Matillion
GxP Guidelines

November 2025

Table of contents

1. Introduction

1.1 Purpose

As life sciences organizations increasingly adopt cloud-based solutions to streamline processes, enhance efficiency, and reduce costs, it is crucial to maintain compliance with regulatory standards that ensure patient safety, product quality, and data integrity.The purpose of this document is to provide a comprehensive guideline for ensuring GxP compliance when using Matillion Data Productivity Cloud. It aims to help organizations navigate the complexities of regulatory compliance while leveraging the benefits of cloud technology. In the life sciences industry, companies must comply with stringent regulations and quality guidelines that regulate practices in various settings to ensure medical products are safe for consumers. Matillion supports GxP, and it helps life sciences organizations qualify the DPC platform so they can validate their GxP workloads. In addition, Matillion provides an extensive portfolio of security certifications such as ISO 27001 and SOC 2 Type II security attestation and granular controls that enable secure and governed access to all data.

1.2 Scope

This GxP guideline document covers all aspects of using Data Productivity Cloud within life sciences organizations, including:

- Compliance Strategy
- Data Productivity Cloud
- Data integrity and security
- Matillion Software Development Life Cycle (SDLC)
- Quality in Test (QiT) strategy and system validation
- Change management protocols
- Data gathering
- Training and documentation standards

By adhering to the guidelines in this document, organizations can ensure that their use of Matillion Data Productivity Cloud complies with GxP regulations and supports their overall quality objectives.

1.3 Audience

This document is intended for a wide range of stakeholders within life sciences organizations, including:

- Quality Assurance (QA) and Quality Control (QC) teams responsible for ensuring regulatory compliance
- IT and system administrators managing cloud-based GxP applications
- Regulatory affairs professionals overseeing compliance with industry standards

- Project managers and team leaders coordinating cloud migration and implementation projects
- Software developers and testers involved in the development and validation of GxP applications
- Compliance officers and auditors evaluating the organization's adherence to GxP regulations
- Senior management and decision-makers seeking to understand the compliance implications of adopting Matillion Data Productivity Cloud

By providing detailed guidance on GxP compliance, this document aims to support these stakeholders in effectively managing and using Matillion Data Productivity Cloud to meet regulatory requirements and enhance operational efficiency.

1.4 Terms and definitions

- **21 CFR Part 11**

A regulation set by the FDA that outlines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records.

- **Adverse Event (AE)**

Any undesirable experience associated with the use of a medical product in a patient. The event is considered serious when it results in death, a life-threatening situation, hospitalization, or significant disability/incapacity.

- **Audit Trail**

A secure, computer-generated, time-stamped electronic record that allows for the reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record.

- **CAPA (Corrective and Preventive Action)**

A systematic approach that includes actions needed to correct (corrective) and eliminate the causes of potential problems (preventive), to prevent their occurrence and recurrence.

- **CFR (Code of Federal Regulations)**

A codification of the general and permanent rules published in the Federal Register by the departments and agencies of the Federal Government.

- **cGMP (Current Good Manufacturing Practice)**

Regulations enforced by the FDA to ensure that products are consistently produced and controlled according to quality standards.

- **Compliance**

The act of adhering to, and demonstrating adherence to, laws, regulations, guidelines, and specifications relevant to the business.

- **CSV (Computer System Validation)**

The process of documenting that a computer system meets a set of defined requirements and specifications, and that it consistently produces results meeting those requirements.

- **Computer Software Assurance**

A risk-based approach to establish confidence in the automation used for production or quality systems, and identify where additional rigor may be appropriate.

- **Data Integrity**

The accuracy, completeness, and reliability of data throughout its lifecycle, ensuring that data is recorded exactly as intended and protected from alteration or destruction.

- **Deviation**

Departure from an approved instruction or established standard. It must be documented and assessed to determine any impact on the quality of the product.

- **GCP (Good Clinical Practice)**

An international ethical and scientific quality standard for designing, conducting, recording, and reporting trials that involve the participation of human subjects.

- **GLP (Good Laboratory Practice)**

A set of principles intended to ensure the quality and integrity of non-clinical laboratory studies intended to support research or marketing permits for products regulated by government agencies.

- **GMP (Good Manufacturing Practice)**

Regulations that require manufacturers, processors, and packagers of drugs, medical devices, some food, and blood to take proactive steps to ensure that their products are safe, pure, and effective.

- **GxP**

A general term for Good Practice quality guidelines and regulations. The "x" stands for various fields, including GCP, GLP, and GMP.

- **IQ (Installation Qualification)**

The process of verifying that a system is installed correctly and according to the manufacturer's specifications and requirements.

