Teradata Vantage Guidelines in a GxP Environment

Table of Contents

Introduction 3

Teradata Vantage 4

System Description........ 4

Teradata Organization and Governance 4

Supply Chain Security / Resiliency 4

Business Continuity Plan 4

Vantage Platform Security 5

Access Control 5

Monitoring 5

Vulnerability Management 5

Encryption 6

Database Administration 6

Data Governance 6

Data Integrity and Access........ 7

Data Availability and Business Continuity 8

Data Backup and Restoration........ 8

Title 21 CFR Part 11 9

Teradata Quality Management 11

Quality System 11

Quality System Procedures 11

Quality System Management Review 11

Quality System Management Audits........11

Software Development Approach 11

Teradata Vantage Operations 12

System Provisioning 12

System Monitoring........14

Incident Management........14

Change Management........14

Operating Models for GxP Validation 15

Conclusion 15

Industry/ Regulatory Guidance Standards........15
Appendix - Teradata Certifications........16
ISO 9001:2015........16
ISO/IEC 27001:2013........16
PCI-DSS 3.2.1........16
Health Insurance Portability and Accountability Act of 1996 (HIPAA)........17
CSA CAIQ........17
CCPA and GDPR........17

Introduction

This document provides transparency to customers planning to use Teradata Vantage in GxP-regulated environments. It explains the steps Teradata takes to align with GxP guidelines. The descriptions in this document may be used to support your electronic record requirements. While references to, and details of regulatory standards and guidance are provided as a framework for discussion, they do not constitute legal advice for customers nor for any other entities.

GxP was established in the U.S. by the Food and Drug Administration (FDA) and encompasses different standards.

- G – stands for “Good”
- x – variable depending on the application
- P – stands for “Practice”

GxP refers to a set of globally accepted current “good practices” about quality. GxPs include:

- Good manufacturing practices (GMPs)
- Good clinical practices (GCPs)
- Good laboratory practices (GLPs)
- Good pharmacovigilance practices (GPVPs)
- Good engineering practices (GEPs)

Teradata is not directly regulated by GxP guidelines; however, Teradata provides support for our customers who must establish GxP compliance. This document has been prepared based on Teradata’s experience with cloud service providers (CSPs), pharmaceutical, medical device, and manufacturing customers. It also describes and clarifies shared responsibilities between Teradata and our customers.

In addition to GxPs, Teradata recognizes that life sciences and manufacturing customer business activities are regulated by national and global health authorities such as the U.S. Food and Drug Administration (FDA) and European Medicines Agency (EMA). Many corporations are subject to regulations such as Title 21 CFR Part 11 and Annex 11: Computerized Systems Validation. Such regulations provide a framework for customers to evaluate whether new technologies support confidentiality, integrity, and availability of their electronic GxP data. It is the responsibility of the GxP-regulated customer to evaluate, operate, and verify that its systems meet GxP compliance, and compliance with 21 CFR 11.

Teradata Vantage

System Description

Teradata Vantage is the connected multi-cloud data platform for enterprise analytics. Vantage integrates analytic tools, languages, and engines to provide insights from customer data. Through Vantage, Teradata manages the performance, security, availability, and operations of the platform as detailed in the Cloud Service Description (CSD). In this document, Vantage is considered a combination of software and activities performed by Teradata operations personnel. Operations include the configuration and management of compute instances, storage, and additional cloud service provider (CSP) resources within a customer-selected region. Vantage is deployed in a dedicated private virtual network within a Teradata-owned CSP account. Vantage inherits its physical infrastructure and network security from the CSP.

Application	Optional Application
Teradata Advanced SQL Engine	Teradata Data Lab
Teradata Query Service	Teradata QueryGrid
Teradata Data Mover	
Teradata Viewpoint	
Vantage Analyst	
Editor	

Table 1: Teradata Vantage Components

Teradata Organization and Governance

Teradata maintains rigorous governance procedures that ensure a culture of quality compliance. This begins with decades of the software development lifecycle (SDLC) in engineering. Quality governance extends to policy documentation, software assurance processes, and quality metrics, which simplifies and ensures Teradata's continued internal and external audit cadence success.

