
			Inspected the supporting change ticket for a population of system patch changes to determine that back out procedures were documented within each change implementation to allow for rollback of changes when changes impair system operation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting change ticket for a sample of application changes to determine that back out procedures were documented within each change implementation to allow for rollback of changes when changes impair system operation.	No exceptions noted.
		System changes are tested prior to implementation and types of testing performed depend on the nature of the change.	Inspected the supporting change ticket for a sample of infrastructure changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.	No exceptions noted.
			Inspected the supporting change ticket for a population of system patch changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.	No exceptions noted.
			Inspected the supporting change ticket for a sample of application changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System changes implemented to the production environment are evaluated for impact to the entity's objectives.	Inspected the supporting change ticket for a sample of infrastructure changes to determine that system changes implemented to the production environment were evaluated for impact to the entity's objectives.	No exceptions noted.
			Inspected the supporting change ticket for a population of system patch changes to determine that system changes implemented to the production environment were evaluated for impact to the entity's objectives.	No exceptions noted.
			Inspected the supporting change ticket for a sample of application changes to determine that system changes implemented to the production environment were evaluated for impact to the entity's objectives.	No exceptions noted.
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Inspected the risk assessment and management policy and procedure to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities.	No exceptions noted.
		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.	Inspected the risk assessment and management policy and procedure to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment and management policy and procedure to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment and management policy and procedure to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
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.	Inspected the supplier security policy and risk assessment policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the supplier security policy to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment and the review of third-party agreements and compliance to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the supplier security policy and risk assessment policies and procedures to determine that identified third-party risks were rated using a risk evaluation process and ratings are approved by management.	No exceptions noted.
			Inspected the completed risk assessment and the review of third-party agreements and compliance to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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	Inspected the third-party agreement template to determine that the entity's third-party agreement outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	No exceptions noted.
			Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.	Inspected the completed third-party attestation report for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.	Inspected the supplier security policy and risk assessment policies and procedures to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements.	No exceptions noted.
		The entity's third-party agreement outlines and communicates confidentiality commitments and requirements.	Inspected the third-party agreement template to determine that the entity's third-party agreement outlined and communicated confidentiality commitments and requirements.	No exceptions noted.
			Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated confidentiality commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management assesses the compliance of confidential commitments and requirements of third-parties annually.	Inspected the review of third-party agreements and compliance meeting minutes to determine that management assessed the compliance of confidential commitments and requirements of third-parties annually.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**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.	Documented confidential policies and procedures are in place that include the following: • Defining, identifying and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed	Inspected the confidentiality policies and procedures to determine that documented confidential policies and procedures were in place that included: • Defining, identifying and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed	No exceptions noted.
		An inventory log is maintained of assets with confidential data.	Inspected the inventory log to determine that an inventory log was maintained of assets with confidential data.	No exceptions noted.
		Confidential information is maintained in locations restricted to those authorized to access.	Inquired of the Chief Information Security Officer regarding confidential information access to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.
			Inspected the file access permissions for an example file marked as confidential to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Confidential information is protected from erasure or destruction during the specified retention period.	Inspected the confidentiality policies and procedures to determine that confidential information was protected from erasure or destruction during the specified retention period.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Documented data destruction policies and procedures are in place that include the following: • Identifying confidential information requiring destruction when the end of the retention period is reached • Erasing or destroying confidential information that has been identified for destruction	Inspected the data destruction policies and procedures to determine that documented data destruction policies and procedures were in place that included: • Identifying confidential information requiring destruction when the end of the retention period is reached • Erasing or destroying confidential information that has been identified for destruction	No exceptions noted.
		An inventory log is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged.	Inspected the inventory log to determine that an inventory log was maintained of assets with confidential data, and as confidential data met the retention period, the data was destroyed or purged.	No exceptions noted.
		The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed.	Inquired of the Chief Information Security Officer regarding data disposal requests to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the data disposal and destruction policies and procedures to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.
			Inspected the service ticket for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	Testing of this control activity disclosed that there were no requests to dispose of data, purge a system, or physically destroy a system during the review period.