- **IaaS (Infrastructure as a Service)**

A form of cloud computing that provides virtualized computing resources over the internet. It offers essential compute, storage, and networking resources on-demand, allowing businesses to scale and manage their workloads flexibly.

- **OQ (Operational Qualification)**

The process of demonstrating that an instrument or system performs as intended throughout the specified operating ranges.

- **PaaS (Platform as a Service)**

A cloud computing service that provides a platform allowing customers to develop, run, and manage applications without dealing with the complexity of building and maintaining the underlying infrastructure.

- **PQ (Performance Qualification)**

The process of verifying that a system is capable of performing consistently over time and under expected conditions.

- **Quality Assurance (QA)**

A way of preventing mistakes and defects in manufactured products and avoiding problems when delivering solutions or services to customers.

- **Quality Control (QC)**

The process through which a business seeks to ensure that product quality is maintained or improved and manufacturing errors are reduced or eliminated.

- **SaaS (Software as a Service)**

A cloud computing service that delivers software applications over the internet on a subscription basis. It allows users to access software from any device with an internet connection, simplifying software maintenance and support.

- **SOP (Standard Operating Procedure)**

A set of step-by-step instructions compiled by an organization to help workers carry out routine operations. SOPs aim to achieve efficiency, quality output, and uniformity of performance.

- **Validation**

Documented evidence that a system or process meets its predetermined specifications and quality attributes.

2. GxP Compliance Strategy

2.1 Overview

A robust GxP compliance strategy is essential for life sciences organizations leveraging cloud-based solutions like Data Productivity Cloud. This strategy outlines the principles, processes, and controls necessary to ensure that all activities conducted within the cloud environment adhere to regulatory requirements and industry best practices. By implementing a comprehensive compliance strategy, organizations can mitigate risks, maintain data integrity, and demonstrate adherence to GxP guidelines.

The GxP compliance strategy encompasses various aspects, including:

- **Regulatory Awareness:** Staying informed about relevant regulations and guidelines, such as FDA 21 CFR Part 11 and EudraLex Volume 4 – Annex 11, and understanding their implications for cloud-based systems. For FDA 21 CFR Part 11 compliance, it is essential to perform a detailed compliance check that assesses each requirement of Part 11. This check should be documented comprehensively to demonstrate how the cloud-based system meets each specific requirement. This approach is often necessary for systems intended for use in GxP environments to ensure adherence to regulatory standards and to provide evidence of compliance.
- **Risk Management:** Conducting risk assessments to identify potential threats to data integrity, security, and regulatory compliance, and implementing controls to mitigate these risks.
- **Validation**: Ensuring that all software and processes within the cloud environment are validated according to regulatory requirements. This includes verifying that software functionalities, data handling procedures, and business processes meet the necessary GxP standards and perform as intended.
- **Qualification**: Ensuring that the underlying infrastructure of the cloud environment, including hardware, operating systems, and network components, is qualified to support GxP-compliant operations. This involves assessing and documenting the infrastructure's capability to maintain the integrity, security, and reliability required for compliance.
- **Change Management:** Establishing processes for managing changes to the cloud environment, including software updates, configuration changes, and system enhancements, while maintaining compliance with GxP standards.
- **User Access Control:** Implementing robust access controls to limit system access to authorized individuals and prevent unauthorized actions that could compromise data integrity or regulatory compliance.
- **Audit Trails and Monitoring:** Implementing secure audit trails and monitoring mechanisms to track user activities, system changes, and data access, enabling organizations to detect and investigate potential compliance issues.
- **Training and Documentation:** Providing comprehensive training for personnel involved in using or managing the cloud environment, and maintaining detailed documentation of all GxP-related activities and procedures.

- **Security Management**: Establishing comprehensive security measures to protect data and system integrity, including:
    - **Backup and Restore**: Implementing regular backup procedures and testing restore processes to ensure data can be recovered in the event of loss or corruption.
    - **Access Controls**: Applying robust controls to restrict unauthorized access to sensitive information.
    - **Data Encryption**: Using encryption to protect data both in transit and at rest.
    - **Incident Response**: Developing a response plan to address and mitigate security incidents.
- **Operational System Monitoring**: Developing processes to monitor and manage the operational aspects of the cloud environment, including:
    - **Incident Management**: Establishing procedures for reporting, tracking, and resolving incidents affecting system performance or data integrity.
    - **Operational Changes**: Managing and documenting changes to operational processes and system configurations.
    - **Periodic Reviews**: Conducting regular reviews of system performance and compliance status to ensure ongoing adherence to GxP standards**.**
- **System/Service Retirement and Archival**: Creating a strategy for the retirement and archival of systems or services in a cloud environment, which includes:
    - **Data Retrieval Agreements**: Ensuring agreements with cloud service providers for retrieving data if necessary during system or service retirement.
    - **Archival Procedures**: Implementing procedures for securely archiving data, maintaining its integrity, and ensuring it remains accessible as needed for compliance.
    - **Decommissioning**: Documenting and executing the process for decommissioning systems to ensure data is handled securely and in compliance with regulatory requirements.