Supply Chain Security / Resiliency

Teradata has documented and implemented a supply chain security process which identifies security requirements for Vantage. Suppliers must identify the country of origin for products and services they sell to Teradata. Teradata Global Security reviews supplier offerings for features that may compromise Vantage security. Teradata also requires suppliers to identify potential risks in supply chain deliveries. Teradata Global Security requires that components be available to the extent forecasted. This includes replacement components within the forecast period.

Business Continuity Plan

Teradata has a documented and implemented business continuity plan (BCP) for Vantage offerings. The plan reduces the risk of loss of revenue and operational control that may occur following a disaster. The BCP directs Teradata's recovery process when unexpected disasters occur. It also covers recovery of business operations and recovery of critical business systems.

Teradata's Business Continuity Manager (BCM) oversees each functional area to recover from a crisis and provides the ability to recover critical processes. The recovery plans for a local crisis and recovery of critical processes are developed by the BCM and senior management responsible for functional areas. Recovery plans for business functions and systems with Teradata-wide impact shall be the responsibility of the BCM and be addressed in the enterprise-wide business continuity plans. The BCM has overall oversight for the creation of local plans to provide leadership and guidance and must assure appropriate consistency and coordination among the various business dependencies, as well as compliance with international standards.

Vantage Platform Security

The customer controls access to their data by administering user accounts and access to their Vantage instance. Customer data is only accessible to Teradata if explicitly requested and granted by the customer. Teradata administers access to the infrastructure that supports Vantage. Teradata treats customer data as sensitive and below are examples of how we manage Teradata's part of our shared responsibility.

Access Control

Teradata cloud operations and support personnel must complete training and sign security agreements before receiving access to Vantage cloud infrastructure. Teradata enforces password complexity with minimum and maximum lifetime restrictions. Passwords are strongly encrypted in storage and when transmitted. Teradata personnel will never access or transfer customer data between countries unless directed by the customer.

Re-approval is a standard security process. It ensures credentials and access grants are reviewed regularly. Teradata uses a strict security re-approval process for Teradata personnel that consists of:

- Remote device access to the cloud requires a VPN and multi-factor authentication.
- Access to systems is logged. Logs go to a central server where they are protected from tampering. Log data is always aggregated and analyzed.
- Account management actions are reviewed and approved.
- Account management operations are monitored for unauthorized actions.
- Inactive accounts are disabled after 90 days.
- Vantage accounts are disabled after an employee is transferred or terminated.
- Role-based access is modified when employee usage or need-to-know requirements change.

Monitoring

The Vantage security monitoring process collects and aggregates relevant security policy events. Vantage systems log events such as failed login attempts, account creation, account removal, system policy changes, privileged access, IPS, etc. The security information and event management system (SIEM) ingests the log files. The SIEM then correlates and analyzes them in near real time. The SIEM log file database is stored in a secure and tamper-proof location. Data events are audited for security-critical functions, new threats, and potential security incidents.

Vulnerability Management

Teradata regularly scans the Vantage operational environment and code to identify vulnerabilities for remediation. This includes software and operating systems. This is a combination of application security analysis and network analysis.

Encryption

All customer data stored in Vantage is encrypted at rest at the CSP infrastructure level. Customer management of storage volume encryption keys is available as an option, including adding CSP-provided Hardware Security Modules (HSMs) into the key vault architecture, where available, Teradata recommends and provides customers with options to encrypt data-in-transit between Vantage and connecting clients with TLSv1.2. MACsec and IPsec protocols are available where supported by customer and CSP infrastructure. Enhanced third-party encryption solutions are also available from Teradata's partners.

Topic	Activity	Teradata	Customer
System Security & Access Management	Encryption: customer data-in-motion	CI	RA
	Encryption: customer data-at-rest	RA	
	Implement/manage network security, firewalls, intrusion detection software	RA	
	Deploy/manage virus detection	RA	
	Maintain password controls, RBAC, multi-factor authentication, disable dormant accounts	RA	
	Decommission Vantage system	RA	CI
Operating System Administration	OS security monitoring	RA	
	OS volume encryption	RA	
Network Administration	Restrict/filter incoming traffic to Vantage	RA	
Cloud Administration	Security monitoring of Vantage platform	RA	
	Cloud access management for Teradata personnel	RA	

R – Responsible **A –** Accountable **I –** Informed **C –** Consulted

Table 2: Shared Responsibilities: Security and Access Management in Vantage

Database Administration

Data Governance

Data governance is a customer business process. Departmental data owners manage data quality, usability, and consistency. Data stewards curate the data and identify subject matter experts. Stewards also deploy data catalogs and master data management tools for added data surveillance. Data governance is clearly a GxP necessity. The goal is to maintain trust in the data and ensure accountability, thereby reducing risk and security concerns. Data management software can help, but governance is performed by the business units.

