MicroStrategy Cloud for Government

SERVICE GUIDE

UPDATE PUBLISHED November 2024

Copyright Information

Trademark Information

Specifications subject to change without notice. MicroStrategy is not responsible for errors or omissions. MicroStrategy makes no warranties or commitments concerning the availability of future products or versions that may be planned or under development.

TABLE OF CONTENTS

1. Overview

The MicroStrategy Cloud for Government service ("MCG Service") is a software-as-a-service ("SaaS") offering that MicroStrategy manages on its customers' behalf in an Amazon Web Services environment for GovCloud that includes access to, collectively, (a) the "Cloud Platform" version of MicroStrategy software products (an optimized version of the MicroStrategy software platform built specifically for deployment in AWS GovCloud) licensed by the customer; (b) Cloud Support, as described below; and (c) Cloud Architecture, as described below. MicroStrategy's SaaS delivery model is designed to allow businesses to consume MicroStrategy Enterprise Analytics in a single-tenant architecture without the need to deploy and manage the underlying infrastructure.

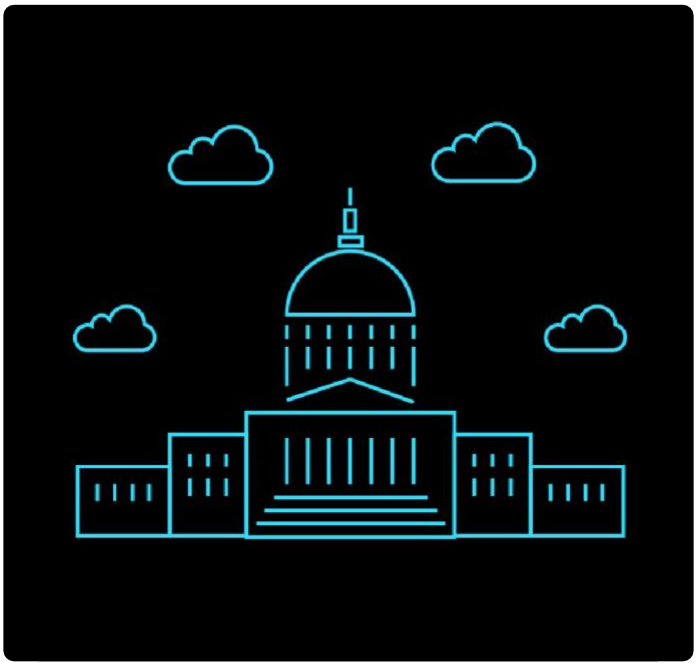
The MCG Service offers a distributed compute architecture using cloud-native services provided by Amazon Web Services. As this technology evolves, MicroStrategy continually incorporates new services that allow for increased availability, security, and performance to ensure the latest architecture is available to our customers. At the core of the solution is MicroStrategy, a secure, scalable, and resilient business intelligence enterprise application platform.

The MCG Service also includes the elements needed to operate, access, and manage the intelligence architecture. Customers are provisioned with their own dedicated intelligence architecture based on a reference architecture. Once provisioned, customers can develop, tailor, and manage the application components to meet their respective needs.

Based on this operating model, customers administer and control the solution while MicroStrategy maintains the supporting cloud-based service.

2. Cloud Support

As an MCG Service customer, you will receive "Cloud Service Support" (Cloud Support) in which our Cloud Support engineers will provide ongoing support over your MCG Service term to assist in maximizing the performance and agility—as well as minimizing the cost—of your MicroStrategy Cloud Platform deployment. Cloud Support includes environment configuration (setting up customer accounts in a selected VPC), enterprise data warehouse integration (including modifying the MicroStrategy configuration for data warehouse connections and opening any connectivity for external data warehouses), authentication (OIDC/SAML), and application integration. Additionally, Standard Support for the Cloud Platform version of MicroStrategy Products is provided with the licenses for such Products pursuant to your contract with MicroStrategy and our Technical Support Policies and Procedures except that all MCG Service customers are entitled to four Support Liaisons and 24x7 support for P1 and P2 issues (as defined in the Technical Support Policies and Procedures).



