

Matillion Limited

SOC 1 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

September 1, 2025 to August 31, 2026



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 ____ *7*

Management Assertions Letter ____ **8**

Description of Relevant Controls Provided by Matillion Limited ____ **10**

Company Overview ____ 10

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication ____ **16**

Control Environment ____ 16

Risk Assessment and Management ____ 23

Monitoring ____ 24

Information and Communication ____ 24

User Control Considerations ____ 25

III. Information Provided by Ascend Audit & Advisory ____ *27*

Control Objectives, Related Controls, and Tests of Operating Effectiveness ____ **28**

Control Objective 1 – Organization and Administration ____ 28

Control Objective 2 – Human Resources Security ____ 30

Control Objective 3 – Data Backup and Recovery ____ 33

Control Objective 4 – Computer Operations ____ 34

Control Objective 5 – Logical Access ____ 36

Control Objective 6 – Data Communications ____ 37

Control Objective 7 – Data Transmission ____ 38

Control Objective 8 – Disaster Recovery Preparedness ____ 39

Control Objective 9 – Secure Storage, Media, Document Destruction ____ 40

Control Objective 10 – Application Development and Change Management ____ 41

Control Objective 11 – Infrastructure Change Management ____ 44

Control Objective 12 – Support Operations ____ 46

Control Objective 13 – Risk Assessment and Internal Audit ____ 47

I. Independent Service Auditor's Report

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

INDEPENDENT SERVICE AUDITOR'S REPORT

Graeme Park
Chief Information Security Officer
Matillion Limited
Two, New Bailey St, Stanley St
Salford M3 5GS, United Kingdom

Scope

We have examined Matillion Limited's ("Matillion" or "the Company") description of its Matillion Platform (Matillion Data Loader, Change Data Capture, Matillion ETL, Data Productivity Cloud) System for processing user entities' transactions throughout the period September 1, 2025 to August 31, 2026 and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

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. The description presents Matillion's controls 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.

Matillion Limited's Responsibilities

In Section II of this report, the Company provided an assertion about the fair presentation of the description and the suitability of design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Company is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria; and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Ascend Audit & Advisory's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination 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 fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period September 1, 2025 to August 31, 2026.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described beginning in Section II. 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.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in the Company's assertion in Section II of this report,

a. The description fairly presents the Matillion Platform System that was designed and implemented throughout the period September 1, 2025 to August 31, 2026.

b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period September 1, 2025 to August 31, 2026 and user entities applied the complementary user entity controls contemplated in the design of the Company's controls throughout the period September 1, 2025 to August 31, 2026.

c. The controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period September 1, 2025 to August 31, 2026.

Description of Tests of Controls

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

Restricted Use

This report and the description of tests of controls and results thereof in Section III of this report are intended solely for the information and use of the Company, user entities of the Company's Matillion Platform System throughout the period September 1, 2025 to August 31, 2026, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about the controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Ascend Audit & Advisory

ASCEND
AUDIT & ADVISORY

St. Petersburg, FL

September 24, 2026

II. Information Provided by Matillion Limited

MANAGEMENT ASSERTIONS LETTER

We have prepared the description of Matillion Limited's Matillion Platform (Matillion Data Loader, Change Data Capture, Matillion ETL, Data Productivity Cloud) System ("description") for user entities of the system throughout the period September 1, 2025 to August 31, 2026, and their user auditors who have sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

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. The description presents Matillion's controls 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.

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

a. The description fairly presents the Matillion Platform System throughout the period September 1, 2025 to August 31, 2026 for processing their transactions. The criteria we used in making this assertion were that the description:

   i. Presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including, if applicable:

      1) The types of services provided including, as appropriate, the classes of transactions processed.

      2) The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.

      3) The related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

      4) How the system captures significant events and conditions, other than transactions.
      5) The process used to prepare reports and other information for user entities.

6) The specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the Company's controls.

7) Other aspects of the control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

ii. Does not omit or distort information relevant to the scope of the Matillion Platform System, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Matillion Platform system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

c. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period September 1, 2025 to August 31, 2026 to achieve those control objectives. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization,

ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

By: /S/ Graeme Park

Graeme Park
Chief Information Security Officer

September 24, 2026

DESCRIPTION OF RELEVANT CONTROLS PROVIDED BY MATILLION LIMITED

Company Overview

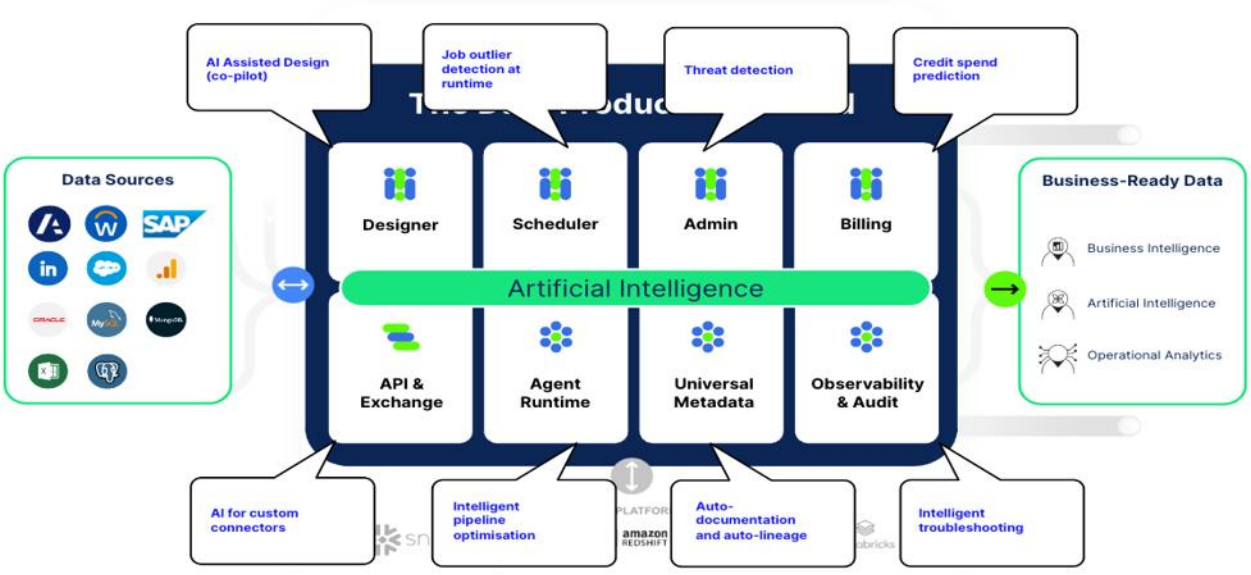
Matillion is a global company, founded in Manchester. Matillion has a globally distributed workforce working between dual headquarters in Denver, CO and Manchester (UK). 1200+ companies including Cisco, DocuSign, Pacific Life, Slack, and TUI trust Matillion to move, transform and automate their data.