Topic	Activity	Teradata	Customer
Database Administration	Database user & object management (creations, permissions, troubleshooting)		RA
	Database system performance data collection		RA
	Collection & management of statistics		RA
Database Security	Security roles, profile, password management		RA
	Reporting on security access violations, DBQL data management		RA
Database Capacity & Performance	Monitor TASM, collect performance data, workload categorization		RA
	Review & analyze Viewpoint setup and canary queries to monitor the database		RA
	Customize & configure Viewpoint database alerts (space, CPU, I/O, AWT, etc.)		RA
	Performance data reporting		RA
	Performance tuning		RA

R – Responsible **A** – Accountable **I** – Informed **C** – Consulted

Table 3: Shared Responsibilities: Database Administration, Security, and Performance in Vantage

Data Integrity and Access

To preserve data integrity and prevent unauthorized changes to customer data, Vantage is protected by a variety of technologies and processes. Hashing, checksum, cyclic redundancy check (CRC), file monitoring and related controls are the primary integrity controls implemented to insure input and output validation of data. To protect from unauthorized access, Vantage provides customers with options for secure authentication, authorization rules through role-based access control, fine-grain access control through row- and column-level security, and encryption of data-in-transit, in-use, and at-rest. When enabled, data is encrypted in transit between Teradata and connecting client sessions. Data is also secure from public exposure as it traverses cloud network segments by implementing customer-selected private connectivity options.

It is a shared responsibility between Teradata and GxP-regulated customers to implement sufficient mechanisms to meet GxP obligations. Specifically, Teradata provides a secure, compliant platform for services, applications, and data. It is important to note that the customer is responsible for authorizing access, managing governance, and configuring settings related to integrity of the data in Vantage.

Topic	Activity	Teradata	Customer
Data Integrity	Properly authorized users who are granted access to the resources & monitor continued appropriateness of access		RA
	Define data classification and retention rules		RA
	Implement Advanced Encryption Standard (AES) or Transport Layer Security (TLS) encryption of customer data in transit		RA
	Establish proper controls over the use of system IDs and passwords		RA

R – Responsible **A** – Accountable **I** – Informed **C** – Consulted

Table 4: Shared Responsibilities: Data Integrity in Vantage

Data Availability and Business Continuity

GxP-compliant customers should consider platform and data availability requirements while undertaking business continuity planning for mission-critical platforms, applications, and services including supporting customer infrastructure and network. While Vantage has a 99.9% SLA, this SLA is not applicable when the CSP availability zone or region is impacted. If Vantage is deployed in a CSP region with multiple availability zones, Teradata will use commercially reasonable efforts to deploy a new system in a secondary, unimpacted availability zone and restore the instance from an existing backup to the secondary, unimpacted availability zone as part of our service. Teradata offers additional disaster recovery services, multi-region high availability, and multi-cloud provider solutions for an additional fee.

Data Backup and Restoration

After initial configuration by Teradata, Teradata provides the customer with the ability to create and manage backup jobs using Teradata Console. A data protection plan defines the schedule, frequency, and retention policy for data backups. Available backup storage and retention policies depend on the cloud platform a customer chooses for its Vantage deployment.

The customer is responsible for ensuring that an appropriate full backup exists. This is scheduled by the customer during system provisioning or via a change request to meet the customer’s desired recovery point objective. These backups will be used by Teradata to restore data and Vantage services in case of a system outage or data corruption that has rendered the database unusable. This may require a full data backup to be restored.