If a production outage issue occurs, MicroStrategy reserves the right to fix the issue on behalf of the customer without pre-authorization. For some specific scenarios where the issue requires detailed analysis, MicroStrategy may require the customer to reproduce the workflow and assist in troubleshooting the issue via a secured screen sharing session. If a support issue is logged and determined through the diagnosis that the Root Cause Analysis (RCA) that the stated issue is due to a customer-specific customization of the MicroStrategy application, the Support team will provide the customer with available options to resolve the issue. These solutions may require the purchase of MicroStrategy Professional Services for additional assistance depending on the complexity of the issue.

3. Cloud Architecture

The Cloud Architecture offered as part of the MCG Service is an optimized reference architecture providing enterprise-grade data design and governance, and consists of (a) the Cloud infrastructure and architecture components required to run your SaaS environment, configured through either the Enterprise MCG Architecture or High-Availability MCG Architecture constructs detailed below, and (b) Cloud Environment Support, the support services and components needed to successfully run the infrastructure and architecture components of the MCG Service offering.

3.1 Cloud Service

Our MCG Service offers an enterprise platform architecture based on industry best practices for security, compliance, and availability. The building block of these SaaS components is an infrastructure package and optional add-ons which allow you to add high availability and extra environments if needed. The MCG Service provides a highly elastic infrastructure that can scale both horizontally and vertically. In addition, MCG Service also provides 24x7x365 system monitoring and alerting, daily backups for streamlined disaster recovery, and an environment with FedRAMP Authorization. This offering is procured on your behalf from Amazon Web Services to host the MCG. Additionally, all MCG customers will receive up to 1 TB per month of data egress. As part of the MCG quarterly service review, we will advise you if your monthly data egress usage is close to or exceeds 1 TB for each MCG environment.

A. The MCG Service offering is a fully managed cloud environment with each customer getting their own tenant along with a dedicated metadata database, load balancers, firewalls, data egress, and other services to ensure ease of use for customers. This also includes MicroStrategy Workstation deployed on the client machine to enable customer administrators to perform tasks such as assigning roles and permissions to users etc.

