

matillion

Matillion Limited

SOC 2 Type II

Independent Service Auditor's Report on Management's Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security

August 1, 2025 – July 31, 2026

ASCEND
AUDIT & ADVISORY

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701

TABLE OF CONTENTS

I. Independent Service Auditor's Report ____ *3*

Independent Service Auditor's Report ____ **4**

II. Information Provided by Matillion Limited ____ *8*

Assertion of Matillion Limited Service Organization Management ____ **9**

Description of Matillion's Platform System ____ **12**
- Company Overview ____ 12
- System Description ____ 18

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication ____ **22**
- Control Environment ____ 22
- Risk Assessment and Management ____ 29
- Monitoring ____ 29
- Information and Communication ____ 29
- User Control Considerations ____ 31

III. Information Provided by Ascend Audit & Advisory ____ *32*

Common Control Criteria – Security Category ____ **33**
- Control Environment ____ 33
- Information and Communication ____ 49
- Risk Assessment ____ 63
- Monitoring Activities ____ 79
- Control Activities ____ 85
- Logical and Physical Access Controls ____ 93
- System Operations ____ 110
- Change Management ____ 122
- Risk Mitigation ____ 129

I. Independent Service Auditor's Report

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701
www.ascendaudit.com

INDEPENDENT SERVICE AUDITOR'S REPORT

The Management Company of Matillion Limited
Two, New Bailey Street, Stanley Street
Salford M3 5GS, United Kingdom

Scope

We have examined Matillion Limited's ("Matillion", or "the Company") description of controls for its Matillion Platform (Matillion Data Loader, Change Data Capture, Matillion ETL, Data Productivity Cloud) System and related transactions throughout the period August 1, 2025 through July 31, 2026, 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 (With Revised Implementation Guidance – 2022)*(AICPA, Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period August 1, 2025 through July 31, 2026, to provide reasonable assurance that Matillion's service commitments and system requirements were achieved based on the trust service criterion for security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022),* in AICPA *Trust Services Criteria*.

Subservice Organizations

Matillion utilizes subservice organizations for the following services and applications:

Subservice Organizations	***Services and Applications***
Amazon Web Services (AWS)	Infrastructure-as-a-Service and cloud computing services
Google	Infrastructure-as-a-Service and enterprise applications
Microsoft – Azure including Dynamics 365	Cloud computing and enterprise applications
Atlassian	Source code and version control and software project management
Auth0	Authentication tools
Okta	Conditional multifactor authentication, access for SaaS applications
Oracle America (NetSuite)	Application hosting services
HiBob	Human Resources information system

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

Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls. Our examination did not extend to controls at the subservice organizations. These subservice organizational controls are specifically included in trust services criterion:

> CC6.4 – *The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.*

Matillion Limited's Responsibilities

Matillion 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 Matillion's service commitments and system requirements were achieved. In Section II, Matillion has provided its assertion titled "Assertion of Matillion Limited Service Organization Management" about the description and the suitability of design and operating effectiveness of controls stated therein. Matillion 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.

Ascend Audit & Advisory's Responsibilities

Our responsibility is to express an opinion on the description of the suitability of the 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 AICPA. 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 operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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 as 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 policies or procedures may deteriorate.

Description of Controls

The specific controls we tested, and the nature, timing, and results of our tests are presented in Section III of our report.

Opinion

In our opinion, in all material respects,

a. the description presents Matillion's system that was designed and implemented throughout the period August 1, 2025 to July 31, 2026, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period August 1, 2025 to July 31, 2026 and designed to provide reasonable assurance that Matillion's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Matillion's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period August 1, 2025 to July 31, 2026, to provide reasonable assurance that Matillion'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 Matillion's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section III, is intended solely for the information and use of Matillion, user entities of its Matillion Platform System during some or all of the period August 1, 2025 to July 31, 2026, business partners of Matillion subject to risks arising from interactions with the Matillion Platform System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Company
- How the Company's system interacts with user entities, subservice organizations, or 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 applicable trust services criteria 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.

Ascend Audit & Advisory



St. Petersburg, FL

September 23, 2026

II. Information Provided by Matillion Limited

ASSERTION OF MATILLION LIMITED SERVICE ORGANIZATION MANAGEMENT

We have prepared the description of the Matillion Platform System ("system" or "the system") throughout the period August 1, 2025 through July 31, 2026, ("the description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization System in a SOC 2 Report (With Revised Implementation Guidance – 2022)* (AICPA, *Description Criteria*). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with Matillion Service Organization's system, particularly information about system controls that Matillion has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criterion relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*(AICPA *Trust Services Criteria*).

Matillion utilizes subservice organizations for the following services and applications:

Subservice Organizations	***Services and Applications***
Amazon Web Services (AWS)	Infrastructure-as-a-Service and cloud computing services
Google	Infrastructure-as-a-Service and enterprise applications
Microsoft – Azure including Dynamics 365	Cloud computing and enterprise applications
Atlassian	Source code and version control and software project management
Auth0	Authentication tools
Okta	Conditional multifactor authentication, access for SaaS applications
Oracle America (NetSuite)	Application hosting services
HiBob	Human Resources information system

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

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

a. The description presents Matillion's system that was designed and implemented throughout the period of August 1, 2025 to July 31, 2026, in accordance with the description criteria.

   i. The description contains the following information:

      (1) The types of services provided.

      (2) The components of the system used to provide the services, which are the following:

      - *Infrastructure* – The physical and hardware components of a system (facilities, equipment, and networks).

- *Software* – The programs and operating software of a system (systems, applications, and utilities).
- *People* – The personnel involved in the operation and use of a system (developers, operators, users, and managers).
- *Procedures* – The automated and manual procedures involved in the operation of a system.
- *Data* – The information used and supported by a system (transaction streams, files, databases, and tables).

(3) The boundaries or aspects of the system covered by the description.

(4) How the system captures and addresses significant events and conditions.

(5) The process used to prepare and deliver reports and other information to user entities and other parties.

(6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each category being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the Company's system.

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the Company, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with privacy commitments.

(9) Any applicable trust services criteria that are not addressed by a control at the Company or a subservice organization and the reasons, therefore.

(10) Other aspects of the Company's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(11) Relevant details of changes to the Company's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the Company's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the description were suitably designed throughout the period August 1, 2025 to July 31, 2026, to provide reasonable assurance that Matillion'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 Matillion's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period August 1, 2025 to July 31, 2026, to provide reasonable assurance that Matillion'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 Matillion's controls operated effectively throughout that period.

By: /S/ Graeme Park

Graeme Park
Chief Information Security Officer

September 23, 2026

DESCRIPTION OF MATILLION'S PLATFORM SYSTEM

Company Overview

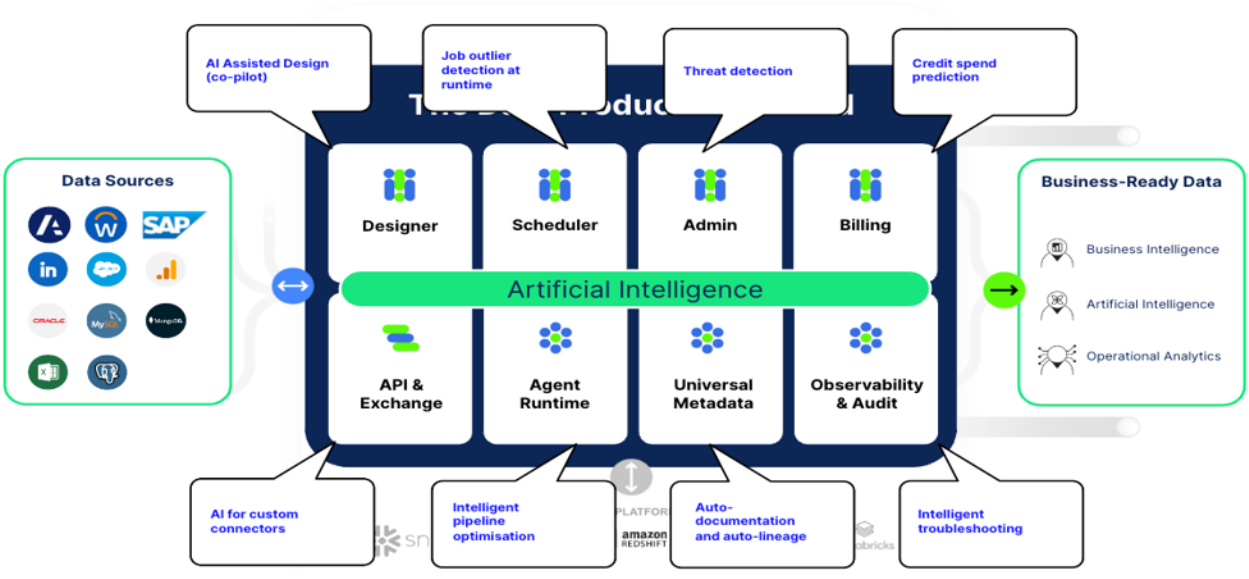
Matillion is a global company, founded in Manchester. Matillion has a globally distributed workforce working between dual headquarters in Denver, CO and Manchester (UK). 1200+ companies including Cisco, DocuSign, Pacific Life, Slack, and TUI trust Matillion to move, transform and automate their data.

Products and Services Overview

Matillion offers services as Maia and Matillion ETL (METL). On June 27, 2023, Matillion launched the Data Productivity Cloud (Formerly DPC), which has since evolved into Maia Foundation with Maia as AI Data Automation Platform from 2025, delivering a Full SaaS and Hybrid-SaaS experience with enhanced data connectivity/migration, flexible pipeline orchestration, and pushdown compute.

In March 2024, Matillion introduced integrated Generative AI capabilities across its platform to enhance data engineering workflows using large language models (LLMs) and retrieval-augmented generation (RAG). This allows data teams to operationalize AI for tasks such as sentiment analysis, preparing draft ticket responses, extracting insights from unstructured data (e.g., PDF reports and call transcripts), and generating automated pipeline documentation to improve organizational data literacy. Matillion seamlessly integrates with leading AI and LLM services - including OpenAI, AWS Bedrock, Azure OpenAI, and Snowflake Cortex - providing flexible text and JSON input/output options while ensuring transformed data remains securely stored within the customer's cloud data platform.

On June 4, 2024, Matillion expanded its AI offerings by introducing no-code Generative AI capabilities for Snowflake users. Through direct integrations with Snowflake Cortex AI, Snowflake ML Functions, and support for Snowpark Container Services, users can deploy out-of-the-box AI use cases - such as product description generation, customer review summarization, key entity extraction, and content translation - directly within their data pipelines.



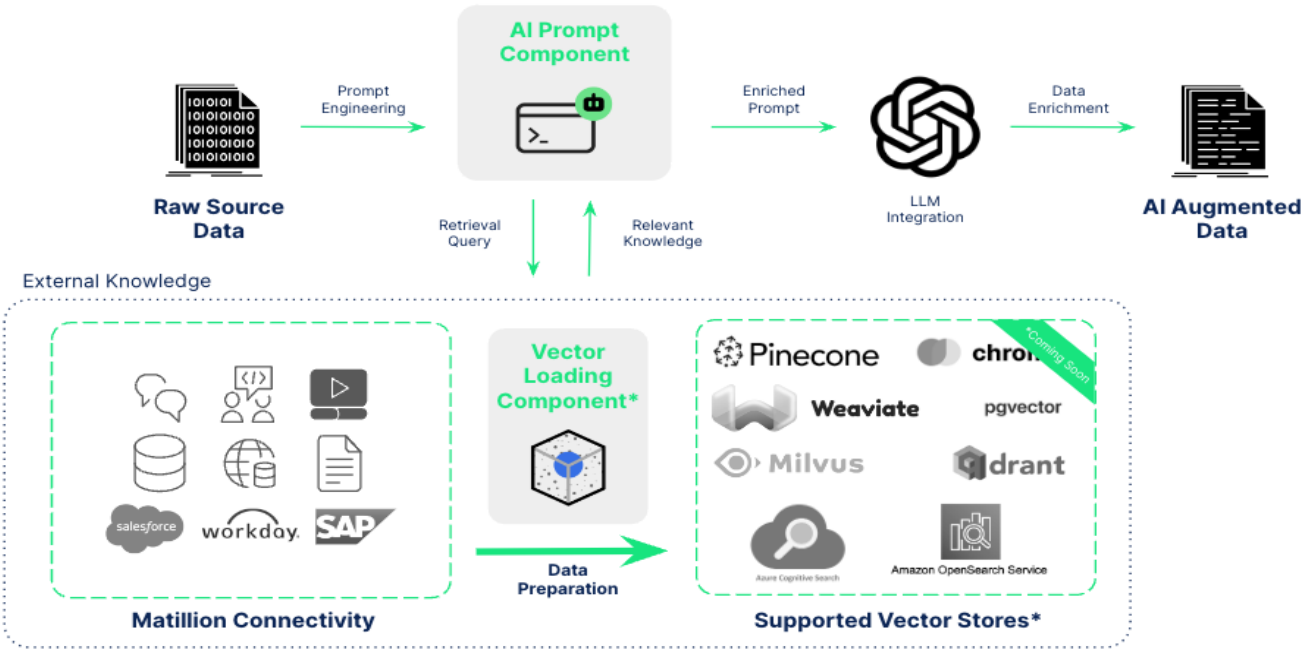
Key benefits of AI Prompt Components and Retrieval Augmented Generation with Matillion:

Prompt Engineering and operationalize the use of Large Language Models inside of a data pipeline to harness the power of Generative AI in data transformations with all existing Matillion connectivity and transformation.

Address intelligent data integration tasks across various domains – one component, many use cases:

- Sentiment Analysis: Extract insights from unstructured data like reviews and social media
- Ticketing: Enhance workflows with AI-powered response drafting and issue prioritization
- Insights Extraction: Automatically analyze PDFs to identify key trends and patterns
- Data Analytics: Transform unstructured data into actionable insights for Customer 360, FP&A, and Sales
- Business Workflows: Streamline tasks and improve decision-making by integrating AI across operations

Vendor agnostic and flexible, the Prompt Component supports OpenAI ChatGPT, AWS Bedrock (many LLMs supported), Azure OpenAI. Leverage the latest and most powerful LLMs in client data pipelines.



Matillion's Maia Foundation

Maia Foundation provides fully SaaS and hybrid cloud SaaS options designed to empower customers in managing their data effectively. With this platform, users create data pipelines that support data movement, data transformation, and data orchestration. Furthermore, it offers robust admin and operational visibility to manage the entire platform end to end. It is important to note that Matillion does not function as a data storage platform. Customer data is not stored within Matillion's systems. Instead, the platform focuses on the orchestration and management of data processes with pushdown architecture (pushdown ELT and AI) to ensure all customer data is within the customer's cloud data platform. Any configurations, user information, and metadata stored within the system are encrypted both at rest and in transit, ensuring the highest level of data security. Maia Foundation represents Matillion's central solution platform, incorporating a range of applications and components that deliver

diverse data services and deployment options. Hosted within Matillion's secure cloud environment, the platform seamlessly integrates with customer networks and virtual networks using standard secure communication protocols. This integration enables efficient and secure data exchange between customer systems and the Matillion platform. Maia Foundation leverages the power of advanced data management capabilities, enabling streamlined data processes, enhanced productivity, and timely data insights.