2.2 Shared Responsibilities

In a cloud computing environment like Matillion Data Productivity Cloud, GxP compliance is a shared responsibility between the cloud service provider and the customer. While the cloud service provider is responsible for the security and compliance of the underlying infrastructure and platform, the customer retains responsibility for ensuring the compliance of their applications, data, and user activities within the cloud environment.

Key areas of shared responsibility include:

- **Infrastructure Security:** The cloud service provider is responsible for securing the underlying infrastructure, including physical data centers, networking, and virtualization layers, while the customer is responsible for securing their applications, data, and access controls within the cloud environment.
- **Compliance Certification:** The cloud service provider maintains certifications and attestations for the security and compliance of their cloud services, while the

customer is responsible for demonstrating compliance with regulatory requirements specific to their industry and applications.

- **Data Protection:** The cloud service provider provides tools and services for encrypting data at rest and in transit, managing access controls, and implementing data protection measures, while the customer is responsible for configuring and managing these controls to ensure compliance with GxP guidelines.

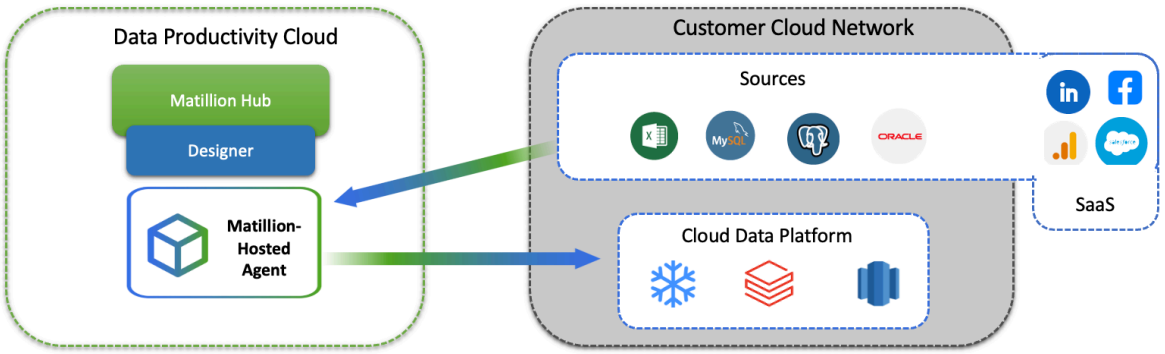
By understanding and clearly defining the shared responsibilities between the cloud service provider and the customer, organizations can effectively collaborate to maintain GxP compliance in the cloud, ensuring the integrity, security, and regulatory compliance of their cloud-based systems and data.

3. Data Productivity Cloud

The Data Productivity Cloud provides users with flexible deployment options tailored to their specific requirements, which can be understood broadly as two models: Full SaaS and Hybrid SaaS. Each deployment model offers distinct features and benefits, allowing organizations to choose the option that best aligns with their needs and infrastructure preferences. Each deployment model also comes with its own security considerations.

3.1 Full SaaS deployment

In Full SaaS, Matillion manages the entire infrastructure, including agent deployment and security measures. Users benefit from a hassle-free experience, as Matillion ensures seamless updates and robust security protocols. The Matillion-hosted agent serves as the backbone, handling execution tasks and securely accessing customer secrets stored in the Matillion Hosted Vault. In this deployment model, the Matillion-hosted agent is automatically updated by Matillion, typically twice a week maximum, on a fixed schedule on Tuesdays and Thursdays. Maintaining a validated state in this deployment mode requires quasi-continuous validation from the customer. Therefore Full SaaS deployment is not recommended to customers requiring GxP compliance, for which Hybrid SaaS deployment is better suited.



3.2 Hybrid SaaS deployment

Hybrid SaaS empowers users to deploy and manage their own execution agents within their private cloud infrastructure. This option grants users full control over security measures, network isolation, and access controls. Users can implement stringent security measures, including network segmentation and access restrictions, to safeguard their data effectively.