Topic	Activity	Teradata	Customer
Backup and Restore (BAR) Operations	Create & maintain default full-system backup jobs & retention policies during system provisioning	RA	CI
	Create & maintain additional custom backup jobs & retention policies (optional)	I	RA
	Monitor backup jobs for completion	I	RA
	Provide execution status of backup jobs	RA	I
	Release locks & abort blocked backup jobs	I	RA
	Create, execute, & monitor restore jobs	RA	CI
	Schedule & request restore jobs	CI	RA

R – Responsible **A** – Accountable **I** – Informed **C** – Consulted

Table 5: Shared Responsibilities: Backup and Restore in Vantage

Title 21 CFR Part 11

Biopharmaceutical drug development and manufacturing operations demand robust analytics applications. Such applications facilitate discovery, development, and production of new drugs. Nowhere are the automation processes employed here more vital than with the rigorous recordkeeping and signature requirements of 21 CFR Part 11. This FDA regulation permits the widest possible legal use of electronic records and signatures.

Independent proof that Teradata can help life sciences companies meet Part 11 obligations was demonstrated when the Vantage database was independently audited by Compliance Implementation Services (CIS). CIS reviewed Teradata's design specifications, business processes, and standard operating procedures (SOPs). CIS interviewed key stakeholders and did system walkthroughs. CIS evaluated system development, security, data extraction, and validation reports. CIS then tested security access attributes. Other areas of testing were change controls, user acceptance testing, training records, and backup/recovery procedures. CIS also evaluated Teradata's audit responsiveness to requests for documentation and data. System controls, documentation, processes, and procedures were reviewed to assess compliance with FDA requirements.

CIS's assessment finding: Vantage addresses all applicable aspects of Part 11. Vantage's extensive logging capabilities, access controls, and authentication methods provide robust flexibility. Data collection and analysis applications can proceed with confidence.

Requirement	The Teradata Approach
21 CFR § 11.10(a) System validation	Teradata Database has successfully undergone an intensive scrutiny of security controls by Compliance Implementation Services, a third-party compliance company.
21 CFR § 11.10(b) Accurate and complete copies of records	Teradata Database ensures that any changes are documented and can hold individuals responsible for changes through extensive logging capabilities
21 CFR § 11.10(c) Protection of records	Teradata Database can enforce strict rules with respect to retention. For example, permissions for select, create, modify, and delete can be assigned separately.
21 CFR § 11.10(d) Limiting system access	Teradata Database implements strict login security controls that ensure that only authorized individuals can gain access to the database, including password complexity restrictions and encrypted credential exchanges.
21 CFR § 11.10(e) Generated audit trail	Teradata Database can log every database access including selects,writes, and deletes.
21 CFR § 11.10(f) Operational system checks	Teradata Database can enforce separation of duties and check to ensure that users are permitted to execute the appropriate SQL statements
21 CFR § 11.10(g) Authority checks	Teradata Database implements strict login security controls that ensure that only authorized individuals can gain access to the database.
21 CFR § 11.10(h) Devices checks	The Teradata Director Program Identifier enables each Teradata client to be assigned a separate host identifier. This allows Teradata to restrict access by username, password, and client workstation.
21 CFR § 11.10(i) Education and training of personnel	The Teradata Database system comes with an extensive library of documentation to assist administrators and end users.
21 CFR § 11.10(j) Personnel accountability	The Teradata Security Administration manual provides guidance for sound security practices related to the security of the overall operating environment.

Table 6: Teradata Helping You on Your Journey to Part 11 Validation

Teradata Quality Management

Quality System

Teradata adheres to a quality system driven by the five P's: Policies, Procedures, Processes, People, and Plans. Policies identify the basic "rules of the game" for the quality system. Procedures means complying with policy directives. Process descriptions identify the sequence of tasks required to achieve quality goals. People's responsibilities clarify procedures and process tasks for roles. Plans and progress reports provide evidence that the quality system is being followed.

Quality System Procedures

The Teradata Quality System is governed by a quality manual, consisting of industry standard policies, procedures, processes, and plan descriptions that comprise the written material necessary to develop hardware and software products and solutions. It also identifies how the quality system satisfies the requirements of the ISO 9001:2015 Standard.

Quality System Management Review

Reviews of the quality system and quality manual are overseen by a quality improvement team consisting of members of Teradata engineering, Teradata leadership, and key strategic partners. The reviews follow the quality management system review procedure as described above. The leadership team executives annually review the effectiveness of the quality system. If significant issues or third-party concerns are raised, the leadership team holds an ad hoc meeting. Their primary responsibility is to ensure the integrity of the quality management processes.

Quality System Management Audits

Teradata has undergone independent examinations of the quality system processes. The certifying agents found Teradata's quality management compliant with ISO 9001:2015. The Teradata quality management system has been re-certified for ISO 9001 periodically since 1999.