Maia Team, Context Engine, and Mission Control

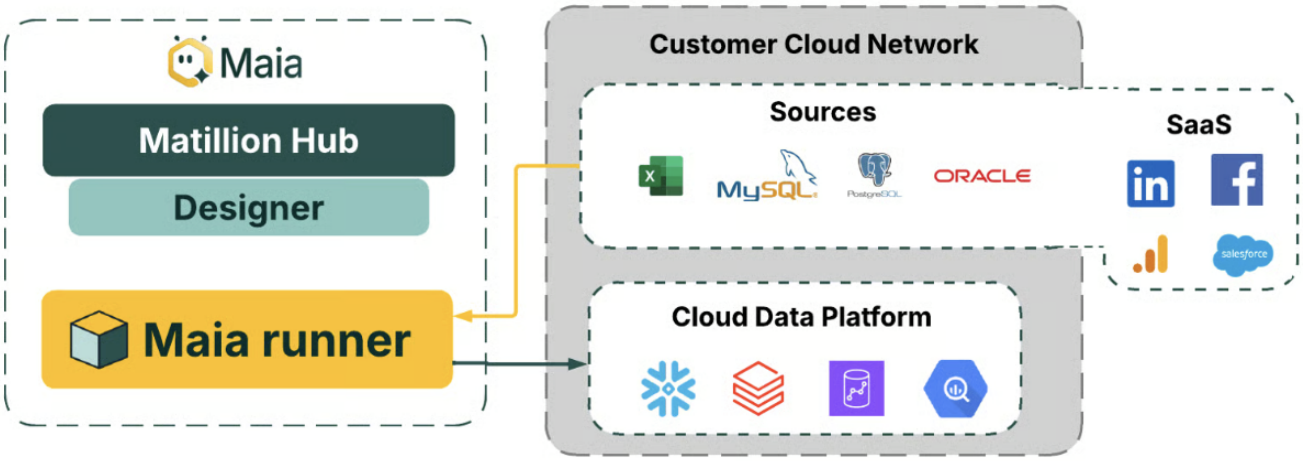
In addition to the Maia Foundation, Maia is made up of two further integrated components that this document previously omitted: Maia Team and the Context Engine. Maia Team is the agentic layer of Maia - an always-on team of AI agents (sometimes referred to internally as Maia agents) that operates inside Maia Foundation and interacts with Designer and the customer's data platform directly, using natural language, to build, maintain, and optimize data pipelines, create custom connectors, query and explore the data warehouse, analyze and fix existing pipelines, and commit and push changes to Git.

The Context Engine is the knowledge layer of Maia. It stores and structures institutional knowledge - including business definitions, compliance rules, data lineage, table and column relationships, and warehouse metadata - organized into knowledge graphs, so that Maia Team can reason against it and produce pipelines consistent with the customer's data standards and business logic. The Context Engine also learns from chat history with Maia Team, so the knowledge base evolves as the data landscape changes.

Mission Control is the organizational center for Maia Team. It lets users create and manage autonomous tasks that Maia Team works through without requiring a user to stay in the chat panel, and provides an agent tasks API for managing tasks programmatically. When creating a task, users select a knowledge graph from the Context Engine to give Maia Team the context it needs for that task.

Recent platform additions not yet reflected elsewhere in this document include Migration Agent (launched March 2026), which autonomously converts legacy ETL pipelines from platforms such as Informatica, Alteryx, SSIS, Talend, and Qlik into native pipelines on Snowflake, Databricks, or Amazon Redshift; and general availability of Maia Foundation on Google BigQuery (July 2026), which joins Snowflake, Databricks, and Amazon Redshift as a supported execution target.

Maia Foundation Components



Maia Foundation comprises applications and services residing inside and outside Matillion's VPC (virtual private cloud), depending on each customer's deployment, and communicating across networks via HTTPS (API microservices). Maia Foundation is a multi-tenant platform with both logical and physical measures in place to ensure

separation. When users log into the Hub they select an account from the list of accounts they have access to. This generates a JWT (JSON Web Token) with a custom claim for the selected account ID.

The Maia runner is a key component of Maia Foundation. It is responsible for processing pipeline tasks, which are individual units of work within a data integration workflow. These tasks handle data integration and transformation operations by securely connecting to data sources and targets. By utilizing secure network protocols, the Maia runner ensures that data is transferred between the Matillion platform and connected data sources in a secure manner. It acts as a bridge, enabling the seamless movement of data while maintaining its integrity and confidentiality.

The Maia runner can be configured in two ways:

1) In Matillion's cloud network, fully managed by Matillion, the Maia runner:

    a. Resides in Matillion's VPC;
    b. Initiates connectivity to Matillion's control plane;
    c. Preforms authentication to ensure access and tenant integrity; and
    d. Logs Agent health and status information (no customer data in logs).

2) Inside the customer's cloud virtual network, the Maia runner:

    a) Runs inside of customer's VPC;
    b) Initiates connectivity to Matillion's control plane to request schedules and exchange data; and
    c) Logs information to the customer's storage container configured by the customer and in their cloud platform.

Applications in Maia Foundation

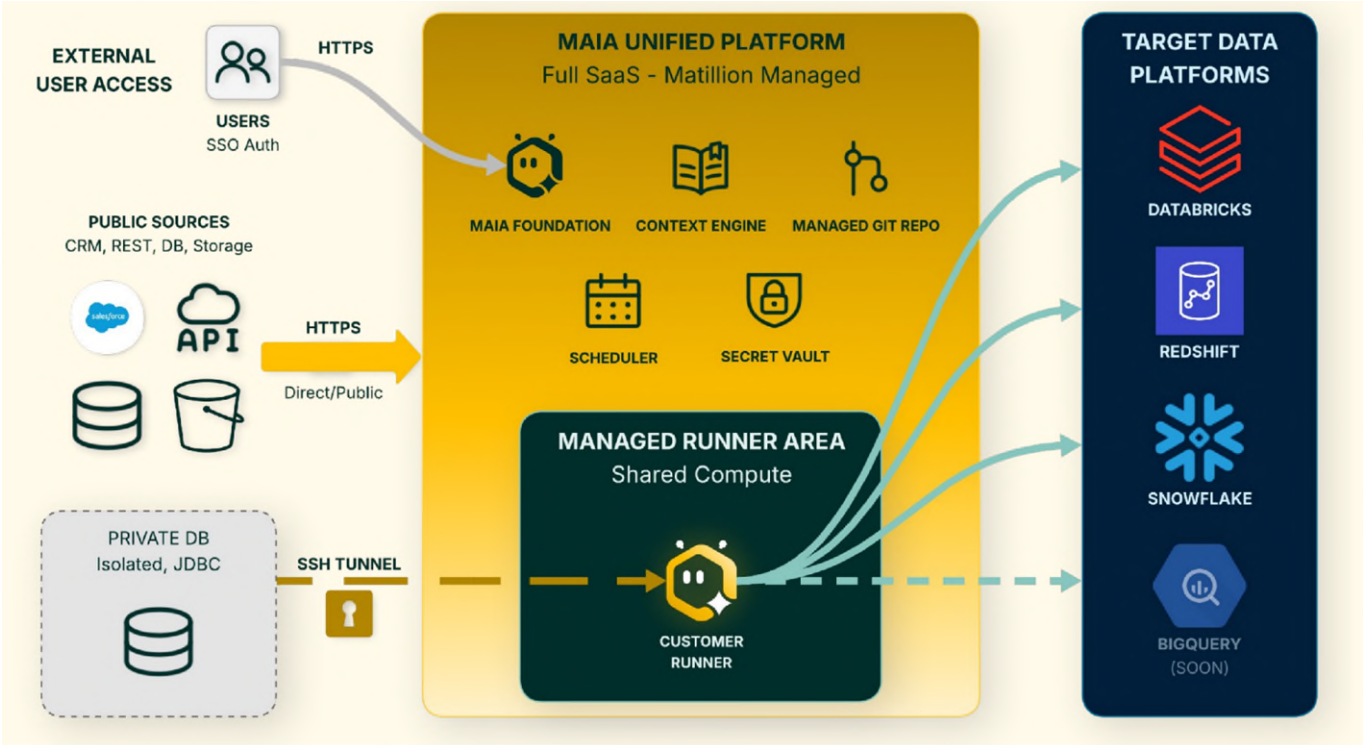
Matillion Hub – serves as the central place for administering and monitoring Maia Foundation. This Web based application offers a multi-tenant environment, allowing users to access and manage their specific environments and data pipelines efficiently. One of the key features of Hub is its ability to aggregate metadata from customer environments and data pipelines. This enables real-time visibility and observability into the performance of pipeline runs, as well as any failures that may occur. Providing comprehensive insights into pipeline execution and status empowers Hub users to quickly identify and address any issues, ensuring smooth data processing and minimizing downtime. In addition to monitoring pipeline performance, Hub also provides information on credit consumption. This allows users to track and manage their credit usage, ensuring optimal utilization of resources within Maia Foundation.

Furthermore, Hub offers visibility into the status of Matillion ETL instances. Users can easily monitor the health and availability of their Matillion ETL instances, enabling proactive management and troubleshooting as needed. The capabilities of Hub allow users to efficiently administer and monitor their data workflows within Maia Foundation. The centralized nature of Hub enhances operational efficiency, enabling users to gain valuable insights, address issues promptly, and optimize the utilization of their Matillion resources. Hub does not collect or store customer data, only the data described in the Control Plane section. Hub also lets users self-service add and manage Maia runner containers for running Designer pipeline tasks, without needing to raise a request with Matillion.

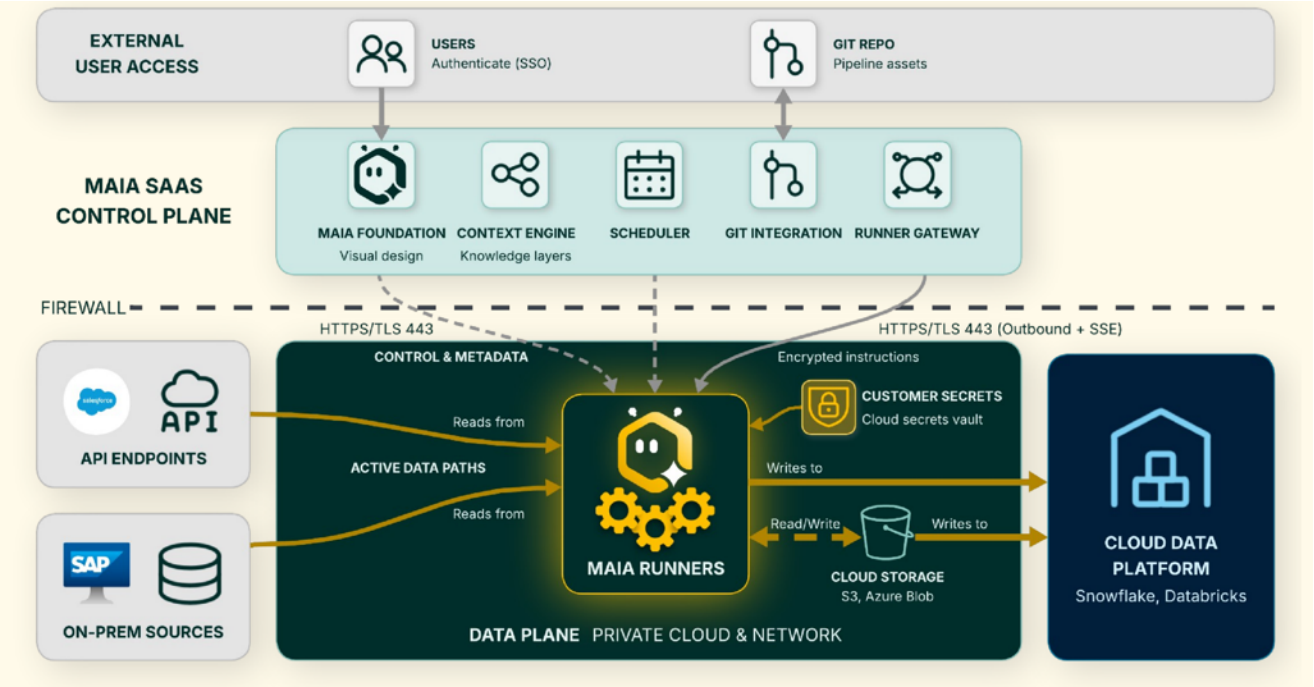
Designer – is a comprehensive and fully managed data pipeline builder. This SaaS Web based application empowers users to create robust and efficient data integration workflows with ease.

As a multi-tenant platform, Designer allows multiple users and teams to work concurrently, leveraging the power of collaborative data integration. With its intuitive interface, users can visually design and configure data pipelines, including data extraction, transformation, and loading processes. The Designer application simplifies complex data integration tasks, enabling users to efficiently handle diverse data sources and formats. Management, upgrades, and performance of the Matillion control plane are meticulously handled by Matillion's Site Reliability Engineering (SRE) team. This ensures that the control plane remains highly available, reliable, and performs optimally, all while being transparent to valued customers. With Matillion taking care of the operational aspects, users can focus on designing and implementing their data integration workflows without worrying about infrastructure management. Designer offers a powerful and streamlined experience for building data integration pipelines. By leveraging its capabilities, users can accelerate their data integration projects, streamline data processes, and unlock the true value of their data assets. Designer uses a Git-based branching model, so multiple team members can work on pipelines simultaneously and promote changes through environments in a controlled way; users can integrate their own Git repository for version control and collaboration.

Designer Deployment and Connectivity (Fully Managed)



Designer Deployment and Connectivity (Hybrid Cloud)



The Designer relies on Maia runners to connect to data sources and targets using the access credentials provided by the customer, which are stored inside the Matillion Secrets Manager or using OAuth securely at pipeline runtime. The Maia runner(s) connect to the Hub to retrieve pipelines and schedules, and to provide pipeline execution status for system observability. Maia runners connect directly to sources and targets, limiting the "hops" of data in transit. Maia runners leverage the encryption protocols employed by the sources and targets, as configured by users at design time. Transformations are orchestrated inside the cloud data platform target after data is landed (ELT).

Designer pipelines can operate with two processing models: Matillion-hosted Maia runners, which orchestrate data pipelines from Matillion's control plane, or with customer-hosted Maia runners in the data plane (inside customers' VPC) to ensure data jurisdiction and isolation requirements are met. These processing models are not mutually exclusive; customers may choose to operate in both modes for different workloads.

A key feature of Designer is Data Sampling. Maia Foundation includes a design-time sampling capability. Users have the ability to see a sample of data in its post-processing state, should a given component be executed. This is intended to ease the pipeline design process by allowing users to preview the results of pipelines without executing them.

System Description

Principal Services Provided

Matillion is the data pipeline platform that empowers data teams to build and manage pipelines faster for AI and analytics – at scale. Matillion allows data engineers to take advantage of AI capabilities and code-optional workflows, harness the processing power of their cloud data platform and cloud providers, and leverage generative AI to enhance data that is used for operational and advanced analytics. Thousands of enterprises including Cisco, DocuSign, Slack, and TUI trust Matillion for a wide range of use cases from insights and operational analytics, to data science, machine learning, and AI. Matillion has dual headquarters in Denver (U.S.) and Manchester (UK).