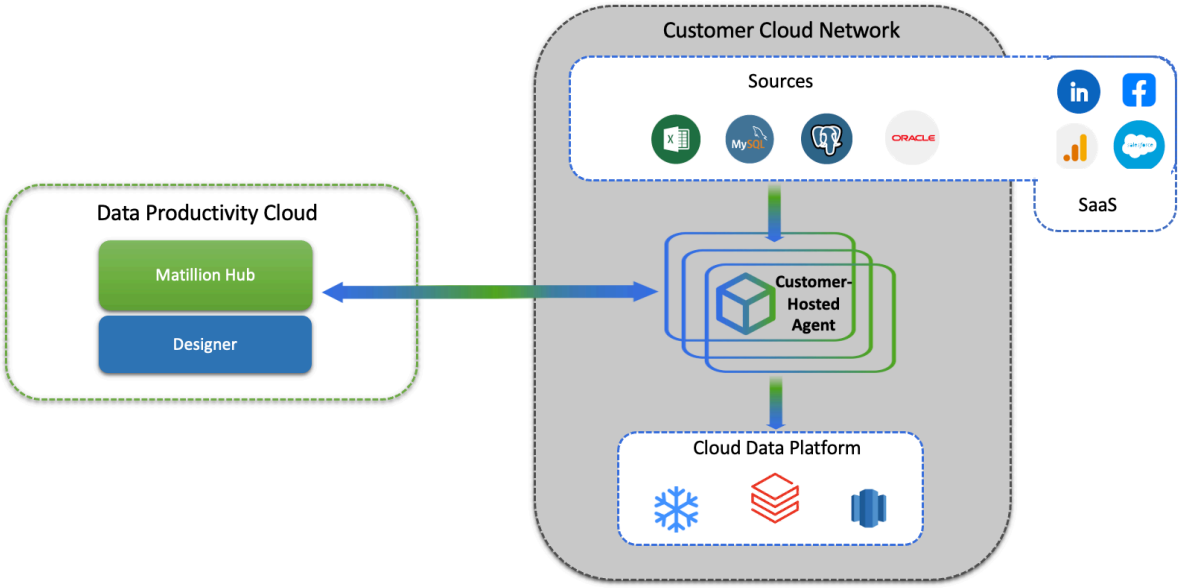
This deployment model also provides users with control on the lifecycle and update frequency of the agents, therefore enabling full change control and native maintenance of the validated state, via 2 control mechanisms: disabling automatic updates and version tracks.

When automatic updates are disabled, customers are notified, natively in the product, that a new agent version is available but their existing agents will remain on their current version until the customer manually proceeds with the update.

Version tracks enable the control of the release cadence of new agent versions. 2 version tracks are available:

- **Current**: supports the latest Data Productivity cloud features and has a faster cadence for releases. This is usually twice a week, typically on a Tuesday and Thursday, though this may vary. These releases may include new features, bug fixes, and security patches. This track is ideal if you want to access the latest features as soon as they are available, and are able to update your agent frequently.
- **Stable**: has a slower, more predictable cadence for releases. This is once per month, on the 1st of the month. Features added to a Stable release have previously been available on a Current release.

The **Stable track is recommended in Production** environments for GxP compliance.



4. Data Integrity and Security

4.1 Data Integrity

Data integrity is fundamental to GxP compliance, ensuring that all data is accurate, complete, and reliable throughout its lifecycle. In the context of Matillion Data Productivity Cloud, data integrity involves implementing robust controls and processes to prevent unauthorized alterations, ensure proper documentation, and maintain traceability of all data-related activities.

Key Principles of Data Integrity:

- **Data Validation:** Implement validation checks to ensure data accuracy and consistency.
- **Audit Trails:** Maintain detailed audit trails for data access and modifications. Data Productivity Cloud stores essential audit information outside of Git. For instance, every pipeline execution is recorded in the Platform Store database, including the ID of the user who triggered it (although this will be a generic machine ID for scheduled runs).
- **Regulatory Compliance:** Ensure data handling practices comply with regulations such as GDPR, HIPAA, and CCPA.
- **Data Classification:** Classify data based on sensitivity and apply appropriate protection measures.
- **Data Governance:** Establish data governance policies to manage data quality, security, and lifecycle.

Matillion Data Productivity Cloud incorporates these principles through various features and best practices, including automated data validation, secure audit trails, and comprehensive logging of user activities.

4.2 Risk Mitigation

Mitigating risks associated with cloud adoption is essential for ensuring data productivity and security:

- **Risk Assessment:** Conduct regular risk assessments to identify potential threats and vulnerabilities.
- **Data Encryption:** Implement encryption for data at rest and in transit to protect sensitive information.
- **Access Control:** Enforce strict access control measures, including multi-factor authentication (MFA) and role-based access control (RBAC).

- **Compliance:** Ensure compliance with relevant regulations, laws and standards, such as GDPR, HIPAA, and SOC 2 Type II.
- **Incident Response:** Develop and maintain an incident response plan to quickly address and mitigate security breaches.