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.



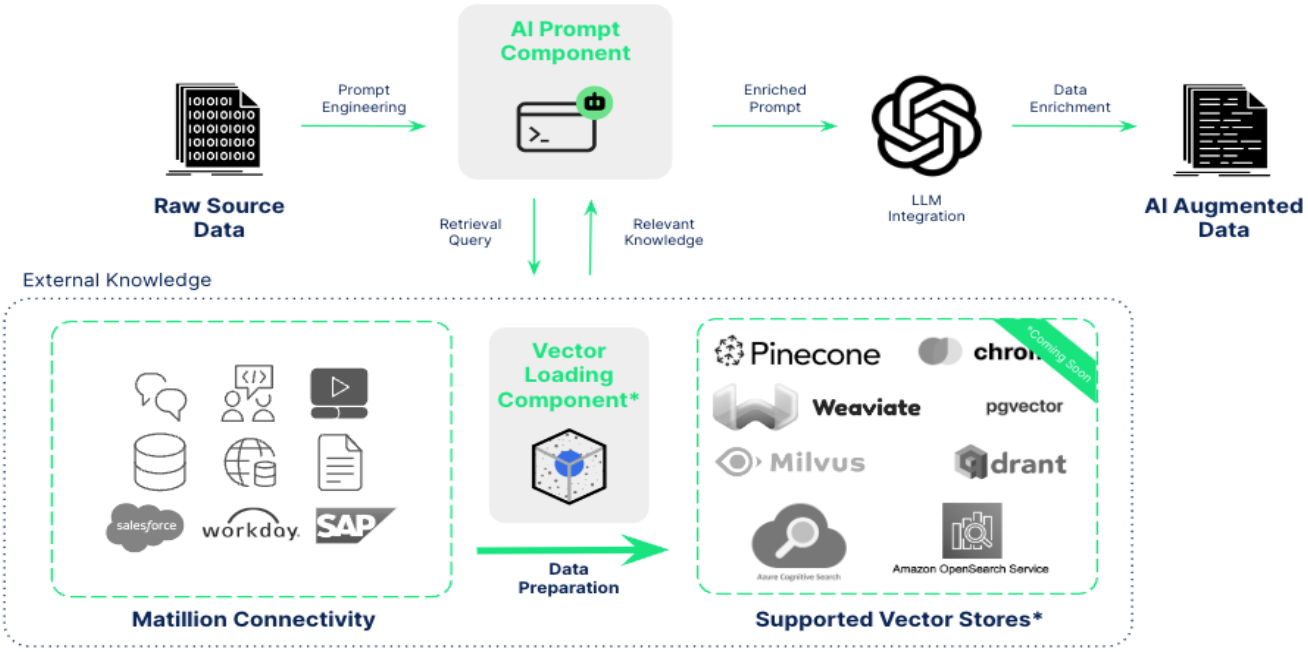
Key benefits of AI Prompt Components and Retrieval Augmented Generation with Matillion:

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

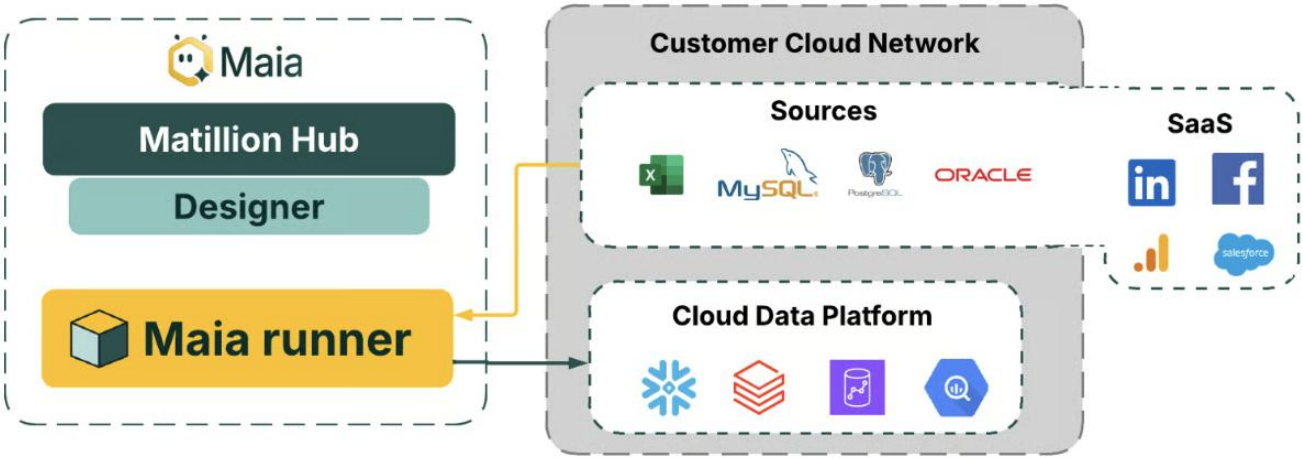
In addition to the Maia Foundation, Maia is made up of two further integrated components that this document previously omitted: Maia Team and the Context Engine. Maia Team is the agentic layer of Maia - an always-on team of AI agents (sometimes referred to internally as Maia agents) that operates inside 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 Maia runner 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