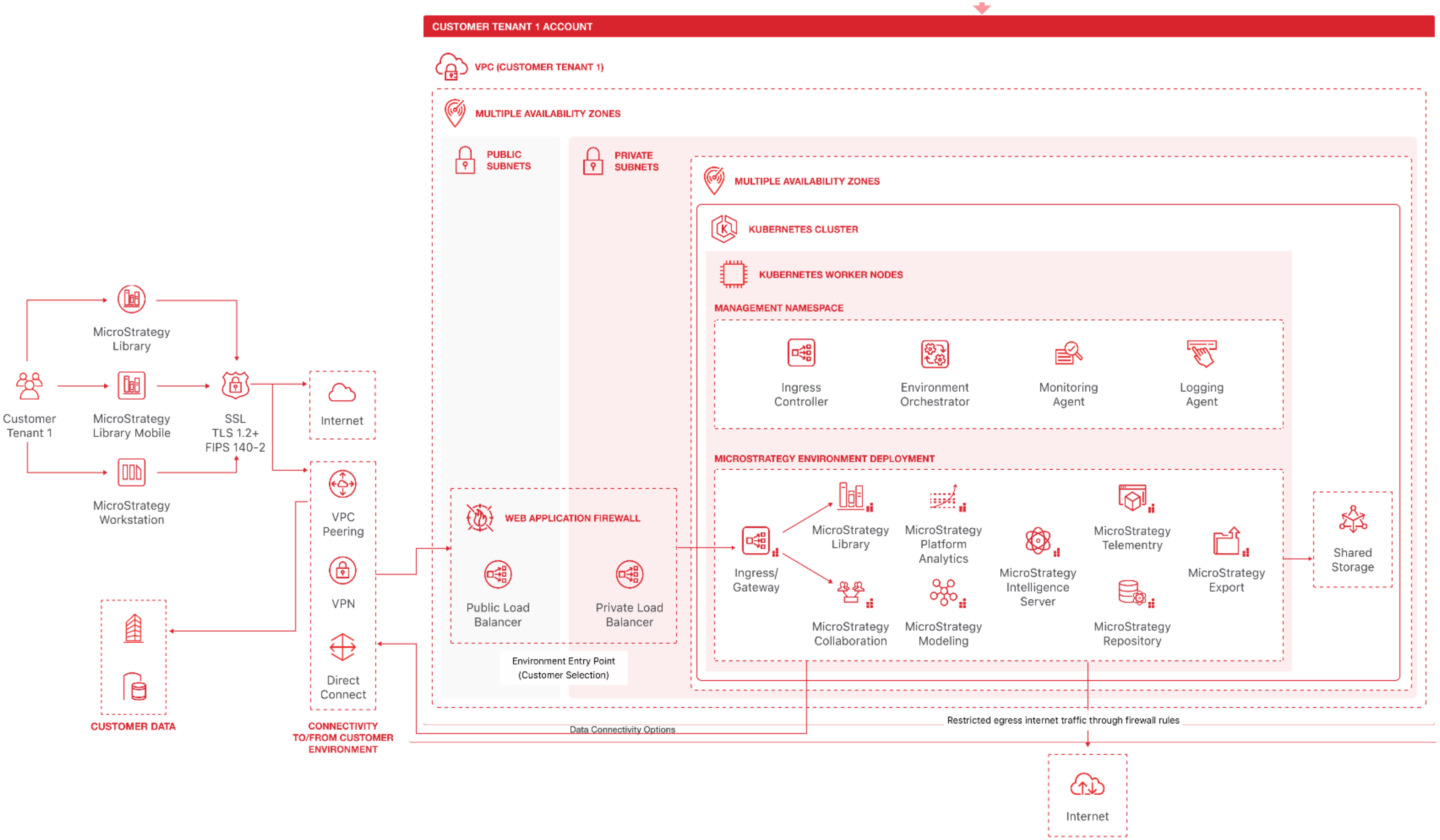
The MicroStrategy Cloud for Government initial offering includes a base environment configuration; administrators have the option to purchase incremental resources as needed.

3.1.1 Enterprise MCG Architecture

Customers who purchase the Standard Cloud offering will receive access to MicroStrategy's Enterprise MCG Architecture built on Amazon Web Services as demonstrated in the diagrams below. Each instance consists of a single server instance for MicroStrategy Intelligence Server, Library, Library Mobile, Modeling Service, Export Engine, Platform Analytics, and Collaboration. Additionally, a database for the MicroStrategy metadata and statistics is provided.

3.1.2 High-Availability MCG Architecture

MicroStrategy's High-Availability MCG Architecture consists of the Enterprise MCG Cloud Architecture plus additional offerings including, but not limited to, a highly availability Production system or a non-highly availability non-Production system for MicroStrategy Intelligence Server, Library, Library Mobile, Modeling Service, Export Engine, Platform Analytics, and Collaboration. The High-Availability MCG Architecture can scale to hundreds of thousands of end use.



CUSTOMER TENANT 1 ACCOUNT

VPC (CUSTOMER TENANT 1)

MULTIPLE AVAILABILITY ZONES

PUBLIC SUBNETS

PRIVATE SUBNETS

MULTIPLE AVAILABILITY ZONES

KUBERNETES CLUSTER

KUBERNETES WORKER NODES

MANAGEMENT NAMESPACE

Ingress Controller

Environment Orchestrator

Monitoring Agent

Logging Agent

MICROSTRATEGY ENVIRONMENT DEPLOYMENT

Ingress/ Gateway

MicroStrategy Library

MicroStrategy Collaboration

MicroStrategy Platform Analytics

MicroStrategy Modeling

MicroStrategy Intelligence Server

MicroStrategy Telementry

MicroStrategy Repository

MicroStrategy Export

Shared Storage

WEB APPLICATION FIREWALL

Public Load Balancer

Private Load Balancer

Environment Entry Point (Customer Selection)