4.3 Data Security

Ensuring data security is critical to protecting sensitive information from unauthorized access, breaches, and other security threats. Matillion Data Productivity Cloud employs a multi-layered security approach to safeguard data and maintain compliance with GxP regulations.

4.3.1 Encryption

Encryption is a vital component of data security, protecting data at rest and in transit by transforming it into an unreadable format for unauthorized users.

- **Data at Rest:** Matillion employs industry-standard encryption algorithms (such as AES-256) to protect data stored within its cloud infrastructure. This ensures that even if physical storage media is accessed without authorization, the data remains unreadable.
- **Data in Transit:** Data transmitted between Matillion services and users is encrypted using Transport Layer Security (TLS) version 1.2 or higher to prevent interception and unauthorized access during transmission. This ensures the confidentiality and integrity of data as it moves across networks.

4.3.2 Authentication and Access Controls

Robust authentication mechanisms and access control measures are fundamental to ensuring that only authorized users can access resources and data within the Data Productivity Cloud environment.

User Authentication

- **Username/Password:** The Data Productivity Cloud supports traditional username/password authentication, requiring users to provide their unique username and a secure password.
- **Multi-Factor Authentication (MFA):** The platform offers Multi-Factor Authentication (MFA) for added security. Users must provide additional verification, such as a one-time code from a mobile app, in addition to their credentials. Integration with various MFA providers is supported, enhancing security measures. MFA is highly recommended for all users.

Integration with Identity Providers

- **Single Sign-On (SSO) Integration:** The Data Productivity Cloud seamlessly integrates with identity providers such as Okta, supporting both SAML and OpenID protocols for Single Sign-On (SSO) functionality. SSO allows users to utilize their existing organizational credentials for authentication, simplifying access to the Matillion platform.

Supported Login Methods

Matillion offers multiple login methods:

- **Username/Password:** Traditional username/password authentication.
- **Social Login:** Users can log in using their Google or Microsoft accounts.
- **Enterprise Login (SSO):** Supported by OIDC and SAML protocols via identity providers like Okta, Entra, Keycloak, etc.

Authentication and Access Control Flow

- **API Token Management:** The Data Productivity Cloud utilizes tokens for API access. Tokens are generated during the authentication and authorization process, where users request an API token using their Client ID and Client Secret. These tokens have a set expiration time to uphold security measures. The platform offers mechanisms for token renewal or regeneration to ensure seamless user activities while maintaining stringent security protocols.

4.3.3 Backup and Recovery

Data backup and recovery processes are crucial to ensure data availability and integrity in case of system failures, data corruption, or other disruptions.

- **Data Replication:** Matillion leverages multiple availability zones (data centers) in the cloud to ensure that multiple copies of data are always available for recovery. These copies of data are encrypted and securely stored to prevent unauthorized access.
- **Disaster Recovery:** Matillion has comprehensive data resiliency by including data replication and geographic redundancy. This ensures that in the event of a significant incident, data can be quickly restored, and services can be resumed with minimal downtime.
- **Uptime:** Matillion maintains SLAs (Service Level Agreements) for various services across the platform and publishes the most up-to-the-minute information on service availability via the Service Health Dashboard https://status.matillion.com/. It is important to note that as part of the shared responsibility model, it is the customer's responsibility to architect their application for resilience based on their organization's requirements.
- **Testing and Validation:** Backup and recovery procedures are regularly tested and validated to ensure they function correctly and meet recovery time objectives (RTO) and recovery point objectives (RPO).

Additional Data Resilience Measures

For further assurance of data resilience, Matillion employs industry-leading practices inspired which include:

- **Continuous Data Protection**: Ensuring data is continuously protected and backed up in near real-time.
- **Data Lifecycle Management**: Implementing policies for managing the lifecycle of data to ensure it is archived and retained according to customer requirements.
- **Multi-Region Backup**: Storing data backups in multiple geographic locations to protect against regional failures.

5. Matillion Software Development Life Cycle (SDLC) Overview

At Matillion, our Software Development Life Cycle (SDLC) is designed to ensure the delivery of high-quality, secure, and efficient software solutions. This document provides a high level overview of our SDLC processes, demonstrating our commitment to maintaining rigorous standards in compliance with GxP requirements.

5.1 Product Team

Our product team consists of Product Owners (POs), Product Managers (PMs), UX Designers, and Programme Management professionals. Their responsibilities include:

- **Requirement Definition**: Gathering and defining customer requirements.
- **Prioritization**: Deciding the order of development for features and enhancements.
- **Lifecycle Management**: Overseeing the entire product lifecycle from ideation through to release.