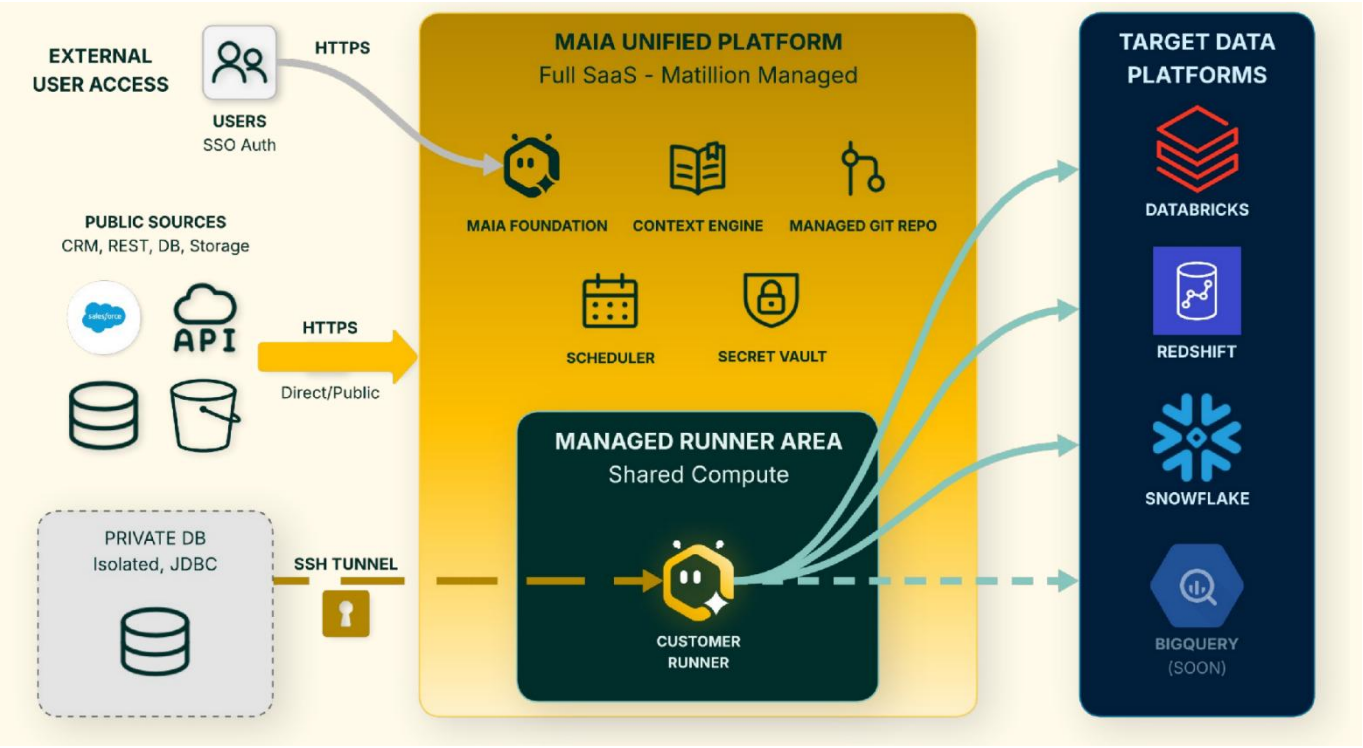
Matillion Hub – serves as the central place for administering and monitoring Maia Foundation. This Web based application offers a multi-tenant environment, allowing users to access and manage their specific environments and data pipelines efficiently. One of the key features of Hub is its ability to 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.

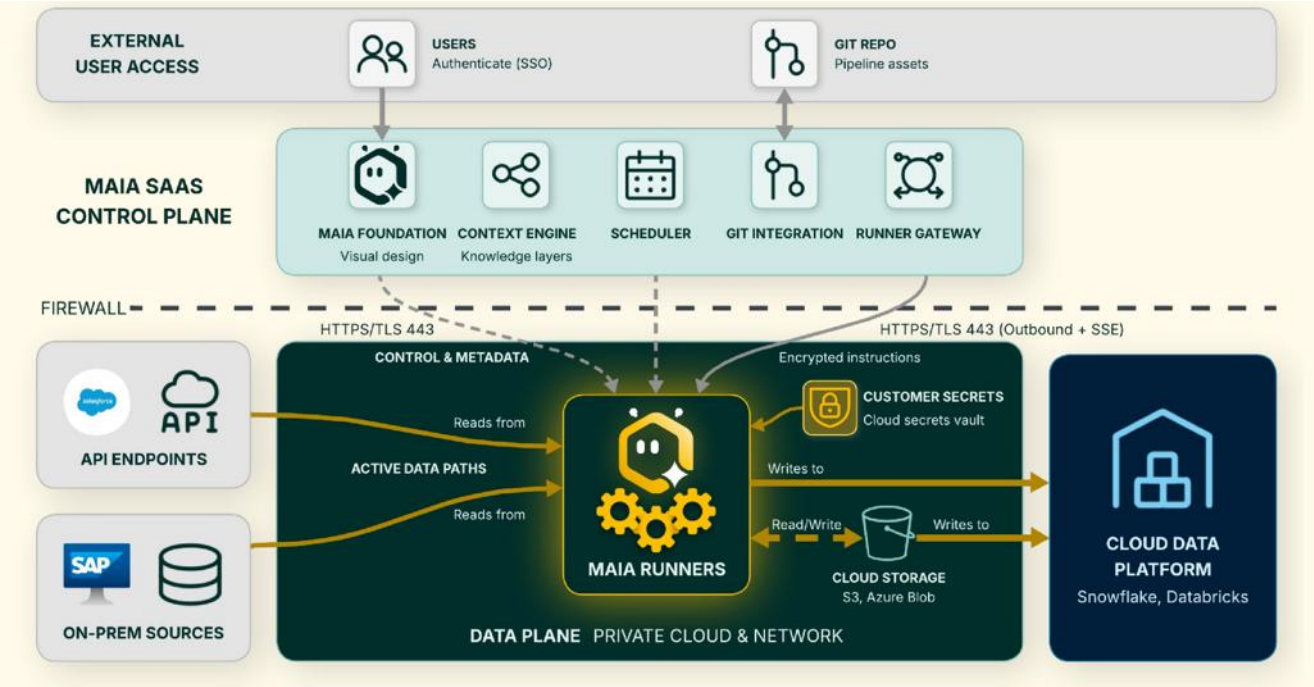
Designer – is a comprehensive and fully managed data pipeline builder. This SaaS Web based application empowers users to create robust and efficient data integration workflows with ease.