Principal Service Commitments and System Requirements

Service commitments to user entities are documented and communicated in the End User License Agreement ("EULA") as well as in the description of the product (METL) and the service offering (Maia Foundation) provided online. Service commitments are generally standardized and include, but are not limited to:

- Confidentiality provisions regarding proprietary technical and business information of both Matillion and its customers
- Define and manage the delivery of services including resources and scheduling
- Service usage level and performance from anonymized aggregate data

In achieving its service commitments and system requirements, Matillion has implemented various internal controls to ensure security such as:

- Use of a strong authentication for client portal
- Role-based access controls and continuous review and monitoring of key applications and the network
- Security monitoring infrastructure including intrusion detection, centralized log management and alerting
- Incident response program designed to minimize the impact of incidents and protect resources

Matillion establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Matillion's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.

Components of the System

The System consists of five key components organized to achieve a specified objective. The five components are categorized as follows:

- Infrastructure – physical hardware components of a system (facilities, equipment, and networks)
- Software – programs and operating software of a system (systems, applications, and utilities)
- People – personnel involved in the operation and use of a system (developers, operators, users and managers)
- Processes and Procedures – automated and manual procedures involved in the operation of a system
- Data – information used and supported by a system (transaction streams, files, databases, and tables). Using the above framework

Infrastructure

Matillion's products and platforms are hosted in a range of different options. Authentication is via a Web portal and leverages a third party authentication provider to manage users and groups with serverless code executed in Matillion's environment and user records stored within an AWS Aurora database. Users can utilize a limited version of the METL product set that is architected using REST APIs to manage their data pipelines. Third party integrations are built into MDL often using OAuth for authentication to data sources. A scheduler is implemented using serverless technologies to execute defined jobs at a certain point in time. These jobs are run in containerized environments.

Within Hybrid deployment models and CDC, a Maia runner (or Streaming runner) is located in the customer VPC that communicates back to the Matillion Hub. In a fully managed model, the functionality provided by the Maia runner is executed within the Matillion VPC as a containerized execution. Infrastructure is hosted in either the EU or U.S.

Software

METL, MDL (and CDC), and Maia Foundation are applications developed and maintained by Matillion's in-house engineering team. The engineering team enhances and maintains these applications to provide services for the Matillion's customer base. Matillion's METL software is sold via a number of cloud platforms (marketplaces) and through the Hub service. MDL is freely available online as a SaaS platform.

Matillion hosts a Web site to supplement their ability to communicate and exchange information with their customers. Each page targets a specific audience and is designed to address their business needs depending upon the version of the Matillion product they are using.

Enterprise applications utilized to support Matillion:

- AWS – cloud computing including EC2, Lambda, Aurora MySQL, VPC, Route 53, API Gateway, S3, CloudWatch
- Google Workspace – cloud computing and productivity and collaboration tools (Gmail, Calendar, Drive, etc.)
- Google Cloud Platform – cloud computing and product testing
- Atlassian – source code repository and version control software, software project management, and Intranet for collaboration
- Statuspage – monitor system uptime and communicate outages on MDL
- CircleCI – software build, test, and deployment
- Auth0 – authentication to the MDL platform
- Okta – conditional access to Matillion SaaS applications
- Snyk – third party dependency analysis
- Slack – collaboration and internal communications
- Datadog – monitoring and analytics of the Matillion Platform
- Expel – security event detection and response activities
- Terraform Cloud – provision, change, and version resources on environments
- Hashicorp Vault – identity based security automation and encryption as a service
- Launch Darkly – deploy features into products in a controlled manner with rollback capabilities
- Netsuite – enterprise resource planning
- Sysdig – security and monitoring for container based environments
- StackHawk – API security testing
- Dispatch – establish and maintain quality gates for automated build pipelines

- PagerDuty / Rootly – manage information security incidents

People

Matillion has a staff of approximately 450-500 employees which is a globally distributed workforce across several locations - Denver, Colorado; San Francisco, California; Manchester, UK; Dubai; Sydney; Hyderabad. Employees meet once per year at the Manchester headquarters for company planning, training, and collaboration.

Processes and Procedures

Matillion has a set of policies and procedures to govern Information Security. Changes to these policies and procedures are performed annually and authorized by Senior Management. These procedures cover:

- Data classification
- Vulnerability and patch management
- Software development lifecycle
- Password and authentication
- Physical security
- Risk assessment and management
- System access and control
- Vendor management
- Acceptable use
- Security awareness training
- Incident response
- Social media
- Electronic monitoring
- Data backup and retention
- AI Usage Policy
- Approved AI Tools Directory & Register
- AI Compliance Adherence Policy

Data

Data, as defined by Matillion, constitutes the following:

- Customer account Metadata
- Transaction data
- Output reports
- Input reports
- System files
- Error logs

The end user initiates transaction processing by operating their instance of Maia Foundation/METL/, and this causes Maia Foundation/METL/ to ingest data from the source and copy it into the customer's target Cloud Data Warehouse, often via customer owned cloud object storage for performance best practices. The customer may optionally choose to subsequently transform the data, and this occurs entirely within the customer's target Cloud Data Warehouse. During the ingestion and transformation of data, system files and error logs may be generated by Maia Foundation/METL/, and the end user may choose to share those files and logs with Matillion. If that is done, the system files and error logs become associated with that customer's account metadata. The end user may choose to view data samples at any time, and these appear inside their METL/Maia Foundation user interface in the form of

Input Reports. Within Maia Foundation, data transits the MDL platform when it is loaded into a CDW, data flows are unique to a particular organization and can only be accessed by members of that organization. Access to the Maia Foundation Web interface is conducted over HTTPS for the purpose of viewing and reporting.

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication

Control Environment

Matillion's organizational structure provides an overall framework for planning, directing and controlling enterprise-wide operations. It relates to controls over the execution of transactions, services and operations and assigns authority and responsibility to provide for applicable staffing, segregation of duties, efficiency of operation and concentration of knowledge and skills.

Control environment elements include the following, and the extent to which each element is addressed at Matillion is described below:

- Management Philosophy, Controls, and Operating Style
- Integrity and Ethical Values
- Security Management
- Physical Security and Environmental
- Organizational Structure
- Assignment of Authority and Responsibility
- Standard Operating Controls
- Audit
- Risk Assessment
- Monitoring

Management Philosophy, Controls, and Operating Style

Matillion's control environment reflects the philosophy of Senior Management concerning the importance of security of product, customer and corporate information. Matillion's Security Working Group works through asynchronous monthly updates and provides a yearly written report to the Executive Leadership Team. In designing its controls, Matillion has taken into consideration the relevance of controls to meet the relevant trust criteria.

Management is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; and setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security and privacy, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. Matillion places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in the daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions and regular departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operate under company policies and procedures, including confidentiality agreements and security policies. Periodic training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring customer base for trends, changes, and anomalies.

Competence should reflect the knowledge and skills needed to accomplish tasks that define an individual's job. Through consideration of an entity's objectives and the strategies and plans for achievement of those objectives, Management must determine how well these tasks need to be accomplished. Management identified the competence levels for particular jobs and translated those levels into requisite knowledge and skills.

Integrity and Ethical Values

Maintaining a climate that demands integrity and ethical values is critical to the establishment and maintenance of an effectively controlled organization. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Matillion has programs and policies designed to promote and ensure the integrity and ethical values in its environment.

Matillion desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. Matillion developed professional conduct policies that set forth policies of importance to all employees relating to ethics, values, and conduct. All employees are expected to know and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing company policies, this does not override or diminish an employee's individual responsibility to be aware of and adhere to these policies. Violations of these policies or other forms of misconduct may lead to disciplinary or corrective action up to and including dismissal.

Standards of Conduct

The Company implemented standards of conduct to guide all employee and contractor behavior. Management monitors behavior closely, and exceptions to these standards lead to immediate corrective action as defined by Human Resources (HR) policies and procedures. Additionally, all employees must sign confidentiality agreements prior to employment. Any employee found to have violated the Company's ethics policy may be subject to disciplinary action, up to and including termination of employment.

Matillion has documented the code of business conduct and ethical standards in the employee handbook which is reviewed at least on an annual basis and updated if required. A copy of the Handbook is made available on the Matillion intranet site. Matillion employees are required to read and accept the code of business conduct and ethical standards included in the Employee Handbook as part of their onboarding process and anytime there are any major updates to the document.

Commitment to Competence

The Company has formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs in a professional and competent fashion. The Company determines the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirement. Management monitors and formally evaluates employee and contractor performance on a periodic basis to determine that performance meets or exceeds Matillion standards.

Security Management

Matillion has a dedicated information security team consisting of a CISO, Director of Cloud Security Ops, Sec-Ops Manager, and GRC Sr Analyst/Manager who are responsible for management of information risk and security throughout the organization. A Cloud Security Engineer is responsible for securing Matillion's cloud network and a Lead Application Security Engineer is responsible for the secure development of all commercial product related code. The Company maintains security credentials which are required to annually sign and acknowledge their review of the

information security policies. They are responsible for developing, maintaining, and enforcing Matillion's information security management system. The information security policy is reviewed annually by the CISO and is approved by the executive leadership team.

As the information security team maintains security, it monitors, for example, known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

Matillion maintains employee training programs to promote awareness of information security requirements as defined in the Security & Privacy Awareness Policy. All employees are required to be trained on information security on an annual basis and within 30 days of hire. All employees are subject to Matillion's policies and procedures regarding system access and policy violations may result in disciplinary action. Employees are instructed to report potential security incidents to the help desk.

Physical Security and Environmental Controls

Matillion's offices are located in a range of serviced office providers. These offices are subject to registration upon entry and are protected by both CCTV and swipe access for all offices. The METL product is self-hosted and is subject to customers' physical controls. Data Productivity Cloud/MDL is hosted in AWS cloud infrastructure or hybrid environment depending upon deployment models. Hence, Matillion relies on AWS's physical security and environmental controls for the physical security of the infrastructure hosting the Data Productivity Cloud/MDL and its data. Matillion has implemented monitoring controls to request, receive and review the SOC 2 Type II report from AWS on an annual basis to determine adequacy of controls implemented by AWS.

Organizational Structure

An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Significant cross training between management positions and between staff positions exists to help ensure smooth operations and maintenance of controls during staff or management absence.

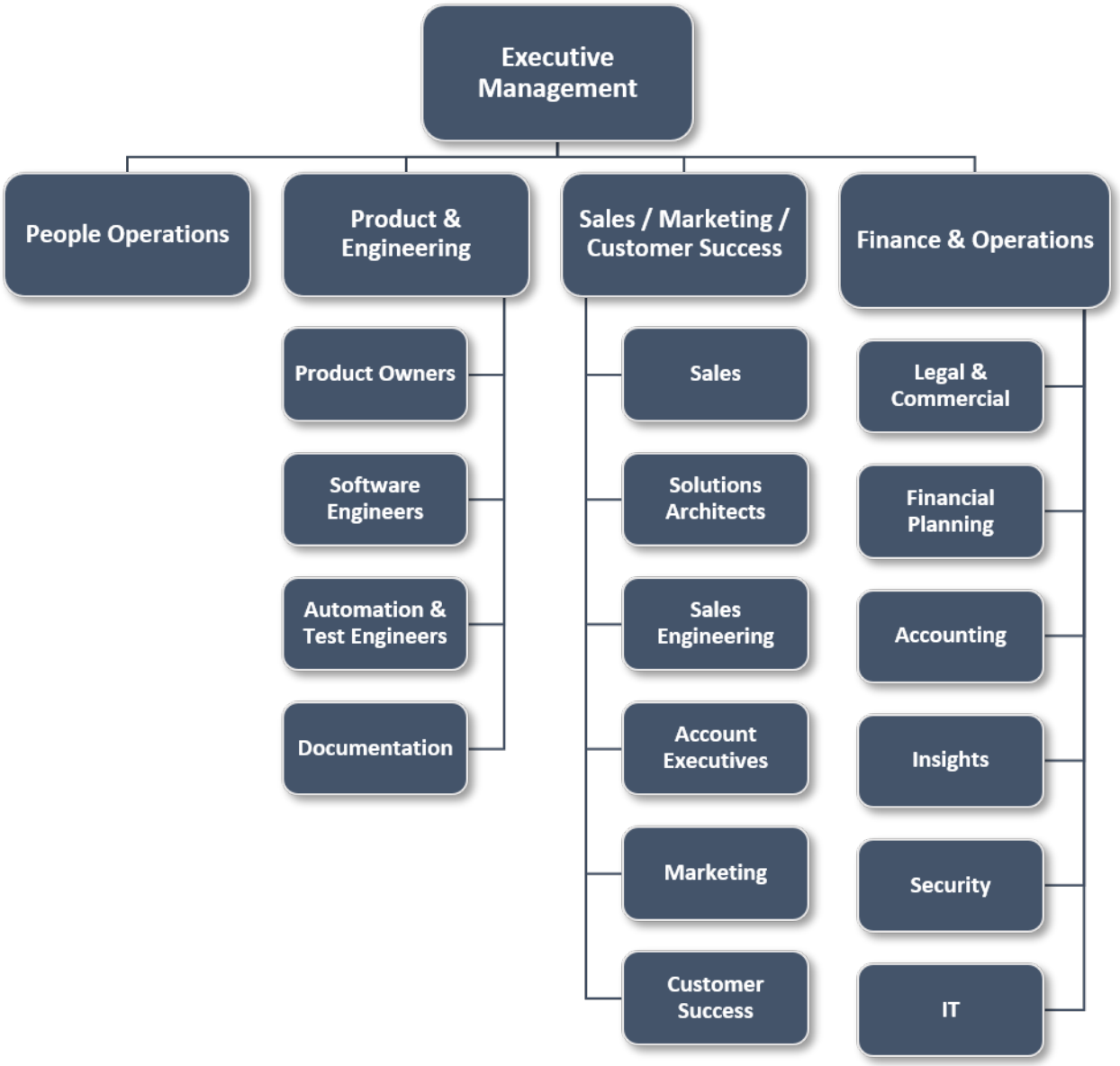
Assignment of Authority and Responsibility

The extent to which individuals recognize that they are held accountable influences the control environment. This holds true for everyone who has ultimate responsibility for activities within an entity, including the internal control system. This includes assignment of authority and responsibility for operating activities, and establishment of reporting relationships and authorization protocols. Matillion's Management encourages individuals and teams to use initiative in addressing issues and resolving problems. Policies describing appropriate business practices, knowledge and experience of key personnel, and available resources are provided to employees in order to assist them in carrying out their duties.

The Company is led by a team of senior executives that assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and any compliance with applicable regulatory requirements. Open dialogue and individual initiative are encouraged as fundamental parts of the Company's goal to deliver client service.

Roles and Responsibilities

The following organizational chart depicts Matillion's corporate structure.



Executive Management – This team comprises the department heads across the organization headed by the CEO. It is responsible for setting and executing on corporate strategy. It uses a range of business intelligence tooling and metrics to measure performance at an overall corporate level.

People Operations – The People Ops Services Team designs and delivers the People Ops product and service offerings across the employee life cycle. People Ops looks after all areas that are hiring, HR policies, employee performance and goals. People-Ops department manages every Matillioner's issues, personal information, promotions, payroll communication, alongside projects on engagement, diversity and inclusion and internal communication.