5.2 Engineering Team

The engineering team at Matillion includes:

- **Developers**: Focus on coding and implementing features.
- **Quality Engineers (QEs)**: Ensure code quality through rigorous testing.
- **Site Reliability Engineers (SREs)**: Maintain system reliability and scalability.
- **Developer Experience (DevX) Team**: Improve developer productivity and efficiency.
- **Release Engineering (RelEng)**: Manage the release process and ensure smooth deployments.

5.3 Security

We prioritize security throughout our development process, ensuring that our software meets high security standards and is resilient against threats. Our security-conscious approach drives us to embed secure practices in every stage of the SDLC and leverages a tailored version of OWASP ASVS standard.

5.4 Agile Scrum Framework

We follow the Scrum framework, incorporating all standard processes and ceremonies. Our teams are cross-functional, including both Product and Engineering members. We utilize JIRA for planning, tracking, and managing our work.

5.5 Delivery Models

We deliver both Software as a Service (SaaS) and monolithic services, catering to a variety of customer needs. This is supported by rigorous processes and standards to ensure reliability, security, and performance.

5.6 Documentation

Technical authors are embedded within our teams to create comprehensive and user-friendly documentation which supports our services and applications.

5.7 SRE and Infrastructure

Our Site Reliability Engineering (SRE) and infrastructure teams play a critical role in maintaining the stability, scalability, and efficiency of our systems. The SRE team is dedicated to applying software engineering principles to infrastructure and operations problems, ensuring that our development environments are robust, automated, and capable of supporting rapid innovation. By proactively monitoring and optimizing system performance, the SRE team helps to minimize downtime and ensure that our services remain reliable and available.

In addition to maintaining system reliability, our SRE and infrastructure teams work closely with development teams to improve deployment processes, enhance system architecture, and implement best practices for security and compliance. This collaboration ensures that our systems can handle increased load, recover quickly from failures, and scale seamlessly as our business grows. Ultimately, our goal is to provide our customers with a seamless and responsive experience, delivering the help they need promptly and effectively.

Our robust incident management processes and structured guidelines maintain high testing standards and minimize customer impact, ensuring every service is thoroughly validated before deployment.

5.8 Testing

Testing is a critical component of our SDLC. Testers are embedded within development teams, with a central core team ensuring overall quality validation. ***(See Quality in Test (QiT) Strategy and System Validation).***

5.9 Development and Validation Environments

We maintain multiple environments for development, testing, and validation before deploying to production. This ensures that all code is rigorously tested in conditions that closely mimic the production environment.

5.10 Continuous Improvement and Feedback

We embrace continuous improvement by leveraging rapid feedback from both customers and internal teams. By actively listening to our customers and encouraging internal ideas, we refine our processes and products, ensuring they meet evolving needs and deliver exceptional value.

5.11 Engagement Processes

Our engagement processes include regular communication with stakeholders to ensure alignment and address any concerns promptly. We have a structured review process to ensure all stages of development and deployment are thoroughly assessed.

5.12 Configuration and Change Management

Configuration management is performed throughout the system design, development, implementation, and operation stages using our Change Management process. Routine, emergency, and configuration changes to existing infrastructure are authorized, logged, tested, approved, and documented in accordance with industry standards including SOC 2 and ISO 27001.

5.13 CI/CD and Controlled Deployments

We follow Continuous Integration/Continuous Deployment (CI/CD) practices, ensuring controlled and efficient deployment of code. Our deployment strategy includes:

- **Rigorous Testing and Quality Criteria**: Ensuring all code meets predefined quality standards.
- **Change Management**: Implementing zero-impact deployments to minimize disruption.
- **Phased Deployment**: Rolling out changes in phases to manage risk.
- **Validation in Production**: Continuously validating the deployed software in the production environment.
- **Separation of Deployment from Release**: Deploying code independently from the release to ensure stability.
- **Roll-Forward/Roll-Back Capability**: Having the ability to quickly roll forward or back in case of issues.

5.14 Monitoring and Review

Post-deployment, we perform ongoing monitoring of performance and security through various processes. Audit trails of changes are maintained, and periodic self-audits ensure compliance with high standards and facilitate continuous improvement. Emergency changes follow a documented incident management process, ensuring swift resolution and minimal impact.

At Matillion, our SDLC processes are designed to deliver high-quality, secure, and reliable software solutions while continuously improving and adapting to meet the needs of our customers.

6. Quality in Test (QiT) Strategy and System Validation

At Matillion, we ensure world-class standards through our rigorous quality testing approach. Formal functional, security, performance and quality assurance testing is performed in every pre-production environment, including development and staging based on defined acceptance criteria. Results are reviewed and approved by the appropriate representatives before deploying to production.