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 Agents 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 Agent(s) connect to the Hub to retrieve pipelines and schedules, and to provide pipeline execution status for system observability. Agents connect directly to sources and targets, limiting the “hops” of data in transit. Agents 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 agents, which orchestrate data pipelines from Matillion’s control plane, or with customer-hosted Agents 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. Matillion Data Productivity Cloud 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.

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

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the structure of business activities, establishment of objectives, and assessment of risks. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent personnel, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in pursuit of the organization's objectives.

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

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

Management Controls, Philosophy, 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.

Organization 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.

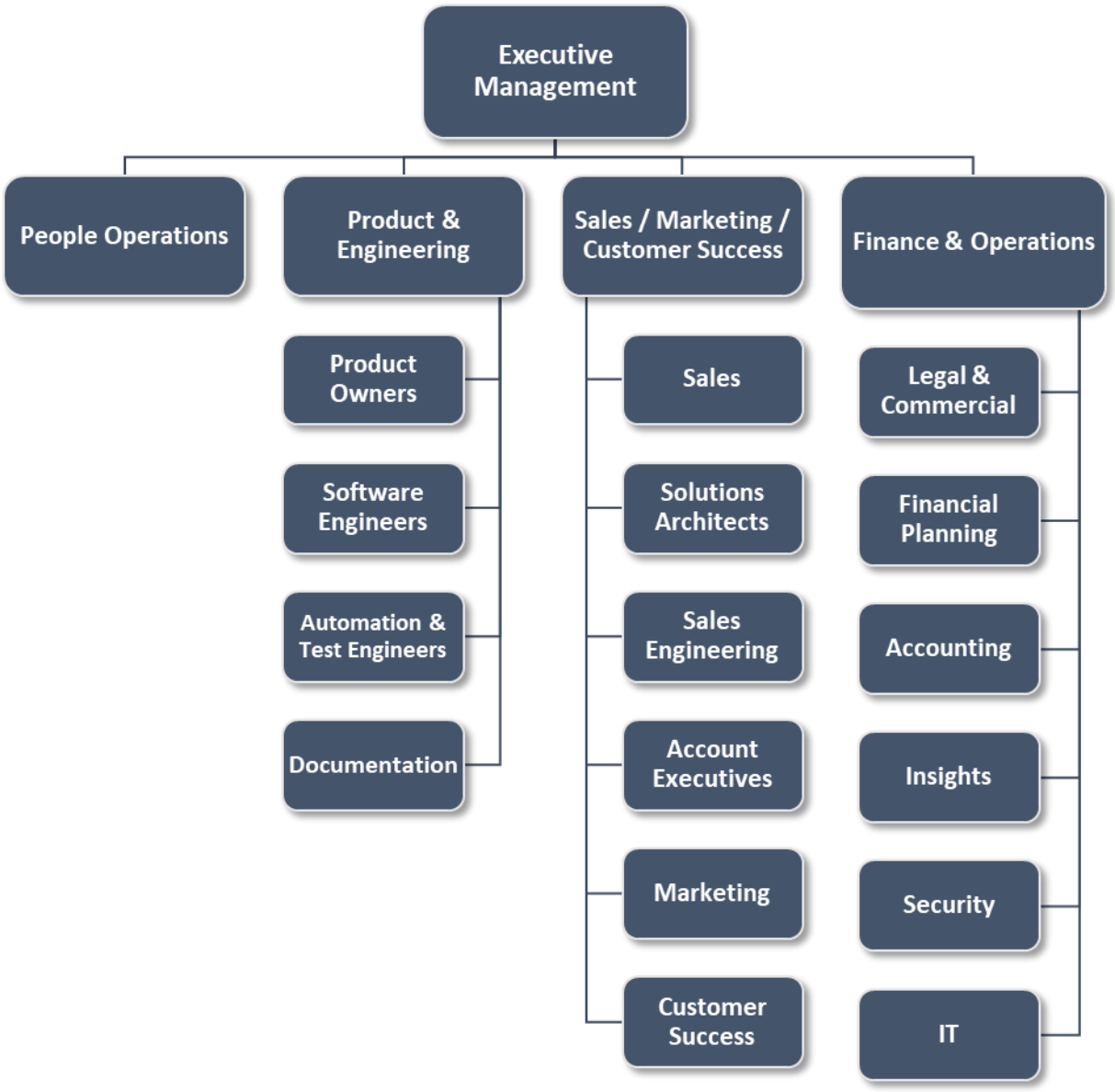
Assignment of Authority and Responsibility

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 Matillion team member'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 are 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 responsible 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.