Software Development Approach

Teradata has implemented Unified Offering Lifecycle (UOL), which is a framework for creating, releasing, and sunsetting products. UOL adheres to SAFe 4.6 principles and practices. UOL/SAFe 4.6 applies to many different types of software, development, migrations, and sustainment. This enables UOL alignment to Good Medical and Pharmaceutical Practices (GMPP).

Unified Offering Lifecycle
as of Feb 2021

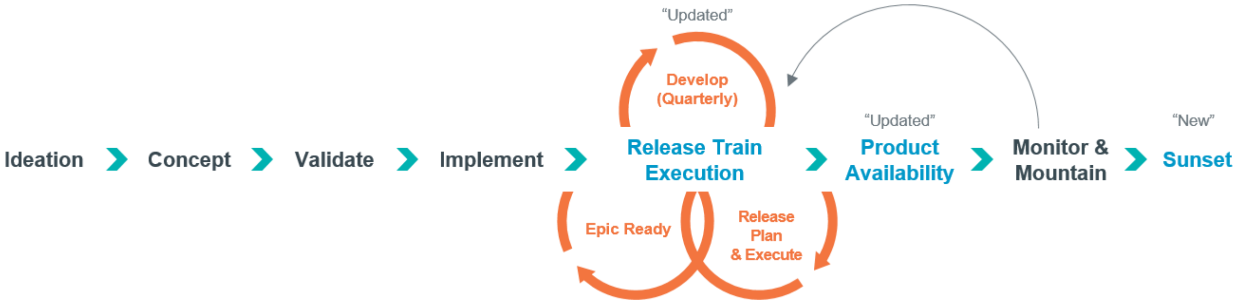

Figure 1: Unified Offering Lifecycle

Adherence to the Unified Offering Lifecyle is mandatory for product teams at Teradata. The standard covers preparation, development, outsourcing, acquisition, and transition to operations. It also covers software maintenance, extensions, and security response in the operational phases. Thus, Teradata does not make changes to customer applications running in the cloud. Changes to Vantage are only carried out in accordance with contractual agreements.

Teradata Vantage Operations

With Vantage, Teradata manages provisioning, patching, and upgrades of the Vantage environment. Teradata provides integrated maintenance and support services for all Vantage customers. Included are well-defined coverage hours and response times. Also included are support portal access, Vantage Console, and other features. Customers can submit cases and service and change requests through the support portal 24/7. Teradata uses Infrastructure Technology Information Library (ITIL) best practices for support tickets.

System Provisioning

Teradata will provision the Vantage system and configure it in accordance with an architecture design approved by Teradata and the GxP-regulated customer. Teradata will configure the Vantage system to facilitate customer network connectivity per the agreed network design. Teradata will notify the customer of the Vantage service availability date. After the service availability launch date, the customer is responsible for:

- Registering to use the support portal, console, and support role as in the Teradata Console
- Retention and control of the DBC password
- Configuring and maintaining the customer infrastructure and network to connect to Vantage
- Approving and maintaining outage windows to perform migrations, assessments, and network tests

Topic	Activity	Teradata	CSP	Customer
Deploy	Platform provisioning & customer onboarding	RA	I	CI
	Network connectivity	RA	I	RA
	Configure AES & TLS encryption on Platform (PS engagement required)	RA		CI
	Configure AES & TLS encryption on clients			RA
Teradata Advanced SQL Engine	Provision & upgrade	RA		CI
	Monitor & report availability	RA		I
Teradata Tools & Utilities	Install & upgrade on clients			RA
Teradata Query Service	Provision & upgrade	RA		
Teradata Data Mover	Provision & upgrade	RA		CI
	Portlet (enable in Viewpoint)	RA		
	Create Data Mover jobs			RA
	Create Data Mover connections (PS engagement required)	RA		CI
Teradata Viewpoint	Provision & upgrade	RA		CI
	User set up and administration			RA
	Provide rules sets for TASM/TIWM			RA
	TASM/TIWM configuration and setup	RA		CI
Vantage Analyst	Provision & upgrade	RA		
Editor	Provision & upgrade	RA		
Teradata QueryGrid (Optional)	Provision & upgrade	RA		CI
	Portlet (enable in Viewpoint)	RA		
	Connectors - Install on SQL engine nodes (PS engagement required)	RA		CI
	QueryGrid connectors - Install on remote nodes/systems (PS engagement required)	RA		CI
	Create & manage jobs			RA
Teradata Data Lab (Optional)	Provision & upgrade	RA		CI
	Portlet (enable in Viewpoint)	RA		
	Create and manage users and labs			RA