Our proactive, shift-left testing strategy is embedded throughout the Software Development Life Cycle (SDLC). This approach includes static and dynamic analysis to monitor application behavior, penetration testing to detect security vulnerabilities, and threat modeling reviews to mitigate new attack vectors.

Automated quality gates at each pipeline stage ensure code integrity, supplemented by exploratory testing and a zero-bug policy. Our testing pyramid emphasizes efficient methods, from automated unit tests to comprehensive end-to-end testing. We also adhere to rigorous testing and quality criteria to maintain high standards.

We leverage a variety of tools for code level testing, security, performance, and end-to-end testing, ensuring transparent reporting and continuous improvement. Our change management practices, aiming for zero-impact deployment, ensure smooth transitions.

Post-deployment releases are monitored for success with immediate rollback for failed implementations. We employ phased deployment and validation in production to ensure stability and performance. Our separation of deployment from release and fix-forward/roll-back capability further enhance our ability to maintain high-quality standards. This comprehensive validation process ensures that each service meets our high-quality standards and operates as intended. All deployments are tested and deployed through our lower environments and continuously through the SDLC.

7. Change Management

At Matillion, we understand that change is inevitable for progress. To ensure a smooth and efficient journey, we've implemented a streamlined change management process that minimizes risk and fosters continuous improvement. This process empowers every team member to participate in shaping the future while maintaining system stability.

7.1 Initiating Change: A Collaborative Effort

Our process starts with the **Initiation** stage, where any team member can submit a change request through the change management system. Here, collaboration is key. To prioritize effectively, each request is categorized based on its **impact** (ranging from standard to high) and **urgency** (normal, immediate).

7.2 Evaluation: Assessing Feasibility and Impact

Once submitted, requests undergo a thorough Evaluation phase. This initial review ensures completeness and may involve requesting additional information to solidify the proposal. We then assess the **feasibility** of the change, considering resource requirements, potential conflicts with existing systems, alignment with Matillion's overall business objectives, and other principles outlined above such as security, quality, and compliance.

7.3 Prioritization

It is a crucial step, ensuring that changes with the highest impact and urgency are addressed first. We employ a multi-faceted approach, considering the established criteria alongside valuable **stakeholder input**.

7.4 Impact Analysis: Understanding the Ripple Effect

Understanding the full scope of a change is vital. The **Impact Analysis** stage delves into the potential ramifications of the proposed change.

- **Risk Assessment:** We conduct a comprehensive analysis to identify potential technical, operational, and business risks associated with the change. This proactive approach allows us to develop effective **mitigation strategies** to address these risks before implementation.
- **Resource Evaluation:** We assess the resources required for successful implementation, including personnel, time, and budget. Resource **availability** is confirmed to ensure a smooth rollout.
- **Stakeholder Impact:** Identifying all stakeholders affected by the change is crucial for effective communication. A communication plan is then developed to keep stakeholders informed and engaged throughout the process.
- **System Dependencies:** We meticulously analyze any dependencies on other systems to ensure compatibility and avoid disruptions.

7.5 Approval Process: Rigorous Review and Clear Communication

The **Approval Process** ensures that all changes undergo a rigorous review and authorization before implementation. The Change Advisory Board (CAB), composed of representatives from various departments, meticulously reviews and approves requests. A **technical review** verifies that the proposed change meets established technical standards and requirements.

Several key criteria are used in the **Approval Decision Making** process:

- **Compliance:** We ensure adherence to all relevant policies, standards, and regulations.
- **Risk Management:** Acceptable risk mitigation strategies are a cornerstone of approval.
- **Resource Allocation:** Confirmation of adequate resources for successful implementation is essential.

Approved changes are then scheduled based on priority and resource availability. Rejected changes receive constructive feedback to guide future proposals.

Transparency throughout the process is paramount. We document all decisions, approvals, and relevant details for future reference. A comprehensive **communication plan** ensures that all stakeholders are informed about approved changes and implementation timelines.

By adhering to this streamlined change management process, Matillion empowers its team members to be agents of positive change. This collaborative approach fosters continuous improvement while safeguarding system stability and minimizing risk.

To keep customers informed, all communication regarding security risks and changes are updated via the Trust Center Updates section on Matillion's Trust Center.

8. Data Gathering

Some Matillion features involve your business data being processed and/or stored in Matillion's infrastructure. Matillion will only process and/or store the data required to use our tools. In these cases, it will only be within the selected region. Your chosen account region might be based on a combination of geographical closeness, legal jurisdiction, or other factors.

Your chosen account region dictates the region of your data and resources and can't be changed after your Hub account is provisioned.

Matillion does not have the ability to access the customer data such as that being loaded from source systems into the customer's data warehouse.

Types of data

Here we delineate between types of data and how they are, or are not, gathered.