Product and Engineering – This team builds the applications and their connectors. The team is comprised of software engineers, automation engineers, and test engineers. Prior to release of a product, the documentation team also ensures supporting documentation is up to date to support customers. This team interfaces with customers and the market to ensure customer requirements are packaged into user stories for the Engineering team to work upon. They also ensure the products are built to have a strong UX/UI.

Product Owners – are responsible for liaising with customers and watching the market to define the product development and associated stores to the engineering team.

Software Engineers – are responsible for creating, modifying and updating the codebase that drives the Company's core applications of METL and MDL. They work using SCRUM techniques across a modern technology stack and defined by Matillion's SDLC.

Automation and Test Engineers – are responsible for testing the finished products and ensuring that release candidates meet the requirements defined in a particular set of specifications.

Documentation – is responsible for writing the supporting documentation that assists Matillion's customer in deploying and utilizing its products.

Sales, Marketing, and Customer Success – this 'go to market' function is responsible for conducting marketing activities in order to create awareness of the brand and products, acquire and retain customers, and manage customers' success with Matillion.

Sales – is responsible for generating awareness with new customer prospects.

Solutions Architects – are responsible for delivering technical know-how and expertise to ensure customers realize the full value of Matillion.

Sales Engineering – is responsible for technical engineering support to sales motions.

Account Executives – are responsible for selling to and securing new customers, along with retaining the customer base and key accounts.

Marketing – is responsible for generating demand and awareness of the organization and products.

Customer Success – is responsible for ensuring customers are managed and supported effectively through the lifecycle of the customer.

Finance and Operations – are responsible for running the financial accounts of Matillion, reporting on the general health of the business and providing internal IT and Security services to the business.

Legal and Commercial – is for providing legal guidance and advice to the organization.

Financial Planning – is responsible for budgeting and forecasting, financial analytics and reporting, and assistance for strategic planning.

Accounting – is responsible for all financial transactions within the business both inbound and outbound.

Insights – is responsible for providing internally focused business intelligence services to Matillion.

Security (i.e., Office of CISO) – is responsible for overseeing the risk and cyber security functions which includes application security, security operations and GRC, along with advising the board of directors and Senior Management on the security risk management posture and initiatives.

IT – is responsible for service desk and systems administration.

Standard Operating Controls

Matillion Management sends guidance to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

Matillion has hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process that assesses their qualifications related to the expected responsibility level of the individual. As part of the onboarding process, requisite background checks and/or employment checks are performed as defined in Matillion's hiring procedures. New employees are required to sign an employment agreement upon hire as acknowledgment not to disclose proprietary or confidential information.

Change Management

Matillion has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Matillion has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

Proposed changes are evaluated to determine if they present a security or operational risk and what mitigating actions, including employee and user entity notifications, must be performed. Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments. Emergency changes follow the formalized change management process, but at an accelerated timeline. Change approvals are sought after any emergency.

Application Development

The Matillion Data Productivity Cloud platform undergoes a meticulous process for updates and version control, ensuring the stability and reliability of the platform. Each release goes through three distinct environments, each with specific quality assurance measures applied. The first environment is a development environment where new features and enhancements are implemented and tested. Here, the development team ensures that the changes meet the required specifications and standards.

Once the development phase is complete, the release moves to a testing environment. In this environment, comprehensive testing procedures are conducted to validate the functionality and performance of the new release. This includes various types of testing, such as functional testing, integration testing, and regression testing, to identify and address any issues or conflicts.

After successful testing, the release progresses to a staging environment. Here, it undergoes further verification and validation to ensure that it is ready for deployment to the production environment. This includes performance testing, security checks, and user acceptance testing, among others. Promotions to the production environment are performed by a limited number of authorized Site Reliability Engineers, adhering to the principle of least privilege.

This strict access control ensures that only qualified personnel can perform deployments to the live production environment.

To maintain a high level of security and accountability, all access to these environments is logged and monitored using Matillion's security monitoring and alerting system. This allows for comprehensive tracking and analysis of all activities within the environments, enhancing the platform's overall security posture. Following this rigorous update and version control process ensures the Matillion Data Productivity Cloud platform remains stable, reliable, and secure, providing customers with a robust and trustworthy solution for their data integration needs.

Incident Management

Security incidents and other IT related problems are reported to the help desk. Issues are tracked using a help desk ticket and monitored until resolved.

Backups

Matillion uses cloud native backup of its data files and software. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized personnel.

System Account Management

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

The People Ops department provides IT personnel with a termination ticket when any terminations are processed. The IT team reconciles the termination report with current access privileges to determine if access has been appropriately removed or disabled. Dormant accounts are reviewed and disabled on a quarterly basis. Administrative access to core services such as Google Workspace (formerly G Suite), Directory services and Cloud based Infrastructure providers is restricted to authorized employees.

Unique user identification numbers, names, and passwords are required to authenticate all users to METL and MDL environments. Password parameters consist of the following:

- Passwords contain a minimum of 8 characters and have varying complexity requirements.
- Passwords are not set to expire based on current National Cyber Security Centre (NCSC) guidance.
- Log-on sessions are terminated after failed log-on attempts.
- Password reuse is prohibited.
- MFA is configured in addition to passwords in all places where possible.

Configuration and Vulnerability Monitoring

Matillion conducts monthly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with Matillion's patch management process.
Matillion maintains centralized admin access to all machines. Device access policies are utilized to ensure compliance goals and block access based on the health of end point devices. Matillion issued desktops and/or laptops are protected against malicious attacks using an anti-virus/anti-malware software which is configured to receive automatic updates and to provide real-time protection.

Audit

Matillion Management performs periodic audits of procedures and holds scheduled compliance meetings with staff to review current and new procedures.

Risk Assessment and Management

Matillion has implemented a Risk Management Program which includes periodic risk assessments, creation of a risk register, and implementation of risk mitigation steps. Matillion regularly reviews the risks that may threaten the achievement of the criteria for the security principle set forth in TSP section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria). A formal risk assessment is maintained and reviewed at least annually by the Risk Committee. As part of the risk assessment, Management assesses the environment, complexity, nature and scope of its operations. Matillion has established an Executive Management Committee comprised of Senior Management. This Committee meets at least on an annual basis to review and approve updates to policies and procedures, Risk Management Program, and Security Dashboard (security incidents, assessment results, and status of remediation items).

Senior Management, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on Matillion's policies. Changes in security threats and risks are reviewed by Matillion, and updates to existing control activities and information security policies are performed as necessary.

Monitoring

Matillion's Management monitors the quality of the internal control performance as a normal part of its activities. As a component of the ongoing monitoring, Management generates and reviews a series of management reports, that contain various data points that enable management to measure the results of various processes.

In addition to the daily oversight, monthly vulnerability assessments, monitoring and alerting, Management provides further security monitoring through internal audits, which include information security assessments.

As an additional measurement, Matillion regularly performs monitoring activities to assess the control activities being performed by subservice organizations utilized to maintain and operate the Matillion system. These monitoring activities vary based on the service provided by the subservice organization but include a range of assessing their independent attestation report, and/or through its daily operational activities through the direct management or interaction with the subservice organization.

Information and Communication

Matillion uses a variety of methods for communication to ensure that significant events and issues are conveyed in a timely manner and that staff understand their role and responsibility over service and controls. These methods include the following: new hire training; ongoing training; policy and process updates; weekly departmental meetings summarizing events and changes; use of email to communicate time sensitive information; and the documentation and storage of historical data in internal repositories for business and support activities. The Company maintains systems that manage the flow of information and facilitate communication with its customers.

Information Flow from Senior Management to Operations Staff

Matillion has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities over processing and controls and communicates significant events in a timely

manner. Employee manuals are provided upon hire that communicate all policies and procedures concerning employee conduct. Security of the physical premises and logical security of systems are reinforced by training and through awareness programs. The communication system between Senior Management and operations staff includes the use of the office email system, written memos when appropriate, and weekly meetings. Managers hold departmental meetings with personnel to discuss new Company policies and procedures and other business issues.

Recurring staff and training meetings are utilized to inform staff of new policy and technology updates. Communication is encouraged at all levels to promote the operating efficiency of Matillion.

Communication

Matillion uses a variety of methods for communication to ensure that significant events and issues are conveyed in a timely manner and that staff understand their role and responsibility over service and controls. These methods include the following: new hire training, ongoing training, policy and process updates, recurring departmental meetings summarizing events and changes, use of email to communicate time sensitive information, and the documentation and storage of historical data in internal repositories for business and support activities. The Company maintains systems that manage the flow of information and facilitate communication with its customers.

Subservice Organizations

Matillion contracts with Amazon Web Services (AWS) for infrastructure-as-a-service and cloud computing. AWS maintains a current SOC 1 Type II and SOC 2 Type II report.

Matillion contracts with Google LLC for infrastructure-as-a-service and enterprise applications. Google maintains a current SOC 1 Type II and SOC 2 Type II report.

Matillion contracts with Microsoft Corporation – Azure including Dynamics 365 for cloud computing and enterprise applications. Microsoft maintains current SOC 2 Type II reports, along with a current ISO/IEC 27001, ISO 27018, ISO 27017, and ISO 27701 certification.

Matillion contracts with Atlassian Corporation PLC for source code repository, version control, and software project management. Atlassian maintains a current SOC 2 Type II report.

Matillion contracts with Okta, Inc. (including Auth0) for authentication tools, conditional multifactor authentication, and access to SaaS applications. Okta maintains a current SOC 2 Type II report, along with a current ISO/IEC 27001 certification.

Matillion contracts with Oracle America, Inc. (NetSuite for application hosting services. Oracle maintains a current SOC 2 Type II report.

Matillion contracts with HiBob for a Human Resources information system. HiBob maintains a current SOC 2 Type II report.

These subservice organizational controls are specifically included in trust services criteria:

> CC6.4 – *The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.*

User Control Considerations

The Company's applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at the Company. User auditors should consider whether or not the following controls are implemented at user organizations:

- Customers are responsible for reviewing contracts with Matillion and ensuring authorized personnel execute contracts for services.
- Customers are responsible for providing and maintaining an information technology infrastructure that has embedded logical and physical environmental controls to protect against unauthorized access. This should include the end user workstation environment used to access MDL as well as the environment where Matillion ETL is installed.
- Customers are responsible for ensuring only authorized users are granted access to the MDL portal and its functionalities.
- Customers are responsible for treating MDL access accounts' sign-in names and password information as secure and private and in accordance with industry best practices.
- Customer are responsible for deploying updates to ETL available from Matillion.
- Customers are responsible for implementing adequate network security controls including perimeter firewall, routing rules, encrypted communication, etc. in their environment where Matillion ETL has been deployed.
- Customers are responsible for reporting to Matillion the incidents specific to their MDL accounts.
- Customers are responsible for developing, maintaining, and testing their own business continuity plan (BCP) or for contracting with Matillion for its BCP services.
- Customers are responsible for the security and integrity of their transmission facilities, operating facilities, and equipment that are used to access Matillion secured software.
- Customers are responsible for the transmission and reception of all data and transactions initiated through their Web sites.
- Customers are responsible for discharging all duties to remain in compliance with their agreements with Matillion.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Providing data center colocation and managed services for customers by Matillion covers only a portion of the overall internal control structure of each customer. The Company products and services were not designed to be the only control component in the internal control environment. Additional control procedures require implementation at the customer level. It is not feasible for all of the control objectives relating to providing data center colocation and managed services to be fully achieved by Matillion. Therefore, each customer's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