Security Awareness

Each member of Matillion is made aware of the security implications that revolve around their functions and actions. Approaching security as an organization has a more profound effect than relying solely on a single group. This process begins with providing individuals with the understanding and knowledge needed to help secure them and their data within established policies. Security awareness programs include the message that individual users can have a significant impact on the overall security of an organization.

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 comprising 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.

Insurance Policies

Matillion maintains insurance coverage in order to transfer certain risks including, but not limited to, the following coverage:

- Employer liability
- Public and products liability
- Professional indemnity
- Cyber liability

Additional insurance policies may be acquired as needed to transfer identified risks or in performance of contractual obligations.

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.

Control Objectives and Related Controls

Section III of this report includes Matillion control objectives and related control activities to eliminate the redundancy that would result from listing them here in Section II and repeating them in Section III. Although the control objectives and related control activities are included in Section III, they are, nevertheless, an integral part of the Matillion description of controls.

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.

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

CONTROL OBJECTIVES, RELATED CONTROLS, AND TESTS OF OPERATING EFFECTIVENESS

Control Objective 1 – Organization and Administration

CO1 – Controls provide reasonable assurance Management provides oversight and segregation of duties and guides consistent implementation of security policies.

C1.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C1.1	Matillion has an information security policy that guides personnel on procedures and policies to ensure information security within the organization.	Inspected the most current information security policy and procedures to determine the policy was in place and guided personnel on procedures and policies to ensure information security within the organization.	No exceptions noted.
C1.2	An organizational chart is in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel and is updated on an annual basis.	Inspected the entity's most current organizational charts to determine organizational charts were in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel and was updated during the period under review.	No exceptions noted.
C1.3	The Company is segregated into separate and distinct functional areas for the purposes of management of customer information, processing of the information, and to ensure adequate separation of duties.	Inspected the entity's most current organizational charts; and observed via walkthrough procedures and inspected the entity's system monitoring, infrastructure-as-a-service (IaaS) and cloud and cybersecurity, threat detection / prevention, and endpoint protection software consoles and system administration procedures to determine the Company was segregated into separate, logical, and distinct functional areas and that a reasonable separation of duties existed.	No exceptions noted.
C1.4	The Company has a code of business conduct and ethics that guides employees on the organization's ethical principles and conduct.	Inspected the entity's most current employee handbook including the business conduct and ethics policy, along with the most current culture code, to determine a code of conduct was in place to guide employees on the organization's ethical principles and conduct.	No exceptions noted.

Control Objective 1 – Organization and Administration (Continued)

CO1 – Controls provide reasonable assurance Management provides oversight and segregation of duties and guides consistent implementation of security policies.

C1.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C1.5	The organization has documented job descriptions that describe the roles and responsibilities of the position.	Inspected the entity's online repository for enterprise-wide job descriptions to determine they were in place and described the roles and responsibilities of the position.	No exceptions noted.
C1.6	Management meetings are held on a regular basis to discuss operational issues.	Inspected board of directors and Management meeting minutes regarding operational objectives and updates, along with cyber security subcommittee and weekly organizational objectives and updates communicated to personnel, to determine Management meetings were held on a regular basis to discuss operational issues.	No exceptions noted.
C1.7	The Company maintains insurance to safeguard against losses due to: • Employer liability • Public and products liability • Professional indemnity • Cyber liability	Inspected the most current certificates of liability insurance from the entity's insurance provider to determine current policies were in place to safeguard against loss due to: • Employer liability • Public and products liability • Professional indemnity • Cyber liability	No exceptions noted.

Control Objective 2 – Human Resources Security

CO2 – Controls provide reasonable assurance employees understand their responsibilities, are suitable for the roles they are considered for, exit the organization or change employment in an orderly manner, and guide consistent implementation of security practices.

C2.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C2.1	Management assesses each job candidate to ascertain whether the candidate possesses the requisite level of competence to fill the job position by conducting a review of position-related qualifications and interview procedures.	Inspected the entity's documented talent acquisition procedures and conducted corroborative inquiry of HR Management to determine Management assessed job candidates to ascertain whether candidates possessed the requisite level of competence to fill the position by conducting a review of position-related qualifications and interview procedures.	No exceptions noted.
C2.2	Management has documented HR policies and practices related to hiring, orientation, performance management, and professional development.	Inspected the entity's documented talent acquisition and new hire onboarding and orientation procedures, most current employee handbook and progressive disciplinary policy and procedures, employee performance policy and procedures, and completed compliance and departmental training recordkeeping to determine Management had documented HR policies and practices for hiring, orientation, performance management, and professional development.	No exceptions noted.
C2.3	New hire onboarding procedures are used to ensure new staff receive the appropriate level of access to information systems.	For the selection of new employees, inspected completed new employee access provisioning requests including case history for each ticket to determine new hire onboarding procedures were used to ensure new staff received the appropriate level of access to information systems.	No exceptions noted.

Control Objective 2 – Human Resources Security (Continued)

CO2 – Controls provide reasonable assurance employees understand their responsibilities, are suitable for the roles they are considered for, exit the organization or change employment in an orderly manner, and guide consistent implementation of security practices.

C2.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C2.4	Management ensures employees are subjected to a background check during the hiring and onboarding process.	For the selection of new employees, inspected completed background check confirmations to determine Management ensured employees were subjected to background checks as a condition of employment and part of the onboarding process.	No exceptions noted.
C2.5	An acceptable use policy is in place that guides staff on the appropriate use of Company computers, information systems, and adherence to security policies.	Inspected the most current acceptable use policies to determine the policy was in place and guided staff on the appropriate use of Company computers, information systems, and adherence to security policies.	No exceptions noted.
C2.6	New employees must sign and acknowledge policies and procedures in the employee handbook and confidentiality and nondisclosure agreement as part of the onboarding process.	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 new employees signed and acknowledged policies and procedures in the employee handbook and confidentiality and nondisclosure agreement as part of the onboarding process.	No exceptions noted.
C2.7	Employees are required to complete security awareness training on an annual basis.	For the selection of active employees, inspected security awareness training course completion reporting to determine employees completed security awareness training, annually.	No exceptions noted.