R – Responsible **A –** Accountable **I –** Informed **C –** Consulted

Table 7: Shared Responsibilities: Deployment and Maintenance in Vantage

System Monitoring

Teradata continuously monitors the Vantage environment for performance, security, and availability as defined in the Cloud Service Description. Teradata provides automated event management to monitor Vantage health and create support cases.

Incident Management

Teradata follows Information Technology Infrastructure Library (ITIL) best practices for a highly available, compliant, and performant Vantage system. Teradata tracks and resolves customer issues, requests, and resolution activity with cases. Vantage has a 5-tier severity level model. When opening a case in the support portal, customers must select a severity based on the impact of the reported issue. Teradata supplies severity level descriptions correlating to business and operations impact. Teradata will evaluate, respond to, and resolve cases based on the assigned severity. Some cases may require customer response. Customers must respond to cases with a status of “Awaiting Info.” Once a case solution arrives, the status is set to “Resolved.” The customer should then review the update and either accept or reject the resolution.

Topic	Activity	Teradata	Customer
Incident Management	Auto incident creation	RA	I
	User incident creation	I	RA
	Initial issue triage and RCA	RA	I
	Vantage software issue resolution	RA	I
	CSP infrastructure issue resolution	RA	I

R – Responsible **A** – Accountable **I** – Informed **C** – Consulted

Table 8: Shared Responsibilities: Incident Management in Vantage

Change Management

Teradata updates Vantage as new versions are released. The latest versions may include new features and patches to mitigate security issues. To minimize disruptions, Teradata works with GxP customers to coordinate upgrade schedules. Teradata provides a minimum four-month notice for major version upgrades. This allows customers to test application compatibility and validate new versions. Upgrades are scheduled to fit into customer approved time windows.

Topic	Activity	Teradata	CSP	Customer
Change Management	Upgrades to Teradata Vantage components & OS	RA		CI
	Upgrades to maintain CSP infrastructure currency	RA	I	I
	Network & firewall changes	R	I	RA
	Customer application, workload & process testing after upgrades			RA
	Creation, development, promotion, backup of customer workloads and processes including ETL and Reporting			RA

R – Responsible **A** – Accountable **I** – Informed **C** – Consulted

Table 9: Shared Responsibilities: Change Management in Vantage

Operating Models for GxP Validation

GxP compliance regarding data and analytics platforms is the responsibility of the customer. As such, Teradata customers will need experience with Vantage and management of cloud instances. Regulatory compliance depends on working together with customer's corporate quality initiatives and applicable validation organizations.

Teradata and its compliance partners are ready to assist in the assessment, design, implementation, and validation of Vantage. Working together, we can ensure compliance with Part 11 and other regulatory requirements. Teradata and its life sciences and manufacturing customers can implement many operating models for GxP validation.

- **Model 1**: A life sciences or manufacturing company takes responsibility for business and technical migration, plus validating GxP applications. The governing control is their quality management system (QMS).

- **Model 2**: A life sciences or manufacturing company retains the business responsibilities. They engage a third party to assist in validating GxP applications using its own QMS. The technology partner would then use its management tools to create a "logical" factory. The factory would plan and coordinate actual execution steps. The factory would also drive the migration and validation of applications and databases.

- **Model 3**: Responsibility for GxP compliance lies with life sciences and manufacturing customers. The shared responsibility model helps customers allocate resources. It reduces the amount of effort needed. This model also helps alleviate some administrative and technical burdens faced by customers. Teradata is generally responsible for securing Vantage infrastructure. Customers are responsible for securing their data.

Conclusion

Teradata Vantage provides life sciences and manufacturing customers with a wide array of best-in-class security, data management, and audit reports. This enables compliance with FDA 21 CFR Part 11 requirements. Vantage maintains secure, consistent, and reliable performance through a series of tried and tested access, security, and privacy controls. These processes and controls are audited and verified on a continuous basis by qualified third-party accredited assessors. Of equal importance are the controls that must be implemented by our life sciences and manufacturing customers while defining their validation and governance strategies to ensure the integrity of their GxP content. Working together, we can achieve compliance, cost savings, efficiency, and innovation.