III. Information Provided by Ascend Audit & Advisory

COMMON CONTROL CRITERIA – SECURITY CATEGORY

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Sets the Tone at the Top—The board of directors and Management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.	Inspected the entity's most current employee handbook including the business conduct and ethics policy, most current culture code, and most current employee confidentiality and non-competition agreement to determine the board of directors and Management, at all levels, demonstrated the importance of integrity and ethical values to support the functioning of the system of internal control.	No exceptions noted.
		Establishes Standards of Conduct—The expectations of the board of directors and Senior Management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.	Inspected the entity's most current employee handbook including the business conduct and ethics policy, most current culture code, most current employee confidentiality and non-competition agreement, and executed vendor and client agreements to determine standards of conduct were communicated at all levels of the entity and to outsourced service providers and business partners.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.1 (Cont.)	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.	For the selection of active employees, inspected system generated reporting of completed employee performance reviews; observed via walkthrough procedures and inspected the employee performance tracking software; and conducted corroborative of HR Management to determine processes were in place to evaluate the performance of individuals against the entity's expected standards of conduct.	No exceptions noted.
		Addresses Deviations in a Timely Manner—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.	Inspected the most current performance and capability and progressive disciplinary policies and procedures, and conducted corroborative inquiry of HR Management to determine deviations from the entity's expected standards of conduct would be identified and remedied in a timely and consistent manner. Informed by Management there were no deviations from expected standards of conduct reported during the period under review.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional point of focus specifically related to all engagements using the trust services criteria:				
CC1.1 (Cont.)	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.	Inspected the most current vendor risk management policy and processes, along with the most current contractor onboarding policy and procedures, to determine Management and the board of directors, at all levels, considered the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.2	COSO Principle 2: The board of directors demonstrates independence from Management and exercises oversight of the development and performance of internal control.	Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.	Inspected board of directors and Management meeting minutes regarding strategic, financial, business, operational, product, and engineering objectives and updates to determine the board of directors identified its oversight responsibilities in relation to established requirements and expectations.	No exceptions noted.
		Applies Relevant Expertise—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of Senior Management and take commensurate action.	Inspected the directors' powers and responsibilities provisions in the entity's certificate of incorporation to determine the board of directors defined and evaluated its members with respect to enabling oversight of Senior Management and took commensurate action.	No exceptions noted.
		Operates Independently—The board of directors has sufficient members who are independent from Management and objective in evaluations and decision making.	Inspected the most current board of directors members listing and associated biographies to determine the board of directors had sufficient members who were independent from Management and objective in evaluations and decision making.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional point of focus specifically related to all engagements using the trust services criteria:				
CC1.2 (Cont.)	COSO Principle 2: The board of directors demonstrates independence from Management and exercises oversight of the development and performance of internal control.	Supplements Board Expertise—The board of directors supplements its expertise relevant to security, as needed, through the use of a subcommittee or consultants.	Inspected board of directors and Management meeting minutes regarding strategic, financial, business, operational, product, and engineering objectives and updates to determine the board of directors supplemented its expertise, as needed, through the use of outside consultation.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.	Inspected board of directors and Management meeting minutes regarding strategic, financial, business, operational, product, and engineering objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, and most current organizational charts to determine Management and the board of directors considered the multiple structures used to support the achievement of objectives.	No exceptions noted.
		Establishes Reporting Lines—Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.	Inspected the entity's most current organizational charts to determine Management designed and evaluated lines of reporting to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.3 (Cont.)	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Defines, Assigns, and Limits Authorities and Responsibilities—Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.	Inspected board of directors and Management meeting minutes regarding strategic, financial, business, operational, product, and engineering objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, and most current organizational charts to determine Management and the board of directors assigned responsibility and segregated duties as necessary at the various levels of the organization.	No exceptions noted.
Additional points of focus specifically related to all engagements using the trust services criteria:				
		Addresses Specific Requirements When Defining Authorities and Responsibilities—Management and the board of directors consider requirements relevant to security when defining authorities and responsibilities.	Inspected board of directors and Management meeting minutes regarding operational and engineering objectives and updates; along with cyber security subcommittee and weekly organizational objectives and updates communicated to personnel; and observed via walkthrough procedures and inspected the entity's risk management program (i.e., ongoing risk assessments, risk ratings, and risk mitigation activities) to determine Management and the board of directors considered requirements relevant to security when defining authorities and responsibilities.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC1.3 (Cont.)	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Considers Interactions with External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities—Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.	Inspected board of directors and Management meeting minutes regarding strategic, business, and operational objectives and updates; along with executed vendor and client agreements; observed via walkthrough procedures and inspected the entity's risk management program; and inspected the most current SOC reports of the entity's subservice organizations to determine Management and the board of directors considered the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Establishes Policies and Practices—Policies and practices reflect expectations of competence necessary to support the achievement of objectives.	Inspected the most current employee handbook and culture code, documented talent acquisition and new hire onboarding and orientation processes and procedures, the entity's online repository of company policies and processes and procedures, and completed compliance and departmental training recordkeeping to determine policies and practices reflected expectations of competence necessary to support objectives.	No exceptions noted.
		Evaluates Competence and Addresses Shortcomings—The board of directors and Management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.	Inspected board of directors and Management meeting minutes regarding business, operational, product, and engineering objectives and updates; system generated reporting of completed employee performance reviews, executed vendor agreements, and the entity's risk management program to determine the board of directors and Management evaluated competence across the entity and had policies and practices in place to address shortcomings. Informed by Management there were no personnel or outsourced provider shortcomings reported during the period under review.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.4 (Cont.)	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Attracts, Develops, and Retains Individuals—The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.	Inspected documented talent acquisition and new hire onboarding and orientation processes and procedures, most current employee handbook and culture code, the entity's online repository of company policies and processes and procedures, and completed compliance and departmental training recordkeeping to determine the entity provided the mentoring and training needed to attract, develop, and retain sufficient and competent personnel to support the achievement of objectives.	No exceptions noted.
		Plans and Prepares for Succession—Senior Management and the board of directors develop contingency plans for assignments of responsibility important for internal control.	Inspected board of directors and Management meeting minutes regarding strategic, business, and operational objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, and most current business continuity and disaster recovery plan to determine Management developed contingency plans for assignments of responsibility for internal control.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria:				
CC1.4 (Cont.)	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Considers the Background of Individuals—The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	For the selection of new employees, inspected completed background check confirmations to determine the entity considered the background of potential personnel when determining whether to employ the individuals.	No exceptions noted.
		Considers the Technical Competency of Individuals—The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	Inspected documented talent acquisition and new hire onboarding and orientation processes and procedures, along with completed compliance and departmental training recordkeeping; and observed via walkthrough procedures and inspected the entity's system monitoring, infrastructure-as-a-service (IaaS) and cloud and cybersecurity, threat detection / prevention, endpoint protection, and backup and restore software consoles and system administration procedures to determine the entity considered the technical competency of individuals with respect to employment and career advancement.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC1.4 (Cont.)	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Provides Training to Maintain Technical Competencies—The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.	Inspected documented new hire onboarding and orientation processes and procedures, most current employee handbook and culture code, the entity's online repository of company policies and processes and procedures, and completed compliance and departmental training recordkeeping to determine the entity provided training programs to ensure the skill sets and technical competency of personnel were developed and maintained.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Enforces Accountability Through Structures, Authorities, and Responsibilities—Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.	Inspected board of directors and Management meeting minutes regarding financial, business, operational, product, and engineering objectives and updates; inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel; and for the selection of new employees, inspected signed acknowledgements of the employee handbook including the conduct policy, online acknowledgements of the culture code, and executed employment agreements, to determine Management and the board of directors established mechanisms to communicate accountability for performance of internal control responsibilities across the entity.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.5 (Cont.)	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Establishes Performance Measures, Incentives, and Rewards—Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.	For the selection of active employees, inspected system generated reporting of completed employee performance reviews; observed via walkthrough procedures and inspected the employee performance tracking software; and conducted corroborative of HR Management to determine Management and the board of directors established performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity including short- and longer-term objectives.	No exceptions noted.
		Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance—Management aligns incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.	For the selection of active employees, inspected system generated reporting of completed employee performance reviews; observed via walkthrough procedures and inspected the employee performance tracking software; and conducted corroborative of HR Management to determine Management aligned incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.5 (Cont.)	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Considers Excessive Pressures—Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.	For the selection of active employees, inspected system generated reporting of completed employee performance reviews; observed via walkthrough procedures and inspected the employee performance tracking software; and conducted corroborative of HR Management to determine Management and the board of directors evaluated and adjusted pressures associated with the achievement of objectives as they assigned responsibilities, developed performance measures, and evaluated performance.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.5 (Cont.)	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Evaluates Performance and Rewards or Disciplines Individuals—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action, as appropriate.	For the selection of active employees, inspected system generated reporting of completed employee performance reviews; observed via walkthrough procedures and inspected the employee performance tracking software; and inspected the most current employee handbook including the ethical conduct and progressive disciplinary and work performance policies to determine Management evaluated performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence and exercised disciplinary action, when appropriate. Informed by Management there were no disciplinary actions required or taken during the period under review.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Identifies Information Requirements—A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.	Inspected board of directors and Management meeting minutes regarding business, operational, product, and engineering objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, most current employee handbook and culture code, the entity's online repository of company policies and processes and procedures, and completed compliance and departmental training recordkeeping to determine processes were in place to identify information required and expected to support the system's functioning of internal control and the achievement of the entity's objectives.	No exceptions noted.
		Captures Internal and External Sources of Data—Information systems capture internal and external sources of data.	Inspected cloud agent and workflow and hub service logging from the entity's production application monitoring software to determine information systems captured internal and external sources of data.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC2.1 (Cont.)	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Processes Relevant Data Into Information—Information systems process and transform relevant data into information.	Inspected cloud agent and workflow and hub service logging from the entity's production application monitoring software, along with application alarming and associated deficiency change requests completed to determine information systems processed and transformed relevant data into information.	No exceptions noted.
		Maintains Quality Throughout Processing—Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.	Inspected cloud agent and workflow and hub service logging from the entity's production application monitoring software, application alarming and associated deficiency change requests completed, and the documented error handling, logging and monitoring procedures to determine information systems maintained quality throughout processing and information was reviewed to assess its relevance in supporting the internal control components.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria:				
CC2.1 (Cont.)	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Documents Data Flow—The entity documents and uses internal and external information and data flows to support the design and operation of controls.	Inspected the entity's most current cloud applications architecture and data flow diagrams to determine the entity documented and used internal and external information and data flows to support the design and operation of controls.	No exceptions noted.
		Manages Assets—The entity identifies, documents, and maintains records of system components such as infrastructure, software, and other information assets. Information assets include physical endpoint devices and systems, virtual systems, data and data flows, external information systems, and organizational roles.	Inspected the most current system generated IT asset inventory register including the associated attributes for each asset to determine the entity maintained records of system components and information assets.	No exceptions noted.
		Classifies Information—The entity classifies information by its relevant characteristics (for example, personally identifiable information, confidential customer information, and intellectual property) to support identification of threats to the information and the design and operation of controls.	Inspected the entity's risk management program (i.e., ongoing risk assessments, risk ratings, and risk mitigation activities), most current system generated IT asset inventory register including the associated attributes for each asset, and most current data classification and handling policy and procedures to determine the entity classified information to support identification of threats to the information and the design and operation of controls.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC2.1 (Cont.)	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Uses Information That Is Complete and Accurate—The entity uses information and reports that are complete, accurate, current, and valid in the operation of controls.	Observed via walkthrough procedures and inspected the entity's production application monitoring software consoles, performance indicators, and system generated event and error logging and notifications to determine the entity used information that was complete, accurate, current, and valid in the operation of controls.	No exceptions noted.
		Manages the Location of Assets—The entity identifies, documents, and maintains records of physical location and custody of information assets, particularly for those stored outside the physical security control of the entity (for example, software and data stored on vendor devices or employee mobile phones under a bring-your- own-device policy).	Inspected the entity's most current cloud applications architecture and data flow diagrams, along with the most current system generated IT asset inventory register including the associated attributes for each asset, to determine the entity maintained records of physical location and custody of information assets and accounted for information assets stored outside the entity's environment.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**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.	Communicates Internal Control Information—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, most current employee handbook, the entity's online repository of company policies and processes and procedures, completed compliance and departmental training recordkeeping, and the entity's risk management program to determine a process was in place to communicate required information to enable personnel to understand and carry out their internal control responsibilities.	No exceptions noted.
		Communicates with the Board of Directors—Communication exists between Management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.	Inspected board of directors and Management meeting minutes regarding strategic, financial, business, operational, product, and engineering objectives and updates to determine communications existed between Management and the board of directors so all had information needed to fulfill their roles and meet the entity's objectives.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC2.2 (Cont.)	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	Inspected the entity's whistleblower reporting and communication mechanism to determine a separate communication channel existed as a fail-safe mechanism to enable anonymous and confidential communication.	No exceptions noted.
		Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the information.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, online repository of company policies and processes and procedures, Management communications to personnel regarding policy updates and training compliance objectives, and the entity's internal messaging platform and communication channels to determine communications considered the timing, audience, and the nature of the information.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria:				
CC2.2 (Cont.)	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Communicates Responsibilities—Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.	Inspected the most current employee handbook, documented new hire onboarding and orientation processes and procedures, system generated reporting of completed employee performance reviews, the entity's online repository of company policies and processes and procedures, completed compliance and departmental training recordkeeping, and the entity's risk management program to determine personnel received communications about their responsibilities and had information to carry out those responsibilities.	No exceptions noted.
		Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters—Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.	Inspected the entity's whistleblower reporting and communication mechanism, along with the most current incident response policy and procedures, to determine personnel were provided with information on how to report systems failures, incidents, concerns, and other complaints.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC2.2 (Cont.)	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Communicates Objectives and Changes to Objectives—The entity communicates its objectives and changes to those objectives to personnel in a timely manner.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, online repository of company policies and processes and procedures, Management communications to personnel regarding policy updates and training compliance objectives, and the entity's internal messaging platform and communication channels to determine objectives were communicated in a timely manner.	No exceptions noted.
		Communicates Information to Improve Security Knowledge and Awareness—The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.	For the selection of active employees, inspected security awareness training course completion reporting to determine the entity communicated information to improve security knowledge and awareness through a security awareness training program.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:				
CC2.2 (Cont.)	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, most current employee handbook, the entity's risk management program, online repository of company policies and processes and procedures, Management communications to personnel regarding policy updates and training compliance objectives, and the entity's internal messaging platform and communication channels to determine the entity prepared and communicated information about the design and operation of the system to authorized personnel.	No exceptions noted.
		Communicates System Objectives—The entity communicates its objectives to personnel to enable them to carry out their responsibilities.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, most current employee handbook, the entity's risk management program, online repository of company policies and processes and procedures, Management communications to personnel regarding policy updates and training compliance objectives, and the entity's internal messaging platform and communication channels to determine the entity communicated objectives to personnel.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level (continued):				
CC2.2 (Cont.)	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Communicates System Changes—System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.	Inspected completed compliance and departmental training recordkeeping, the entity's risk management program, online repository of company policies and processes and procedures, Management communications to personnel regarding policy updates and training compliance objectives, and the entity's internal messaging platform and communication channels to determine system changes that affected responsibilities were communicated in a timely manner.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Communicates to External Parties—Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.	Inspected the entity's online AI data automation platform user guide and reference material, support and knowledge base user interfaces, term and conditions and service agreements, release notes, and products and services updates to determine processes were in place to communicate relevant and timely information to external stakeholders.	No exceptions noted.
		Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing Management and the board of directors with relevant information.	Inspected the online support and knowledge base user interfaces to determine communication channels allowed input from external entities for providing Management with relevant information.	No exceptions noted.
		Communicates with the Board of Directors—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors and the Management Team.	Inspected board of directors and Management meeting minutes regarding business, operational, product, and engineering objectives and updates; along with the entity's risk management program, to determine relevant information from assessments by external entities was communicated to the board of directors and Management.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC2.3 (Cont.)	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	Inspected the online support and knowledge base user interfaces to determine separate communication channels were in place to enable anonymous and confidential communication.	No exceptions noted.
		Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.	Inspected the entity's online AI data automation platform user guide and reference material, support and knowledge base user interfaces, term and conditions and service agreements, release notes, and products and services updates to determine communications considered the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:				
CC2.3 (Cont.)	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.	Inspected executed vendor and client agreements; and inspected the entity's online AI data automation platform user guide and reference material, support and knowledge base user interfaces, term and conditions and service agreements, release notes, and products and services updates to determine the entity prepared and communicated information about the design and operation of the system and its boundaries to authorized external users.	No exceptions noted.
		Communicates System Objectives—The entity communicates its system objectives to appropriate external users.	Inspected executed vendor and client agreements; and inspected the entity's online AI data automation platform user guide and reference material, support and knowledge base user interfaces, term and conditions and service agreements, release notes, and products and services updates to determine system objectives were communicated to appropriate external users.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Information and Communication (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level (continued):				
CC2.3 (Cont.)	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Communicates System Responsibilities—External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the information necessary to carry out those responsibilities.	Inspected executed vendor and client agreements; and inspected the entity's online AI data automation platform user guide and reference material, support and knowledge base user interfaces, term and conditions and service agreements, release notes, and products and services updates to determine external users received communications about their responsibilities and were provided information to carry out those responsibilities.	No exceptions noted.
		Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters—External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected executed vendor and client agreements; and inspected the entity's online AI data automation platform user guide and reference material, support and knowledge base user interfaces, term and conditions and service agreements, release notes, and products and services updates to determine external users were provided information on how to report failures, issues, and concerns to appropriate personnel.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Risk Assessment			
CC3.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	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.	Reflects Management's Choices—Operations objectives reflect Management's choices about structure, industry considerations, and performance of the entity.	Inspected board of directors and Management meeting minutes regarding business and operational objectives and updates, cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, and the entity's risk management program (i.e., ongoing risk assessments, risk ratings, and risk mitigation activities) to determine operations objectives reflected Management's structure and performance posture.	No exceptions noted.
		Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, along with the entity's risk management program, to determine Management considered acceptable levels of variation relative to the achievement of operational objectives.	No exceptions noted.
		Includes Operations and Financial Performance Goals—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.	Inspected board of directors and Management meeting minutes regarding financial, business, and operational objectives and updates to determine the organization reflected operational and financial performance within operations objectives.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.1 (Cont.)	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Forms a Basis for Committing of Resources—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.	Inspected board of directors and Management meeting minutes regarding financial, business, and operational objectives and updates; along with the entity's risk management program, to determine Management used a formal process for meeting operational and business objectives.	No exceptions noted.
		Complies with Externally Established Frameworks—Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.	Inspected executed vendor and client agreements, most current employee handbook, most current vulnerability assessment and penetration testing attestations, most current Payment Card Industry Data Security Standard (PCI DSS) attestation of compliance, and most current ISO 27001 certification to determine Management established objectives consistent with laws and regulations, standards, and frameworks of recognized external organizations.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.1 (Cont.)	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.	Inspected executed vendor and client agreements, most current vulnerability assessment and penetration testing attestations, most current PCI DSS attestation of compliance, and most current ISO 27001 certification to determine Management reflected the required level of precision and accuracy suitable for user needs and was based on criteria established by third parties in nonfinancial reporting.	No exceptions noted.
		Reflects Entity Activities—External reporting reflects the underlying transactions and events within a range of acceptable limits.	Inspected the support and knowledge base user interfaces, release notes, and products and services updates to determine external reporting reflected underlying transactions and events within acceptable limits.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.1 (Cont.)	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Reflects Management's Choices—Internal reporting provides Management with accurate and complete information regarding Management's choices and information needed in managing the entity.	Inspected board of directors and Management meeting minutes regarding financial, business, and operational objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, completed compliance and departmental training record keeping, and most current system generated IT asset inventory register including the associated attributes for each asset to determine internal reporting provided Management with accurate and complete information needed in managing the entity.	No exceptions noted.
		Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.	Inspected board of directors and Management meeting minutes regarding financial, business, and operational objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, and the entity's risk management program to determine Management reflected the required level of precision and accuracy suitable for nonfinancial reporting objectives and materiality within financial reporting objectives.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.1 (Cont.)	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Reflects Entity Activities—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.	Inspected board of directors and Management meeting minutes regarding financial, business, and operational objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, completed compliance and departmental training record keeping, and most current system generated IT asset inventory register including the associated attributes for each asset to determine internal reporting reflected the underlying transactions and events within a range of acceptable limits.	No exceptions noted.
		Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.	Inspected the entity's most current employee handbook including the business conduct and ethics policy, most current culture code, and most current employee confidentiality and non-competition agreement; and for the selection of new employees, inspected signed acknowledgements of the employee handbook including the conduct policy to determine the entity established minimum standards of conduct in its compliance objectives.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.1 (Cont.)	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.	Inspected board of directors and Management meeting minutes regarding operational objectives and updates, along with the entity's risk management program, to determine Management considered acceptable levels of variation for the achievement of operations objectives.	No exceptions noted.
Additional point of focus specifically related to all engagements using the trust services criteria:				
		Establishes Sub-Objectives for Risk Assessment—Management identifies sub-objectives for use in risk assessment related to security to support the achievement of the entity's objectives.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, along with the entity's risk management program, to determine Management identified sub-objectives for use in risk assessment related to security to support the achievement of the entity's objectives.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
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.	Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, most current vulnerability assessment and penetration testing attestations, the lifecycle of completed infrastructure change requests in the ticketing and project management software, and most current disaster recovery processes and procedures and associated testing results to determine the entity identified and assessed risks throughout the organization with respect to the achievement of objectives.	No exceptions noted.
		Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, most current vulnerability assessment and penetration testing attestations, the lifecycle of completed infrastructure change requests in the ticketing and project management software, and most current disaster recovery processes and procedures and associated testing results to determine Management considered both internal and external factors and their impact on the achievement of objectives.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.2 (Cont.)	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.	Involves Appropriate Levels of Management—The entity puts into place effective risk assessment mechanisms that involve appropriate levels of Management.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, most current vulnerability assessment and penetration testing attestations, the lifecycle of completed infrastructure change requests in the ticketing and project management software, and most current disaster recovery processes and procedures and associated testing results to determine the entity had effective risk assessment mechanisms that involved appropriate levels of Management.	No exceptions noted.
		Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.	Inspected the entity's risk management program to determine identified risks were analyzed which included estimating the potential significance of the risks.	No exceptions noted.
		Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, along with the entity's risk management program, to determine Management considered how to manage risks with respect to mitigation strategies.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria:				
CC3.2 (Cont.)	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.	Identifies Threats to Objectives—The entity identifies threats to the achievement of its objectives from intentional (including malicious) and unintentional acts and environmental events.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, and most current disaster recovery processes and procedures and associated testing results to determine the entity identified threats to the achievement of objectives from intentional and unintentional acts and environmental events.	No exceptions noted.
		Identifies Vulnerability of System Components—The entity identifies the vulnerabilities of system components, including system processes, infrastructure, software, and other information assets.	Inspected the entity's risk management program, online support knowledge base and release notes, and most current vulnerability assessment and penetration testing attestations to determine the entity identified vulnerabilities of system components, system processing, infrastructure, and software.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC3.2 (Cont.)	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.	Analyzes Threats and Vulnerabilities from Vendors, Business Partners, and Other Parties—The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.	Inspected executed vendor and client agreements, the entity's risk management program, and most current SOC reports of the entity's subservice organizations to determine the entity's risk assessment process included analysis of potential threats from vendors, contractors, and business partners with respect to third party access to the entity's information systems.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC3.2 (Cont.)	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.	Assesses the Significance of the Risks— The entity assesses the significance of the identified risks, including (1) determining the criticality of system components, including information assets, in achieving the objectives; (2) assessing the susceptibility of the identified vulnerabilities to the identified threats (3) assessing the likelihood of the identified risks (4) assessing the magnitude of the effect of potential risks to the achievement of the objectives; (5) considering the potential effects of unidentified threats and vulnerabilities on the assessed risks; (6) developing risk mitigation strategies to address the assessed risks; and (7) evaluating the appropriateness of residual risk (including whether to accept, reduce, or share such risks).	Inspected the entity's risk management program and conducted corroborative inquiry of Governance, Risk, and Compliance (GRC) Management to determine the entity assessed the significance of the identified risks including criticality of the system components achieving objectives, vulnerabilities to identified threats, likelihood of identified risks, magnitude of effects of potential risks, risk mitigation strategies, and appropriateness of residual risk.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Considers Various Types of Fraud—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	Inspected the most current employee handbook and acceptable use policies, most current culture code, employee confidentiality and non-competition agreement, the entity's risk management program, and most current information security policy and procedures to determine fraud was considered as part of risk management objectives.	No exceptions noted.
		Assesses Incentives and Pressures—The assessment of fraud risks considers incentives and pressures.	the most current employee handbook and acceptable use policies, most current culture code, employee confidentiality and non-competition agreement, the entity's risk management program, and most current information security policy and procedures to determine aspects of fraud were identified as risk objectives.	No exceptions noted.
		Assesses Opportunities—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.	Inspected the most current IT asset request policy, most current employee handbook and acceptable use policies, and most current asset disposal policy and procedures to determine fraudulent opportunities for unauthorized acquisition, use, and disposal of assets were considered with respect to altering reporting and other inappropriate acts.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.3 (Cont.)	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Assesses Attitudes and Rationalizations—The assessment of fraud risk considers how Management and other personnel might engage in or justify inappropriate actions.	Inspected the most current employee handbook and acceptable use policies, most current culture code, employee confidentiality and non-competition agreement, the entity's risk management program, most current information security policy and procedure, and most current IT asset request and asset disposal policies and procedures to determine the assessment of fraud risk considered how Management and other personnel might engage in inappropriate actions.	No exceptions noted.
Additional point of focus specifically related to all engagements using the trust services criteria:				
		Considers the Risks Related to the Use of IT and Access to Information—The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.	Inspected the most current IT asset request policy, most current employee handbook and acceptable use policies, most current information security policy and procedures, and most current asset disposal policy and procedures to determine an assessment of fraud risk included consideration of threats and vulnerabilities from the use of IT and access to information.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Assesses Changes in the External Environment—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.	Inspected the entity's risk management program, along with the most current physical and environmental security policy and procedures, to determine the risk assessment considered changes to external factors and the entity's physical environment.	No exceptions noted.
		Assesses Changes in the Business Model—The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.	Inspected board of directors and Management meeting minutes regarding business and operational objectives and updates, Management communications to personnel regarding policy updates and training compliance objectives, and most current PCI DSS attestation of compliance to determine the entity considered potential impacts to the business with respect to lines of business and business operations.	No exceptions noted.
		Assesses Changes in Leadership—The entity considers changes in Management and respective attitudes and philosophies on the system of internal control.	Inspected board of directors and Management meeting minutes regarding strategic, business, operational, product, and engineering objectives and updates; along with cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, to determine the entity considered material changes in Management and respective attitudes and philosophies on the system of internal control.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria:				
CC3.4 (Cont.)	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Assesses Changes in Systems and Technology—The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, most current vulnerability assessment and penetration testing attestations, and the lifecycle of completed infrastructure change requests in the ticketing and project management software to determine the risk assessment process considered changes with respect to the entity's systems and changes to the technology environment.	No exceptions noted.
		Assesses Changes in Vendor and Business Partner Relationships—The risk identification process considers changes in vendor and business partner relationships.	Inspected board of directors and Management meeting minutes regarding strategic, business, operational, product, and engineering objectives and updates; executed vendor and client agreements, and most current SOC reports of the entity's subservice organizations to determine the risk assessment process considered changes in vendor and business partner relationships.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC3.4 (Cont.)	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Assesses Changes in Threats and Vulnerabilities—The risk identification process assesses changes in (1) internal and external threats to and vulnerabilities of the components of the entity's systems and (2) the likelihood and magnitude of the resultant risks to the achievement of the entity's objectives.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, and most current vulnerability assessment and penetration testing attestations to determine the risk identification process assessed changes in internal and external threats and vulnerabilities of system components and the likelihood and magnitude of risks to the achievement of objectives.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Monitoring Activities**			
CC4.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**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.	Considers a Mix of Ongoing and Separate Evaluations—Management includes a balance of ongoing and separate evaluations.	Inspected board of directors and Management meeting minutes regarding financial, business, operational, product, and engineering objectives and updates; the entity's risk management program (i.e., ongoing risk assessments, risk ratings, and risk mitigation activities), most current vulnerability assessment and penetration testing attestations, most current PCI DSS attestation of compliance, and most current ISO 27001 certification to determine Management included a balance of ongoing and separate evaluations.	No exceptions noted.
		Considers Rate of Change—Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.	Inspected board of directors and Management meeting minutes regarding business, operational, and product objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, and Management communications to personnel regarding policy updates and training compliance objectives to determine Management considered the rate of change in business processes.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Monitoring Activities (Continued)**			
CC4.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC4.1 (Cont.)	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.	Establishes Baseline Understanding—The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, most current vulnerability assessment and penetration testing attestations, most current PCI DSS attestation of compliance, and most current ISO 27001 certification to determine the design and current state of the internal control system was used to establish a baseline for system evaluations.	No exceptions noted.
		Uses Knowledgeable Personnel—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.	Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, endpoint protection, and backup and restore software consoles and system administration procedures to determine system evaluators had sufficient knowledge to understand what was being evaluated.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Monitoring Activities (Continued)**			
CC4.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC4.1 (Cont.)	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.	Integrates with Business Processes—Ongoing evaluations are built into the business processes and adjust to changing conditions.	Inspected board of directors and Management meeting minutes regarding business, operational, and product objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, and the entity's risk management program to determine ongoing evaluations were built into business processes with respect to adjustments to changing conditions.	No exceptions noted.
		Adjusts Scope and Frequency—Management varies the scope and frequency of separate evaluations depending on risk.	Inspected board of directors and Management meeting minutes regarding financial, business, operational, product, and engineering objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, and the entity's risk management program to determine Management monitored the scope and frequency of separate evaluations depending on risk.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Monitoring Activities (Continued)**			
CC4.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC4.1 (Cont.)	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.	Objectively Evaluates—Separate evaluations are performed periodically to provide objective feedback.	Inspected most current vulnerability assessment and penetration testing attestations, most current PCI DSS attestation of compliance, and most current ISO 27001 certification to determine separate evaluations were performed periodically for objective feedback.	No exceptions noted.
Additional point of focus specifically related to all engagements using the trust services criteria:				
		Considers Different Types of Ongoing and Separate Evaluations—Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, most current vulnerability assessment and penetration testing attestations, most current PCI DSS attestation of compliance, and most current ISO 27001 certification to determine Management used various types of ongoing and separate evaluations and internal audit assessments.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Monitoring Activities (Continued)**			
CC4.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
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.	Assesses Results—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, most current vulnerability assessment and penetration testing attestations, most current PCI DSS attestation of compliance, most current ISO 27001 certification, and most current disaster recovery processes and procedures and associated testing results to determine Management assessed results of ongoing and separate evaluations.	No exceptions noted.
		Communicates Deficiencies—Deficiencies are communicated to parties responsible for taking corrective action and to Senior Management and the board of directors, as appropriate.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, along with the lifecycle of completed infrastructure change requests in the ticketing and project management software, to determine deficiencies were communicated to parties responsible for taking corrective action and to Senior Management.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Monitoring Activities (Continued)**			
CC4.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC4.2 (Cont.)	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.	Monitors Corrective Action—Management tracks whether deficiencies are remedied on a timely basis.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, along with the lifecycle of completed infrastructure change requests in the ticketing and project management software, to determine Management tracked deficiencies remediation on a timely basis.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Activities**			
CC5.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**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.	Integrates with Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program (i.e., ongoing risk assessments, risk ratings, and risk mitigation activities), Management communications to personnel regarding policy updates and training compliance objectives, most current vulnerability assessment and penetration testing attestations, and most current disaster recovery processes and procedures and associated testing results to determine control activities helped ensure risk mitigation was carried out.	No exceptions noted.
		Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, and most current disaster recovery processes and procedures and associated testing results to determine Management considered entity-specific factors for the selection and development of control activities.	No exceptions noted.