- **Customer data**: Refers to data that a user loads from a source system into a target data warehouse or storage area. This is the data that is the direct subject of ETL pipelines. This data is subject to regional protections and is not stored or accessible by Matillion.

- **Customer metadata:** Refers to information about a customer's Designer pipeline and project configurations. This data must be accessed in order for Designer and other functions to be useful. This data is typically held by Matillion but some of it (such as pipeline configurations) can be held in a customer's Git repository.
- **Matillion metadata:** Refers to information about how a customer uses Matillion products, such as user logins, telemetry regarding component usage, roles, and permissions, and metadata required for billing purposes. This data is analyzed at a collective level to improve our services, ensuring that no individual user can be identified. Personal data specific to regions subject to regulations (such as the EU, UK, USA) is excluded from the metadata captured by Matillion to protect individual privacy. Matillion metadata is used globally and is not subject to regional protections.

Global Resources	Regional Resources
Hub Account Information	**Project and Pipeline Configurations**
- Centralized account details for the entire platform.	- Specific configurations for projects and pipelines within a region.
Hub User Information	**Agents**
- Information about all users who have access to the hub.	- Regional agents responsible for executing tasks and processes.
Roles and Permissions	**Custom Connectors**
- Definitions of roles and permissions that apply globally.	- Region-specific connectors for integrating with local systems.
Subscription and Billing Information	**Schedules**
- Centralized subscription and billing details for managing costs.	- Scheduling configurations for running tasks and jobs at regional levels.

9. Training and documentation

Matillion understands the importance of empowering users with the knowledge and resources they need to succeed. We offer a comprehensive training and documentation program to ensure user proficiency, system understanding, and adherence to Standard Operating Procedures (SOPs).

9.1 User Training

Matillion provides a robust **User Training** program designed to equip your team with the skills required to effectively leverage the Data Productivity Cloud platform. We offer a variety of training options to cater to different learning styles and preferences:

- **Online Courses:** Self-paced courses available through the Matillion Learning Portal, allowing users to learn at their own convenience.
- **Webinars and Workshops:** Interactive sessions led by Matillion experts to provide hands-on experience and real-time Q&A.
- **Documentation and Tutorials:** Comprehensive guides and step-by-step tutorials available in the Matillion Documentation Center.

Evaluation and Feedback

- **Quizzes and Assessments:** Users are encouraged to complete quizzes and assessments to test their understanding and proficiency.
- **Feedback Mechanisms:** Regular feedback is collected from users to improve training content and delivery methods.

9.2 Documentation

System documentation provides detailed information about the Matillion Data Productivity Cloud, enabling users to understand and effectively use the platform.

Types of Documentation

- **User Guides:** Detailed guides covering all aspects of the platform, from basic navigation to advanced features.
- **API Documentation:** Comprehensive documentation for developers, detailing API endpoints, request/response formats, and example code.
- **Configuration Guides:** Step-by-step instructions for configuring various components of the platform, including integration with external systems.
- **Release Notes**: Regularly updated release notes detailing new features, improvements, bug fixes, and other changes. These can be accessed on the Data Productivity Cloud Changelog.

Accessibility

- **Online Documentation Portal:** All documentation is available online, easily accessible from the Matillion website.
- **Searchable Database:** Users can quickly find relevant information using the powerful search functionality.

Updates and Maintenance

- **Regular Updates:** Documentation is regularly updated to reflect new features, changes, and improvements in the platform.
- **Version Control:** Historical versions of documentation are maintained for reference.

9.3 Standard Operating Procedures (SOPs)

Standard Operating Procedures (SOPs) provide a framework for consistent and efficient operation of the Matillion Data Productivity Cloud.

Purpose of SOPs

- **Consistency:** Ensure that all processes are carried out in a consistent manner across the organization.
- **Efficiency:** Streamline operations by providing clear and concise instructions for routine tasks.
- **Compliance:** Ensure adherence to regulatory and organizational requirements.

9.4 Document Revisions

Date	Description
June 2024	**v1.0.0** • Initial release of the document. • Formatting and layout set for readability.

July 2024	**v1.1.0**
	• Updated security certificate
	• Added new points in GxP Compliance Strategy
	  ◦ Security Management
	  ◦ Operational System Monitoring
	  ◦ System/Service Retirement and Archival
	• Revised section on Audit trails
	• Added Additional Data Resilience Measures in Backup & Recovery section.
	• Revised Matillion Software Development Life Cycle (SDLC) section.
	• Updated Approval Process.
	• Added Release Notes reference in Documentation section.

November 2025	**v1.1.1** • Added Agent updates considerations in Full SaaS Deployment • Added Agent tracks and Disabling Auto-updates details in Hybrid Saas Deployment