Control Objective 2 – Human Resources Security (Continued)

CO2 – Controls provide reasonable assurance employees understand their responsibilities, are suitable for the roles they are considered for, exit the organization or change employment in an orderly manner, and guide consistent implementation of security practices.

C2.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C2.8	Management maintains a disciplinary policy for employees who are suspected of rule infractions or violations of Company policies.	Inspected the entity's most current progressive disciplinary policy and procedures to determine Management maintained a disciplinary policy to address employee nonconformities.	No exceptions noted.
C2.9	Termination procedures are in place to confirm the revocation of system access privileges as a component of the employee termination process.	For the selection of terminated employees, inspected terminated employee access deprovisioning requests, along with confirmations of associated accounts disabled, to determine terminated employee revocation of system access was completed in an orderly and timely manner.	No exceptions noted.

Control Objective 3 – Data Backup and Recovery

CO3 – Controls provide reasonable assurance data is backed up regularly and is available for restoration in the event of processing errors or unexpected processing interruptions.

C3.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C3.1	Management maintains documented backup policies and procedures to guide personnel on the Company's requirements for backing up critical data.	Inspected entity's most current data backup policy and procedures to determine Management maintained documentation to guide personnel on the requirements for backing up critical data.	No exceptions noted.
C3.2	Automated backup systems are utilized to perform scheduled system backups of target data.	Observed via walkthrough procedures and inspected automated database snapshot logs and backup job status indicators in the entity's IaaS backup management console to determine automated backup systems were utilized to perform scheduled system backups of target data.	No exceptions noted.
C3.3	Backup jobs are logged and monitored in the event of backup failure.	Observed via walkthrough procedures and inspected logs and status indicators of automated daily database snapshots in the entity's IaaS management console to determine backup jobs were monitored in the event of backup job success or failure.	No exceptions noted.
C3. 4	Restores of systems and data are performed as a component of normal business operations to verify system components can be recovered and target data restored.	Inspected the most current disaster recovery processes and procedures and associated testing results, documented processes and procedures for full system restores of production applications, and completed backup and recovery tickets including case history; and observed via walkthrough procedures and inspected automated daily database snapshot logs and the data restore process to determine restores of systems and data were performed as a component of normal business operations to verify system components were recovered and target data restored.	No exceptions noted.

Control Objective 4 – Computer Operations

CO4 – Controls provide reasonable assurance systems are maintained in a manner that helps ensure system availability.

C4.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C4.1	Monitoring applications are utilized to monitor infrastructure and software for noncompliance with standards and sends alert notifications to operations personnel when predefined thresholds are exceeded on monitored computing resources.	Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cybersecurity, threat detection / prevention, and endpoint protection software consoles and system administration procedures, along with associated system generated event logging and notifications, to determine monitoring applications were utilized to monitor infrastructure and software and sent notifications to operations personnel when predefined events occur.	No exceptions noted.
C4.2	The Company has a security incident response policy in place to provide policy guidance for responding to and reporting security incidents.	Inspected the most current incident response policy and procedures to determine the policy was in place and guided personnel on responding to and reporting security incidents.	No exceptions noted.
C4.3	Anti-virus software is maintained and scans computing resources and endpoint devices on a real-time basis.	Observed via walkthrough procedures and inspected the entity's cybersecurity (with 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 software scanned production resources and endpoint devices on a real-time basis.	No exceptions noted.
C4.4	Anti-virus software is configured to notify cyber security operations of malware and unauthorized software detected, prevented and removed.	Observed via walkthrough procedures and inspected the entity's cybersecurity (with advanced anti-virus and anti-malware) management console, along with system generated event logging and notifications to determine anti-virus software notified personnel of malware and unauthorized software security events.	No exceptions noted.

Control Objective 4 – Computer Operations (Continued)

CO4 – Controls provide reasonable assurance systems are maintained in a manner that helps ensure system availability.

C4.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C4.5	Policies and procedures are in place for patch management on production systems.	Inspected completed patch update tickets including case history for each request to determine policies and procedures were in place for patch management on production systems.	No exceptions noted.

Control Objective 5 – Logical Access

CO5 – Controls provide reasonable assurance network logical security settings prevent unauthorized access to infrastructure, limit access to computing resources based on business need, and provide Management with an audit trail of certain events that occur within the infrastructure and computing environments.

C5.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C5.1	Password complexity is required for users accessing the entity's IaaS and enterprise applications and must meet the following standards: • Minimum length • Reuse history • Maximum age • Account lockout • Password complexity	Observed via walkthrough procedures and inspected the password policy configured in the entity's identity and access management software to determine password complexity was required and enforced for users accessing IaaS and enterprise applications and met the following standards: • Minimum length • Reuse history • Maximum age • Account lockout • Password complexity	No exceptions noted.
C5.2	Security groups are configured and enforced by the entity's identity and access management software to ensure access is restricted to sensitive data stored in the entity's IaaS and enterprise applications.	Observed via walkthrough procedures and inspected system generated lists of authorized system administrators, users, and security groups of the entity's identity and access management software and enterprise applications to determine security groups were configured and enforced to restrict access to sensitive data stored in the entity's IaaS and enterprise applications.	No exceptions noted.
C5.3	User access rights to computing resources are reviewed for appropriateness on a periodic basis and as part of the Company's risk management posture.	Inspected completed logical access rights reviews for the entity's identity and access management system and enterprise applications, along with the entity's risk management program (i.e., ongoing risk assessments, risk ratings, and risk mitigation activities) to determine the entity reviewed access credentials on a periodic basis for appropriateness and as part of the entity's risk management posture.	No exceptions noted.