`	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Activities (Continued)**			
CC5.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC5.1 (Cont.)	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.	Determines Relevant Business Processes—Management determines which relevant business processes require control activities.	Inspected board of directors and Management meeting minutes regarding business, operational, and product objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, and most current disaster recovery processes and procedures and associated testing results to determine Management identified relevant business processes that required control activities.	No exceptions noted.
		Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.	Inspected board of directors and Management meeting minutes regarding financial, business, operational, product, and engineering objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, most current vulnerability assessment and penetration testing attestations, most current PCI DSS attestation of compliance, and most current ISO 27001 certification to determine Management evaluated a mix of control activity types with respect to risk mitigation.	No exceptions noted.

`	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Activities (Continued)**			
CC5.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC5.1 (Cont.)	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.	Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity.	Inspected board of directors and Management meeting minutes regarding financial, business, operational, product, and engineering objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, and the entity's risk management program to determine Management considered control activities at various levels in the entity.	No exceptions noted.
		Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical, Management selects and develops alternative control activities.	For the selection of new employees, inspected completed new employee access provisioning requests including case history for each ticket to determine Management segregated incompatible duties with respect to control activities.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Control Activities (Continued)			
CC5.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.	Inspected board of directors and Management meeting minutes regarding business, operational, and product objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, and most current disaster recovery processes and procedures and associated testing results to determine Management considered dependencies and linkage between business processes and various control activities.	No exceptions noted.
		Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.	Observed via walkthrough procedures and inspected the entity's production application monitoring software consoles, performance indicators, and system generated event and error logging and notifications; along with the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, endpoint protection, and backup and restore software consoles and system administration procedures; and inspected the most current disaster recovery processes and procedures and associated testing results to determine Management developed and implemented control activities to help ensure complete, accurate, and available technology processing.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Activities (Continued)**			
CC5.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC5.2 (Cont.)	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Establishes Relevant Security Management Process Controls Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.	Inspected completed logical access rights reviews for the entity's identity and access management (IAM) system and enterprise applications to determine Management implemented control activities to restrict access rights with respect to appropriateness of user job functions and protected assets from external threats.	No exceptions noted.
		Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve Management's objectives.	Inspected board of directors and Management meeting minutes regarding product and engineering objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, online release notes, and lifecycle of completed infrastructure change requests in the ticketing and project management software to determine Management implemented control activities with respect to the development and maintenance of technology and infrastructure.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Activities (Continued)**			
CC5.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
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.	Establishes Policies and Procedures to Support Deployment of Management's Directives—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.	Inspected board of directors and Management meeting minutes regarding business, operational, and product objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, and most current disaster recovery processes and procedures and associated testing results to determine Management established control activities that were built into business processes establishing what was expected and procedures specifying actions.	No exceptions noted.
		Establishes Responsibility and Accountability for Executing Policies and Procedures—Management establishes responsibility and accountability for control activities with Management (or other designated personnel) of the business unit or function in which the relevant risks reside.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, and Management communications to personnel regarding policy updates and training compliance objectives to determine Management established responsibility and accountability for control activities of the business function in which associated risks resided.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Activities (Continued)**			
CC5.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC5.3 (Cont.)	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Performs in a Timely Manner—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, and the lifecycle of completed infrastructure change requests in the ticketing and project management software to determine responsible personnel performed control activities in a timely manner per policy and procedures.	No exceptions noted.
		Takes Corrective Action—Responsible personnel investigate and act on matters identified as a result of executing control activities.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, the entity's risk management program, most current disaster recovery processes and procedures and associated testing results, and the lifecycle of completed infrastructure change requests in the ticketing and project management software to determine personnel took action on matters identified as a result of executing control activities.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Activities (Continued)**			
CC5.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC5.3 (Cont.)	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.	Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, endpoint protection, and backup and restore software consoles and system administration procedures to determine appropriate personnel performed control activities per control activity objectives.	No exceptions noted.
		Reassesses Policies and Procedures—Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.	Inspected board of directors and Management meeting minutes regarding financial, business, operational, product, and engineering objectives and updates; cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, and the entity's risk management program to determine Management periodically reviewed control activities for continued relevance or adjustments.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**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.	Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets.	Inspected the most current system generated IT asset inventory register including the associated attributes for each asset, most current data classification and handling policy and procedures, and the entity's risk management program (i.e., ongoing risk assessments, risk ratings, and risk mitigation activities) to determine the entity identified, inventoried, classified, and managed information assets.	No exceptions noted.
		Assesses New Architectures—The entity identifies new system architectures and assesses their security prior to implementation into the system environment.	Not applicable – new architecture security assessments. Informed by Management there were no identified new system architectures required or assessed during the period under review.	No testing performed.
		Restricts Logical Access—Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.	Observed via walkthrough procedures and inspected system generated lists of authorized system administrators, users, and security groups of the entity's IAM system, enterprise applications, and remote access software; along with configured inbound and outbound access rules of the entity's virtual private cloud (VPC), to determine logical access to information assets was restricted through the use of access control software and rule sets.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.1 (Cont.)	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.	Identifies and Authenticates Users—Persons, infrastructure, and software are identified and authenticated prior to accessing information assets, whether locally or remotely.	Observed via walkthrough procedures and inspected system generated lists of authorized system administrators, users, and security groups of the entity's IAM system, IaaS, enterprise applications, and remote access software to determine personnel and the systems were identified and authenticated prior to accessing information assets.	No exceptions noted.
		Considers Network Segmentation—Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.	Observed via walkthrough procedures and inspected configured inbound and outbound access rules and subnets of the entity's VPC; and inspected the entity's most current network topology diagram to determine the network was segmented for critical system isolation.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.1 (Cont.)	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.	Manages Points of Access—Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.	Observed via walkthrough procedures and inspected system generated lists of authorized system administrators, users, and security groups of the entity's IAM system, enterprise applications, and remote access software; along with configured inbound and outbound access rules of the entity's VPC; and inspected completed logical access rights reviews for the entity's IAM system and enterprise applications to determine points of access and the types of users were identified, logged, and managed.	No exceptions noted.
		Restricts Access to Information Assets—Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets.	Observed via walkthrough procedures and inspected system generated lists of authorized system administrators, users, and security groups of the entity's IAM system, enterprise applications, and remote access software; along with configured inbound and outbound access rules of the entity's VPC, to determine the entity utilized a combination of access controls that restricted access to information assets.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.1 (Cont.)	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.	Manages Identification and Authentication—Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.	Observed via walkthrough procedures and inspected system generated lists of authorized system administrators, users, security groups, and authentication mechanisms (i.e., password policy and multi-factor authentication) of the entity's IAM system, enterprise applications, and remote access software; and inspected completed logical access rights reviews for the entity's IAM system and enterprise applications to determine identification and authentication requirements were established and managed for personnel and systems.	No exceptions noted.
		Manages Credentials for Infrastructure and Software—New internal and external infrastructure and software users are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required, or the infrastructure and software are no longer in use.	For the selection of new employees, inspected completed new employee access provisioning requests including case history for each ticket to determine new users were registered, authorized, and documented prior to network access provisioning.	No exceptions noted.
			For the selection of terminated employees, inspected terminated employee access deprovisioning requests, along with confirmations of associated accounts disabled, to determine credentials were removed and access disabled when no longer required.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.1 (Cont.)	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.	Uses Encryption to Protect Data—The entity uses encryption to supplement other measures used to protect data-at-rest when such protections are deemed appropriate based on assessed risk.	Inspected the production database storage configuration with encryption enabled, along with encryption enabled settings of the entity's endpoint protection systems, to determine the entity utilized encryption to protect data-at-rest.	No exceptions noted.
		Protects Cryptographic Keys—The entity protects cryptographic keys during generation, storage, use, and destruction. Cryptographic modules, algorithms, key lengths, and architectures are appropriate based on the entity's risk mitigation strategy.	Inspected the key management service software console for the entity's managed keys to determine cryptographic keys were protected and appropriate.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**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.	Creates Access Credentials to Protected Information Assets—The entity creates credentials for accessing protected information assets based on an authorization from the system's asset owner or authorized custodian. Authorization is required for the creation of all types of credentials of individuals (for example, employees, contractors, vendors, and business partner personnel), systems, and software.	For the selection of new employees, inspected completed new employee access provisioning requests including case history for each ticket to determine access credentials were created based on an authorization from associated stakeholders.	No exceptions noted.
		Reviews Validity of Access Credentials—The entity reviews access credentials on a periodic basis for validity (for example, employees, contractors, vendors, and business partner personnel) and inappropriate system or service accounts.	Inspected completed logical access rights reviews for the entity's IAM system and enterprise applications to determine the entity reviewed access credentials on a periodic basis for appropriateness.	No exceptions noted.
		Prevents the Use of Credentials When No Longer Valid—Processes are in place to disable, destroy, or otherwise prevent the use of access credentials when no longer valid	For the selection of terminated employees, inspected terminated employee access deprovisioning requests, along with confirmations of associated accounts disabled, to determine processes were in place to disable or otherwise prevent the use of access credentials when no longer valid.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**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, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Creates or Modifies Access to Protected Information Assets—Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.	For the selection of new employees, inspected completed new employee access provisioning requests including case history for each ticket to determine processes were in place to create access to protected information assets based on authorization from asset owners.	No exceptions noted.
		Removes Access to Protected Information Assets—Processes are in place to remove access to protected information assets when an individual no longer requires access.	For the selection of terminated employees, inspected terminated employee access deprovisioning requests, along with confirmations of associated accounts disabled, to determine processes were in place to remove access to protected information assets when an individual no longer required access.	No exceptions noted.
		Uses Access Control Structures—The entity uses access control structures, such as role-based access controls, to restrict access to protected information assets, limit privileges, and support segregation of incompatible functions.	Observed via walkthrough procedures and inspected system generated lists of authorized system administrators, users, and security groups of the entity's IAM system, enterprise applications, and remote access software to determine access control structures were utilized to restrict access to protected information assets, limit privileges, and support segregation of incompatible functions.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.3 (Cont.)	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Reviews Access Roles and Rules—The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals (for example, employees, contractors, vendors, business partner personnel) and in- appropriate system or service accounts. Access roles and rules are modified, as appropriate.	Inspected completed logical access rights reviews for the entity's IAM system and enterprise applications to determine appropriateness of access roles and access rules were reviewed on a periodic basis and access roles and rules were modified, as appropriate.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Creates or Modifies Physical Access—Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.	For the selection of new employees requiring office space access, inspected enabled accounts in the entity's physical access control system to determine processes were in place to create physical access to the entity's corporate office based on authorization from system asset owners.	No exceptions noted.
			Carve out. Processes to create and modify physical access to outsourced data centers were managed and maintained by the entity's subservice organizations in accordance with completed SOC reporting.	No testing performed.
		Removes Physical Access—Processes are in place to remove access to physical resources when an individual no longer requires access.	For the selection of terminated employees provisioned with office space access, inspected terminated employee physical access deprovisioning requests, along with the associated accounts deprovisioned, to determine processes were in place to remove access to the entity's corporate office when an individual no longer required access.	No exceptions noted.
			Carve out. Processes to remove physical access to outsourced data centers were managed and maintained by the entity's subservice organizations in accordance with completed SOC reporting.	No testing performed.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.4 (Cont.)	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Recovers Physical Devices—Processes are in place to recover entity devices (for example, badges, laptops, and mobile devices) when an employee, contractor, vendor, or business partner no longer requires access.	For the selection of twenty-five (25) terminated employees, inspected twenty-four (24) confirmations of entity devices recovered or decommissioned in the entity asset management system to determine processes were in place to recover entity devices when an employee no longer required access. *Exception noted*: There was no evidence of device recovery for one (1) terminated employee. *Management response*: a process improvement was implemented for the terminated employee device recovery control.	Exception noted.
		Reviews Physical Access—Processes are in place to periodically review physical access to ensure consistency with job responsibilities.	Inspected the entity's most current physical access rights review reports to determine processes were in place to periodically review physical access to office space for appropriateness.	No exceptions noted.
			Carve out. Processes to periodically review physical access to outsourced data centers were managed and maintained by the entity's subservice organizations in accordance with completed SOC reporting.	No testing performed.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
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.	Removes Data and Software for Disposal—Procedures are in place to remove, delete, or otherwise render data and software inaccessible from physical assets and other devices owned by the entity, its vendors, and employees when the data and software are no longer required on the asset or the asset will no longer be under the control of the entity.	Inspected the most current asset disposal policy and procedures, along with reporting of secure asset decommissioning, to determine procedures were in place to remove, delete, or otherwise render data and software inaccessible from equipment when data and software were no longer required and equipment no longer under control of the entity.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Restricts Access—The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.	Observed via walkthrough procedures and inspected configured security groups and inbound and outbound access rules of the entity's VPC to determine types of activities through communication channels were restricted.	No exceptions noted.
		Protects Identification and Authentication Credentials—Identification and authentication credentials are protected during transmission outside its system boundaries.	Observed via walkthrough procedures and inspected system generated lists of authorized system administrators, users, and security groups of the entity's IAM system, enterprise applications, and remote access software to determine identification and authentication credentials were protected.	No exceptions noted.
		Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.	Inspected the entity's IAM system authenticators mechanism, along with defense-in-depth authentication mechanisms (i.e., multi-factor) of the entity's enterprise applications, to determine additional authentication credentials were required when accessing the system from outside its boundaries.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.6 (Cont.)	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Implements Boundary Protection Systems—Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.	Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, and endpoint protection software consoles and system administration procedures; along with associated system generated event logging and notifications, to determine boundary protection systems were implemented to protect external access points from unauthorized access and access attempts were monitored.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
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.	Restricts the Ability to Perform Transmission—Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information.	Inspected the data loss prevention policies enabled in the entity's cyber security console to determine data loss prevention processes and technologies were utilized to restrict the ability to authorize and execute transmission, movement, and removal of information.	No exceptions noted.
		Uses Encryption Technologies or Secure Communication Channels to Protect Data—Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.	Inspected the advanced setting of the entity's remote access software, along with the most current Secure Socket Layer (SSL) certificate for the entity's Web server, to determine encryption technologies were utilized to protect transmission of data.	No exceptions noted.
		Protects Removable Media—Encryption technologies and physical asset protections are used for removable media (such as USB drives and backup tapes), as appropriate.	Inspected the removable media policy in the most current data classification policy and procedures, along with the USB policies configured in the entity's endpoint protection software, to determine encryption technologies and physical protections were required and utilized for removable media.	No exceptions noted.
		Protects Endpoint Devices—Processes are in place to protect endpoint devices (such as laptops, smart phones, tablets, and sensors).	Inspected the entity's endpoint protection software management console, policies enabled, and endpoints protected to determine processes were in place to protect endpoint devices.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**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.	Restricts Installation and Modification of Application and Software—The ability to install and modify applications and software is restricted to authorized individuals. Utility software capable of bypassing normal operating or security procedures is limited to use by authorized individuals and is monitored regularly.	Observed via walkthrough procedures and inspected system generated lists of authorized system administrators and security groups of the entity's IAM system and enterprise applications; and inspected the most current acceptable use policies to determine the ability to install and modify applications and software was restricted to authorized personnel.	No exceptions noted.
		Detects Unauthorized Changes to Software and Configuration Parameters—Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.	Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, and endpoint protection software consoles and system administration procedures; along with associated system generated event logging and notifications, to determine processes were in place to detect changes to software and configuration parameters that could be indicative of unauthorized or malicious software.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.8 (Cont.)	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Uses a Defined Change Control Process—A management-defined change control process is used for the implementation of software.	Inspected the most current change management and software development lifecycle (SDLC) policies and procedures, along with the lifecycle of completed infrastructure change requests in the ticketing and project management software; and observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software to determine defined change control processes were utilized for software implementations.	No exceptions noted.
		Uses Anti-virus and Anti-malware Software—Anti-virus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.	Observed via walkthrough procedures and inspected the entity's cyber security (i.e., advanced anti-virus and anti-malware) and endpoint protection management consoles, policies enabled, and endpoints protected; along with associated system generated event logging and notifications, to determine anti-virus and anti-malware software was implemented and maintained.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.8 (Cont.)	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.	Observed via walkthrough procedures and inspected the entity's cyber security and endpoint protection management consoles, policies enabled, and endpoints protected; along with associated system generated event logging and notifications, to determine procedures were in place to scan information assets for malware and unauthorized software and to remove items detected prior to implementation on the network.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**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.	Uses Defined Configuration Standards—Management has defined configuration standards.	Inspected the most current change management, SDLC, and network security policies and procedures and standards; and observed via walkthrough procedures and inspected the entity's source code repository and version control software to determine Management had defined configuration standards.	No exceptions noted.
		Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, and endpoint protection software consoles and system administration procedures, along with associated system generated event logging and notifications, to determine the entity monitored infrastructure and software for noncompliance with standards.	No exceptions noted.
		Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.	Observed via walkthrough procedures and inspected the entity's cloud security software consoles including the file integrity monitoring setting enabled to determine the IT system had change-detection mechanisms to alert personnel to unauthorized modifications of critical files of the system.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.1 (Cont.)	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.	Detects Unknown or Unauthorized Components—Procedures are in place to detect the introduction of unknown or unauthorized components.	Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, and endpoint protection software consoles and system administration procedures, along with associated system generated event logging and notifications, to determine procedures were in place to detect the introduction of unauthorized components.	No exceptions noted.
		Conducts Vulnerability Scans—The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.	Inspected most current vulnerability assessment and penetration testing attestations to determine the entity conducted vulnerability scans to identify potential vulnerabilities and took action to remediate deficiencies on a timely basis.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
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.	Implements Detection Policies, Procedures, and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, along with the most current incident response policy and procedures, to determine detection policies and procedures were defined for security event detection. Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, and endpoint protection software consoles and system administration procedures; along with associated system generated event logging and notifications, to determine the entity utilized detection tools on infrastructure and software to identify anomalies in the operation or unusual activity on systems.	No exceptions noted. No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.2 (Cont.)	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.	Designs Detection Measures—Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.	Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, and endpoint protection software consoles and system administration procedures; along with associated system generated event logging and notifications, to determine detection measures were designed to identify anomalies that could result in security threats.	No exceptions noted.
		Implements Filters to Analyze Anomalies—Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.	Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, and endpoint protection software consoles and system administration procedures; along with associated system generated event logging and notifications; and inspected completed security event change requests in the ticketing and project management software to determine Management implemented procedures to process anomalies to identify security events.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.2 (Cont.)	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.	Monitors Detection Tools for Effective Operation—Management has implemented processes to monitor the effectiveness of detection tools.	Inspected cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, along with the entity's risk management program (i.e., ongoing risk assessments, risk ratings, and risk mitigation activities); and observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cyber security, threat detection / prevention, and endpoint protection software consoles and system administration procedures; along with associated system generated event logging and notifications, to determine Management implemented processes to monitor the effectiveness of detection tools.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Responds to Security Incidents—Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine procedures were in place for responding to security incidents and evaluating the effectiveness of policies and procedures on a periodic basis.	No exceptions noted.
		Communicates and Reviews Detected Security Events—Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.	Inspected completed security event change requests in the ticketing and project management software, to determine detected security events were communicated and reviewed by Management and actions were taken when necessary.	No exceptions noted.
		Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine procedures were in place to analyze security incidents and identify system impact.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**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.	Assigns Roles and Responsibilities—Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.	Inspected the most current incident response policy and procedures to determine roles and responsibilities for the program were assigned.	No exceptions noted.
		Contains and Responds to Security Incidents—Procedures are in place to respond to and contain security incidents that actively threaten entity objectives.	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine procedures were in place to contain security incidents.	No exceptions noted.
		Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents.	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine procedures were in place to mitigate the effects of ongoing security incidents.	No exceptions noted.
		Resolves Security Incidents—Procedures are in place to resolve security incidents through closure of vulnerabilities, removal of unauthorized access, and other remediation actions.	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine procedures were in place to resolve security incidents through closure of vulnerabilities and other remediation actions.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.4 (Cont.)	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Restores Operations—Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.	Inspected the most current disaster recovery processes and procedures and associated testing results; observed via walkthrough procedures and inspected automated database snapshot logs and backup job status indicators in the entity's IaaS backup management console; and inspected documented processes and procedures for full system restores of production applications, along with completed backup and recovery requests including case history for each ticket, to determine procedures were in place to restore data and business operations.	No exceptions noted.
		Develops and Implements Communication of Security Incidents—Protocols for communicating, in a timely manner, information regarding security incidents and actions taken to affected parties are developed and implemented to support the achievement of the entity's objectives.	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine protocols for communicating security incidents and actions to be taken were developed and implemented in a timely manner.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.4 (Cont.)	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Obtains Understanding of Nature of Incident and Determines Containment Strategy—An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine the nature and severity of security incidents were evaluated for appropriate containment strategies.	No exceptions noted.
		Remediates Identified Vulnerabilities—Identified vulnerabilities are remediated through the development and execution of remediation activities.	Inspected a resolved security incident ticket including case history to determine identified vulnerabilities were remediated through the development and execution of remediation activities.	No exceptions noted.
		Communicates Remediation Activities—Remediation activities are documented and communicated in accordance with the incident response program.	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine remediation activities were documented and communicated in accordance with the incident response program.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.4 (Cont.)	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Evaluates the Effectiveness of Incident Response—The design of incident response activities is evaluated for effectiveness on a periodic basis.	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine the design of the incident response activities was evaluated for effectiveness on a periodic basis.	No exceptions noted.
		Periodically Evaluates Incidents—Periodically, Management reviews incidents related to security and identifies the need for system changes based on incident patterns and root causes.	Inspected a resolved security incident ticket including case history to determine Management periodically reviewed incidents related to security and identified needed system changes based on incident patterns and root causes.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Restores the Affected Environment—The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.	Inspected the most current disaster recovery processes and procedures and associated testing results; observed via walkthrough procedures and inspected automated database snapshot logs and backup job status indicators in the entity's IaaS backup management console; and inspected documented processes and procedures for full system restores of production applications, completed backup and recovery requests including case history for each ticket, and completed patch update tickets including case history for each request to determine activities were in place to rebuild systems, update software, as well as install patches and change configurations as needed.	No exceptions noted.
		Communicates Information About the Incident—Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security incidents are made to Management and others as appropriate (internal and external).	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine procedures were in place for communications of incident details to Management and associated stakeholders.	No exceptions noted.
		Determines Root Cause of the Incident—The root cause of the incident is determined.	Inspected a resolved security incident ticket including case history to determine the root cause of the incident was determined.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.5 (Cont.)	The entity identifies, develops, and implements activities to recover from identified security incidents.	Implements Changes to Prevent and Detect Recurrences—Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.	Inspected a resolved security incident ticket including case history to determine additional changes to preventative and detective controls were implemented to prevent and detect recurrences on a timely basis.	No exceptions noted.
		Improves Response and Recovery Procedures—Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.	Inspected the most current incident response policy and procedures, along with a resolved security incident ticket including case history, to determine lessons learned were analyzed with respect to incident response plan and process improvement.	No exceptions noted.
		Implements Incident Recovery Plan Testing—Incident recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.	Inspected the most current business continuity plan, along with the most current disaster recovery processes and procedures and associated testing results, to determine incident recovery plan testing was performed on a periodic basis.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Change Management**			
CC8.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**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.	Manages Changes Throughout the System Lifecycle—A process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software, and manual and automated procedures) is used to support the achievement of entity objectives.	Inspected the most current change management and SDLC policies and procedures, along with the lifecycle of completed infrastructure change requests in the ticketing and project management software; and observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software to determine a process for managing system changes throughout the lifecycle of the system and its components was used to support the achievement of entity objectives.	No exceptions noted.
		Authorizes Changes—A process is in place to authorize system and architecture changes prior to design, development, or acquisition and configuration.	Inspected the most current change management and SDLC policies and procedures, along with the lifecycle of completed infrastructure change requests in the ticketing and project management software; and observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software to determine a process was in place to authorize system changes prior to design, development, and configuration.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Change Management (Continued)**			
CC8.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC8.1 (Cont.)	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Designs and Develops Changes—A process is in place to design and develop system changes in a secure manner to support the achievement of entity objectives.	Observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software to determine a process was in place to design and develop system changes in a secure manner.	No exceptions noted.
		Documents Changes—A process is in place to document system changes to support ongoing maintenance of the system and to support internal and external users in performing their responsibilities.	Inspected the lifecycle of completed infrastructure change requests in the ticketing and project management software; and observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software to determine a process was in place to document system changes to support ongoing maintenance of the system and users in performing their responsibilities.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Change Management (Continued)**			
CC8.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC8.1 (Cont.)	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Tracks System Changes—A process is in place to track system changes prior to implementation.	Inspected the lifecycle of completed infrastructure change requests in the ticketing and project management software; and observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software to determine a process was in place to track system changes prior to implementation.	No exceptions noted.
		Configures Software—A process is in place to select, implement, maintain, and monitor configuration parameters used to control the functionality of developed and acquired software.	Observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software, along with the entity's source code repository and version control software, to determine a process was in place to select, implement, maintain, and monitor configuration parameters used to control functionality of software.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Change Management (Continued)**			
CC8.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC8.1 (Cont.)	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Tests System Changes—A process is in place to test internally developed and acquired system changes prior to implementation into the production environment. Examples of testing may include unit, integration, regression, static and dynamic application source code, quality assurance, or automated testing (whether point in time or continuous). Approves System Changes—A process is in place to approve system changes prior to implementation.	Observed via walkthrough procedures and inspected the lifecycle of completed application development code builds in the ticketing and project management software, and conducted corroborative inquiry of Application Development Management to determine a process was in place to test system changes prior to implementation into the production environment. Inspected the lifecycle of completed infrastructure change requests in the ticketing and project management software; and observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software to determine a process was in place to approve system changes prior to implementation.	No exceptions noted. No exceptions noted.