Data Connectivity Options

Restricted egress internet traffic through firewall rules

Internet

Customer Tenant 1

MicroStrategy Library

MicroStrategy Library Mobile

MicroStrategy Workstation

SSL TLS 1.2+ FIPS 140-2

Internet

VPC Peering

VPN

Direct Connect

CONNECTIVITY TO/FROM CUSTOMER ENVIRONMENT

CUSTOMER DATA

3.2 Cloud Environment Support

As part of the Cloud Service offering, we will provide Cloud Environment Support to you by maintaining one or more production and/or non-production environments for the total number of infrastructure units purchased as part of an MCG Service subscription, by providing the following:

3.2.1 Support Availability

The MCG Service will provide 24x7 operations support for production systems and non-production systems in the customer's local time zone. These parameters may be changed based upon mutual agreement.

3.2.2 Root Cause Analysis (RCA)

For production outages, an RCA is generated by the Cloud Support team. For other P1 cases (outside of a production outage) that are logged, an RCA can be requested by the customer. Customers will receive the RCA report within 10 business days of the production outage or the requested RCA.

Cloud Support will cover all support regarding the diagnosis of the RCA. It will also cover product defects, security updates, operating system updates, and changes. As noted in Section 2, if an RCA determines an issue to be created by a customer-specific customization, MicroStrategy can provide options outside of Cloud Support, such as Professional Services engagements, to remedy the issue.

3.2.3 24/7 Cloud Help Desk

For Production system outages where system restoration is paramount, all alerts are sent to a 24x7 dedicated operations support team within the US Region for prompt resolution.

3.2.4 24/7 Monitoring and Alerting

Key system parameters are tagged and monitored. MicroStrategy has alerts on CPU utilization, RAM utilization, disk space, SSL certification expiration, daily backups, host failures, application-specific performance counters, VPN Tunnel, and ODBC warehouse sources monitoring. System performance is logged over time to give the customer and Cloud Support team the ability to maintain a performant cloud platform.

3.2.5 Backups

Daily backups are performed for all customer systems, including system state, metadata, customizations, and performance characteristics. MicroStrategy retains at least ninety consecutive days of backups. Backups are dispersed across availability zones to ensure multiple points of failure (for example, a single cloud data center).

3.2.6 Platform Analytics

MicroStrategy Platform Analytics is set up for all MicroStrategy customers on MCG and maintained to allow for instant access to system performance metrics. In the event the space availability is less than 20% of the allocated storage, after receiving the customer's consent, MicroStrategy will purge older data from the MCG Service-based Platform Analytics database in 30- day increments until the disk availability is below the 80% capacity threshold. The amount of data that the customer chooses to keep may have a corresponding cost to the customer. Contact your Account team for a cost estimate to modify the MCG Service, including increases to the data repository and/or cube memory requirements.

3.2.7 Maintenance and Updates

Maintenance windows are scheduled monthly to allow for a monthly update of MicroStrategy and third-party security updates to be applied to the MCG platform. Updates will not include any new, unlicensed products. During these scheduled interruptions, the MCG Service systems may be unable to transmit and receive data through the provided services. Customers should plan to create a process that includes the pause and restart of applications, rescheduling subscriptions, and including but not limited to, related data load routines. When it is necessary to execute emergency maintenance procedures, MicroStrategy will notify customer-specific support liaisons via email as early as possible—identifying the nature of the emergency and the planned date and time of execution. Customers will normally receive a minimum of two weeks' advance notification for planned maintenance windows. However, if emergency maintenance work is required, we will use commercially reasonable efforts to give 48-hour notice before applying a remedy.

3.2.8 Quarterly Service Reviews

The designated Cloud Technical Account Manager (TAM) for your MCG Service will conduct the Quarterly Service Reviews (QSR) with your business and technical contacts on a regular cadence.

3.2.9 Intra-Region Failover

The MCG Service is architected to withstand the failure of an individual service or process to achieve high availability. This is achieved by utilizing underlying application features and building on best practices such as clustering along with the advantage AWS allows through the splitting of the GovCloud Region into multiple Availability Zones ("AZ") to withstand AZ-wide failure. The use of multiple AZs creates a physical separation of data between the machines storing production and backup environments.