Control Objective 6 – Data Communications

CO6 – Control activities provide reasonable assurance the security infrastructure and practices secure against unauthorized access to the entity's infrastructure and threats from connections to external networks are limited.

C6.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C6.1	Perimeter protection (i.e., cloud-based firewall solution) is in place to prevent unauthorized identities, resources, and networks from accessing the entity's infrastructure, applications, and computing resources.	Observed via walkthrough procedures and inspected the virtual private cloud (VPC) management console, VPC instances and security groups, and associated inbound and outbound access rules of the entity's IaaS to determine perimeter protection was in place to prevent unauthorized identities, resources, and networks from accessing the entity's infrastructure, applications, and computing resources.	No exceptions noted.
C6.2	Management restricts the ability to administer the perimeter protection for the entity's IaaS to certain personnel.	Observed via walkthrough procedures and inspected the VPC management console, along with the associated security groups and membership, to determine the entity restricted the ability to administer the perimeter protection for the IaaS to authorized personnel only.	No exceptions noted.
C6.3	Processes are in place to monitor and remediate anomalies identified as security events, malicious and unusual activity on systems, and unauthorized access attempts. Events are logged and notifications are sent to system administrators for operational effectiveness and investigatory purposes.	Observed via walkthrough procedures and inspected the entity's system monitoring, IaaS and cloud and cybersecurity, 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 monitor and remediate suspicious activities on systems and notify personnel of security events.	No exceptions noted.

Control Objective 7 – Data Transmission

CO7 – Control activities provide reasonable assurance sensitive data and information is transmitted utilizing secure communication methods.

C7.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C7.1	Management maintains a remote access policy that provides Company requirements for remote access to internal systems and resources.	Inspected the remote access policy in the most current teleworking policy to determine the policy provided requirements for remote access to internal systems and resources.	No exceptions noted.
C7.2	Remote user VPN connections are utilized by staff to establish encrypted communication sessions to internal systems and resources.	Inspected the entity's remote access software (i.e., remote user VPN application), configuration, and advanced settings to determine VPN connections were in place and utilized by staff for establishing encrypted communication sessions to internal systems and resources.	No exceptions noted.
C7.3	Secure communication tunnels are in place for file transfers requiring encryption to the Company's Web server through the use of Secure Socket Layer (SSL) encryption.	Inspected the most current SSL certificate for the entity's Web server to determine secure communication tunnels were utilized for file transfers requiring encryption to the entity's Web server via SSL encryption.	No exceptions noted.

Control Objective 8 – Disaster Recovery Preparedness

CO8 – Controls provide reasonable assurance policies and procedures are in place to minimize disruption of processing activities and services to user organizations in the event of a business interruption or natural disaster.

C8.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C8.1	Management maintains a business continuity (and disaster recovery) plan with developed contingencies for assignments of responsibility for internal controls.	Inspected the most current business continuity plan and conducted corroborative inquiry of Management to determine Management developed and maintained a plan for assignments of responsibility for internal controls.	No exceptions noted.
C8.2	The business continuity (and disaster recovery) plan is reviewed by Management on at least an annual basis.	Inspected the most current business continuity plan and its revision history to determine Management reviewed and revised, if necessary, at least once during the period under review.	No exceptions noted.
C8.3	Certain aspects of the business continuity (and disaster recovery) plan are tested on an annual basis.	Inspected the most current business continuity plan, along with the most current disaster recovery processes and procedures and associated testing results, to determine certain aspects of the business continuity plan were tested during the period under review.	No exceptions noted.

Control Objective 9 – Secure Storage, Media, Document Destruction

CO9 – Controls provide reasonable assurance procedures are in place and followed regarding the destruction of electronic media and sensitive documents.

C9.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C9.1	Documented procedures are in place to ensure all media are physically destroyed rendering all sensitive information unreadable before being discarded.	Inspected the most current asset disposal policy and procedures, along with reporting of secure asset decommissioning, to determine documented procedures were in place and followed to ensure electronic media and assets were securely disposed of rendering sensitive information unreadable.	No exceptions noted.

Control Objective 10 – Application Development and Change Management

CO10 – Controls provide reasonable assurance new applications and changes to existing applications are authorized, tested, approved, properly implemented, and documented.

C10.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C10.1	The Company's application program code is designed and documented in accordance with written standards and procedures established by Management in their software development lifecycle (SDLC) documentation.	Inspected the most current change management and SDLC policies and procedures; 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 the entity's application development was designed and documented in accordance with Management's written standards.	No exceptions noted.
C10.2	A ticket tracking system is utilized for managing reported software releases, enhancements, and deficiencies through completion.	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 ticketing system was utilized to document and track software changes through completion.	No exceptions noted.
C10.3	Source code management software is utilized for version control of development projects and to control access to source code libraries.	Observed via walkthrough procedures and inspected the entity's source code repository and version control software to determine source code management software was utilized for version control and access control to source code libraries.	No exceptions noted.
C10.4	Separate source code environments exist for development, testing, and production to prevent making changes that would affect the performance, availability, and integrity of production application code.	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 logically separated source code environments and the release management process, to determine separate source code environments existed for development, testing, and production.	No exceptions noted.

Control Objective 10 – Application Development and Change Management (Continued)

CO10 – Controls provide reasonable assurance new applications and changes to existing applications are authorized, tested, approved, properly implemented, and documented.

C10.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C10.5	QA testing is documented and performed for development and maintenance activities prior to production release.	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 Management to determine QA testing was performed for development and maintenance activities prior to production release.	No exceptions noted.
C10.6	Depending on the nature of the change, the following types of testing are performed: regression testing, user acceptance testing, and performance load testing if required.	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 Management to determine depending on the nature of the change, the following types of testing were performed: regression testing, user acceptance testing, and performance load testing if required.	No exceptions noted.
C10.7	Development projects including features and enhancements are reviewed for feasibility, function, and must be approved by Management prior to development.	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 Management to determine development projects were subjected to Management review and approval prior to implementation into the production environment.	No exceptions noted.