Industry/ Regulatory Guidance Standards

Ref. [1] **ISO/IEC 27001:2013 Information Technology – Security techniques – Information Security Management Systems – Requirements**

Ref. [2] **ISO 9001:2015 Quality management systems — Requirements**

Ref. [3**] PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1**

Ref. [4] **Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (ICFR)**

Ref. [5] **Regulation (EU) 2016/679 (General Data Protection Regulation)**

Ref. [6] **Current Good Manufacturing Practice for Finished Pharmaceuticals (Title 21 CFR Part 11)**

Ref. [7] **U.S. FDA, Code of Federal Regulations, Title 21 Part 11, Electronic Records; Electronic Signatures**

Ref. [8] **U.S. FDA, Guidance for Industry - Part 11, Electronic Records; Electronic Signatures — Scope and Application, August 2003**

Ref. [9] **U.S. FDA, Use of Electronic Records and Electronic Signatures in Clinical Investigations under 21 CFR Part 11-- Questions and Answers (Draft Guidance), June 2017**

Ref. [10] **Whitepaper: Building a solid foundation for GxP-regulated workloads on AWS**

Ref. [11] **Microsoft 365 GxP Guidelines, published April 2020**

Appendix - Teradata Certifications

Teradata holds many certifications and attestations from regulatory bodies and auditors. These substantiate Teradata's efforts to achieve compliance and security. Vantage is periodically audited for compliance with the following regulatory standards.

ISO 9001:2015 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. Specific sections of the standard contain information on topics such as:

- Requirements for a quality management system, including documentation
- Responsibilities of management
- Management of resources, including human resources and an organization's work environment
- Measurement, analysis, and improvement of the QMS through internal audits

ISO/IEC 27001:2013 is a standard for Information Security Management Standard (ISMS). It defines a set of information security management requirements. Under this standard, information includes data, documents, communications, conversations, messages, recordings, and photographs. It includes everything from digital data and email to faxes and telephone conversations.

The **SOC 1** reports focus on controls at a service organization relevant to financial audit. The Teradata SOC 1 report covers a financial audit. It also covers security organization, employee user access, logical security, secure data handling, physical security, change management, data integrity, availability, and incident handling.

The **SOC 2** report evaluates controls defined by the American Institute of Certified Public Accountants (AICPA). These principles define controls for security, availability, processing integrity, confidentiality, and privacy. They are applicable to Service Organizations such as Teradata. The SOC 2 Type 2 report outlines Teradata's controls relevant to security, availability, and confidentiality services. This SOC 2 report relates directly to GxP compliance.

PCI-DSS 3.2.1

PCI Data Security Standards are requirements designed to protect branded credit cardholder data. The standards apply to all entities that store, process, or transmit cardholder data. Compliance is enforced by the PCI Council: American Express, Discover Financial Services, JCB, MasterCard and Visa Inc. Vantage is not directly involved with handling cardholder data. Even so, Teradata offers products and services to help banks worldwide comply with PCI-DSS 3.2.1.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Teradata Consultants perform assessments of the controls needed to satisfy the HIPAA Security Rules. They also assess the Breach Notification Rule from the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. The specific objectives include:

- Evaluation of the security posture of the ePHI environment in accordance with the requirements of the HIPAA Security and Breach Notification Rules

- Identification of gaps related to the required and addressable administrative, technical, and physical safeguard requirements

CSA CAIQ

The Cloud Security Alliance (CSA) Consensus Assessment Initiative Questionnaire (CAIQ) is a publicly available document that provides transparency of cloud provider security controls and processes. As such, customers may utilize the report to assess which controls are fully leveraged or shared as part of the service and better understand the security controls of the service provider. Teradata completes the voluntary CSA Self-Assessment to document compliance with CSA-published best practices. Teradata provides the completed CSA CAIQ to customers upon request.

CCPA and GDPR

Teradata uses independent, industry-recognized auditors to annually audit Vantage. Periodic audits help customers meet their privacy responsibilities. Annual audit results are made available for CCPA and GDPR customer review

17095 Via Del Campo, San Diego, CA 92127 **Teradata.com**