9	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Change Management (Continued)**			
CC8.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC8.1 (Cont.)	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Deploys System Changes—A process is in place to implement system changes with consideration of segregation of responsibilities (for example, restricting unilateral code development or testing and implementation by a single user) to prevent or detect unauthorized changes.	Observed via walkthrough procedures and inspected the lifecycle of completed application development code builds in the ticketing and project management software, the entity's release management process, and conducted corroborative inquiry of Development Operations Management to determine a process was in place to deploy system changes in a secure manner.	No exceptions noted.
		Identifies and Evaluates System Changes—Objectives affected by system changes are identified, and the ability of the modified system to support the achievement of the objectives is evaluated throughout the system development life cycle.	Inspected the lifecycle of completed infrastructure change requests in the ticketing and project management software; observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software; and conducted corroborative inquiry of Application Development and Development Operations Management to determine objectives of system changes were evaluated throughout the system development lifecycle.	No exceptions noted.

9	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Change Management (Continued)**			
CC8.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC8.1 (Cont.)	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents—Changes in infrastructure, data, software, and procedures required to remediate incidents are identified and the change process is initiated upon identification.	Inspected a resolved security incident ticket including case history to determine changes to the system to remediate incidents were identified and the change process was initiated upon identification.	No exceptions noted.
		Creates Baseline Configuration of IT Technology—A baseline configuration of IT and control systems is created and maintained.	Inspected the most current change management and SDLC policies and procedures, along with the lifecycle of completed infrastructure change requests in the ticketing and project management software; and observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software, along with the entity's source code repository and version control software, to determine a baseline configuration of IT and control systems was created and maintained.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Change Management (Continued)**			
CC8.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC8.1 (Cont.)	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Provides for Changes Necessary in Emergency Situations—A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent timeframe).	Inspected completed emergency change requests including case history for each ticket to determine a process was in place for the lifecycle management of emergency change requests.	No exceptions noted.
		Manages Patch Changes—A process is in place to identify, evaluate, test, approve, and implement patches in a timely manner on infrastructure and software.	Inspected completed patch update requests including case history for each ticket to determine a process was in place to manage the implementation of patches in a timely manner on infrastructure and software.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Mitigation**			
CC9.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Considers Mitigation of Risks of Business Disruption—Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the entity's objectives during response, mitigation, and recovery efforts.	Inspected the most current business continuity plan, the entity's risk management program (i.e., ongoing risk assessments, risk ratings, and risk mitigation activities), and most current disaster recovery processes and procedures and associated testing results to determine the entity considered mitigation of risks of business disruption and had policies and procedures in place to meet entity objectives.	No exceptions noted.
		Considers the Use of Insurance to Mitigate Financial Impact Risks—The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.	Inspected the most current certificates of liability insurance from the entity's insurance provider to determine risk management activities considered the use of insurance to offset the impact of loss events.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Mitigation (Continued)**			
CC9.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Establishes Requirements for Vendor and Business Partner Engagements—The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.	Inspected executed vendor and client agreements, most current vendor risk management policy and processes, and most current SOC reports of the entity's subservice organizations to determine the entity established specific requirements for vendor and business partner engagements that included scope of services and specifications, roles and responsibilities, compliance requirements, and service levels.	No exceptions noted.
		Identifies Vulnerabilities—The entity evaluates vulnerabilities arising from vendor and business partner relationships, including third-party access to the entity's IT systems and connections with third party networks.	Inspected executed vendor and client agreements, the entity's risk management program, most current vendor risk management policy and processes, and most current SOC reports of the entity's subservice organizations to determine the entity evaluated vulnerabilities from vendor and business partner relationships and third party access to the entity's systems.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Mitigation (Continued)**			
CC9.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC9.2 (Cont.)	The entity assesses and manages risks associated with vendors and business partners.	Assesses Vendor and Business Partner Risks—The entity inventories, tiers, and assesses, on a periodic basis, threats arising from relationships with vendors and business partners (and those entities' vendors and business partners) and the vulnerability of the entity's objectives to those threats. Examples of threats arising from relationships with vendors and business partners include those arising from their (1) financial failure, (2) security vulnerabilities, (3) operational disruption, and (4) failure to meet business or regulatory requirements.	Inspected executed vendor and client agreements, the entity's risk management program, most current vendor risk management policy and processes, and most current SOC reports of the entity's subservice organizations to determine vendor and business partner risks were assessed on a periodic basis.	No exceptions noted.
		Assigns Responsibility and Accountability for Managing Vendors and Business Partners—The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.	Inspected executed vendor and client agreements, the entity's risk management program, most current vendor risk management policy and processes, and most current SOC reports of the entity's subservice organizations to determine the entity assigned responsibility and accountability for the management of risks associated with vendors and business partners.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Mitigation (Continued)**			
CC9.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC9.2 (Cont.)	The entity assesses and manages risks associated with vendors and business partners.	Establishes Communication Protocols for Vendors and Business Partners—The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.	Inspected executed vendor and client agreements, along with the online support and knowledge base user interfaces, term and conditions, and service agreements, to determine the entity established communication and resolution protocols for service issues related to vendors and business partners.	No exceptions noted.
		Establishes Exception Handling Procedures from Vendors and Business Partners—The entity establishes exception handling procedures for service or product issues related to vendors and business partners.	Inspected executed vendor and client agreements, along with the online support and knowledge base user interfaces, term and conditions, and service agreements, to determine the entity established exception handling procedures for service issues related to vendors and business partners.	No exceptions noted.
		Assesses Vendor and Business Partner Performance—The entity assesses the performance of vendors and business partners, as frequently as warranted, based on the risk associated with the vendor or business partner.	Inspected executed vendor and client agreements, the entity's risk management program, most current vendor risk management policy and processes, and most current SOC reports of the entity's subservice organizations to determine the entity assessed the performance of vendors and business partners as frequently as warranted.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Risk Mitigation (Continued)**			
CC9.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC9.2 (Cont.)	The entity assesses and manages risks associated with vendors and business partners.	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments—The entity implements procedures for addressing issues identified with vendor and business partner relationships.	Inspected executed vendor and client agreements, along with the online support and knowledge base user interfaces, term and conditions, and service agreements, to determine the entity implemented procedures for addressing issues identified with vendor and business partner relationships.	No exceptions noted.
		Implements Procedures for Terminating Vendor and Business Partner Relationships—The entity implements procedures for terminating vendor and business partner relationships based on predefined considerations. Those procedures may include safe return of data and its removal from the vendor or business partner system.	Inspected executed vendor and client agreements, along with the most current vendor risk management policy and processes, to determine the entity implemented procedures for terminating vendor and business partner relationships in an appropriate manner.	No exceptions noted.