Control Objective 10 – Application Development and Change Management (Continued)

CO10 – Controls provide reasonable assurance new applications and changes to existing applications are authorized, tested, approved, properly implemented, and documented.

C10.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C10.8	Management restricts the ability to move code into the production environment to specific personnel.	Observed via walkthrough procedures and inspected the lifecycle of completed application development code builds and releases in the ticketing and project management software, the release management process, and conducted corroborative inquiry of Application Development and Development Operations Management to determine Management restricted the ability to move code into the production environment to specific personnel.	No exceptions noted.

Control Objective 11 – Infrastructure Change Management

CO11 – Controls provide reasonable assurance new infrastructure and changes to existing infrastructure are authorized, tested, approved, properly implemented, and documented.

C11.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C11.1	A formal change management procedure is in place to provide guidance on infrastructure change implementations.	Inspected the most current change management policy and procedures to determine a formal change management procedure was in place to provide guidance on infrastructure change implementations.	No exceptions noted.
C11.2	Change requests are tracked in a ticket tracking system to record the initial change request throughout the lifecycle and completion of the change request.	Inspected the lifecycle of completed infrastructure change requests in the ticketing and project management software to determine change requests were tracked in a ticketing system from initial change request throughout the lifecycle and completion of the change request.	No exceptions noted.
C11.3	Changes are tested (when applicable) prior to being released into the production environment.	Inspected the lifecycle of completed infrastructure change requests in the ticketing and project management software, and conducted corroborative inquiry of IT Management to determine changes were tested (when applicable) prior to being released into the production environment.	No exceptions noted.
C11.4	System maintenance windows are scheduled, communicated, and managed according to the change management process.	Inspected the most current change management policy and procedures, along with a sample of production application maintenance notifications including start and duration details, to determine system maintenance windows were scheduled, communicated, and managed according to the change management process.	No exceptions noted.

Control Objective 11 – Infrastructure Change Management (Continued)

CO11 – Controls provide reasonable assurance new infrastructure and changes to existing infrastructure are authorized, tested, approved, properly implemented, and documented.

C11.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C11.5	Matillion maintains an emergency change management process for unscheduled or urgent change requests.	Inspected the emergency change management procedures in the most current change management policy and procedures, along with completed emergency change requests including case history for each ticket, to determine the entity had a process for unscheduled or emergency change requests.	No exceptions noted.
C11.6	Unscheduled or emergency changes are reviewed at completion following the change management close-out procedures.	Inspected the emergency change management procedures in the most current change management policy and procedures, completed emergency change requests including case history for each ticket, and conducted corroborative inquiry of IT Management to determine unscheduled or emergency change requests were reviewed at completion as per change management procedures.	No exceptions noted.

Control Objective 12 – Support Operations

CO12 – Controls provide reasonable assurance client issues are documented and completed in a timely and accurate manner.

C12.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C12.1	Management has documented client support procedures including service level commitments, hours of operation, and support contact information available to clients for reporting issues and remediation expectations.	Inspected the online support and knowledge base user interfaces, term and conditions and service agreements, release notes, and products and services updates to determine Management had documented client support procedures including service level commitments, hours of operation, and support contact information available to clients for reporting issues and remediation commitments.	No exceptions noted.
C12.2	Client reported problems are entered into a trouble ticket system. Tickets are opened, investigated, and resolved per problem management procedures.	Inspected completed product support requests including case history for each ticket to determine client reported problems were entered into a trouble ticket system, investigated, and resolved per problem management procedures.	No exceptions noted.
C12.3	Tickets are assigned to a responsible group or individual with appropriate technical background.	Inspected completed product support requests including case history for each ticket, along with the most current job descriptions for support managers, specialists, and product owners to determine tickets were assigned to a responsible group or individual with appropriate technical background.	No exceptions noted.
C12.4	Escalation procedures are in place to assign tickets that require an elevated level of support to technical or application personnel.	Inspected the entity's internal and online support escalation process and procedures to determine escalation procedures were in place to assign tickets that required an elevated level of support to technical and application personnel.	No exceptions noted.

Control Objective 13 – Risk Assessment and Internal Audit

CO13 – Controls provide reasonable assurance a risk and internal audit function is in place and reviewed in a timely manner.

C13.0	Controls Specified by Matillion	Testing Performed by Ascend Audit & Advisory	Results of Tests
C13.1	A formal risk management program is in place, maintained, and reviewed annually.	Inspected the entity's risk management program (i.e., ongoing risk assessments, risk ratings, and risk mitigation activities) to determine a formal risk management program was in place, maintained, and reviewed during the period under review.	No exceptions noted.
C13.2	An internal audit function is in place and maintained in support of the annual risk assessment and program.	Inspected the entity's risk management program, completed internal audit tickets in the project management software, and conducted corroborative inquiry of Governance, Risk, and Compliance (GRC) Management to determine an internal audit function was in place and maintained with respect to the annual risk assessment and program.	No exceptions noted.
C13.3	The Company’s risk assessment process includes identifying and maintaining information technology assets with respect to ongoing risk mitigation.	Inspected the most current system generated IT asset inventory register including the associated attributes for each asset to determine the entity’s risk assessment process included identifying and maintaining information technology assets with respect to ongoing risk mitigation.	No exceptions noted.
C13.4	Management reviews outcomes of risk and threat scenarios as part of the Company’s documented risk posture.	Inspected board of directors and Management meeting minutes regarding business, operational, 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 reviewed outcomes of risk and threat scenarios as part of the Company’s documented risk posture.	No exceptions noted.