MicroStrategy develops, documents, and disseminates a comprehensive set of procedures for implementing DR and contingency planning activities for the MCG Service. Each MCG Service deployment includes an intra-region DR zone such as within the AZs in the AWS region in use.

The procedures have been developed for a Moderate (M) impact system and are designed to recover the MCG Service's essential missions/business functions within our target Recovery Time Objective (RTO) of 24 hours and the Recovery Point Objective (RPO) of 24 hours when the primary processing capabilities are unavailable.

3.2.10 Non-Migrated Components

Stated below are MicroStrategy components that will not be hosted in cloud. Customers are highly encouraged to move away from legacy components and leverage newer and modern replacement of such tools:

- MicroStrategy Narrowcast Server replaced with Distribution services
- MicroStrategy Enterprise Manager replaced with Platform Analytics
- Web is replaced with Library
- MDX Cubes to be converted to MTDI/OLAP
- Big Data and Cloud Connectors are not supported for MCG
- Mobile is replaced with Library Mobile
- SDK/Plugins are not supported for MCG
- 32 bit Client Tools (ex. Developer, Object Manager, Command Manager, System Manager, Project Duplication, Integrity Manager) is replaced with Workstation

The following items below are supported only for connectivity to MCG. MicroStrategy will not host them in the Cloud. These solutions may require additional assistance from MicroStrategy Professional Services.

- ETL/Scheduling Tools

Distribution Services

All MicroStrategy Cloud customers are required to use their own SMTP server for delivery of email and history list subscriptions. File subscriptions are pushed to AWS S3 bucket provided to the customer as part of the MCG infrastructure to all customers. Customers may pull file subscriptions from the storage locations provided during the on-boarding process with their CTMs.

3.2.11 AI Capabilities

The “AI Power User,” “AI Consumer User,” “AI Architect User,” “MicroStrategy AI,” and “MicroStrategy AI User” SKUs provide artificial intelligence capabilities as a part of your MCE Service (“AI Capabilities”).

AI Capabilities are designed to accommodate various user roles, and provide AI-assisted data exploration, automated dashboard design processes, SQL generation tools, and ML-based visualization methods. The AI Capabilities within the framework of the MicroStrategy analytics platform augment the platform's data processing and presentation capabilities. The use of AI Capabilities may have limitations which impact the effectiveness, quality and/or accuracy of output from your MCE Service and should not replace human decision-making.

You remain responsible for judgments, decisions, and actions you make or take based on the output of your MCE Service.

Notwithstanding anything to the contrary, we may provide AI Capabilities to you from an environment that is different from the operating environment specified on your MCE Service order. You may not perform any penetration testing on the artificial intelligence service powering the AI Capabilities.

Consumption-Based Licensing and Auto-Replenishment of the MicroStrategy AI SKU

For each MicroStrategy AI SKU quantity you license, you may consume up to twenty thousand (20,000) Questions (as defined below) for a period of up to twelve (12) months beginning on the order effective date and, in the case of a replenishment, from the beginning of the replenishment effective date (each period, a "Use Period"). Unconsumed Questions are automatically forfeited at the earlier of (a) the end of the Use Period, or (b) termination or expiry of the MCE Service term, and do not carry over to any subsequent Use Periods. Upon the earlier of the expiration of the Use Period or the full consumption of 20,000 Questions, we will automatically replenish your right to consume an additional 20,000 Questions for each licensed MicroStrategy AI SKU quantity for a subsequent Use Period, each at the then current list price for such MicroStrategy, unless you provide written notice to us that you desire not to auto-replenish (a) at least ninety (90) days before the expiration of the then current Use Period, or (b) before 18,000 Questions have been consumed, whichever occurs first. MicroStrategy AI is otherwise non- cancelable by you, and non-refundable.

For the avoidance of doubt, the foregoing does not apply to the licensing of the other AI Capability SKUs, which are licensed on a named user basis, with no limit on the number of questions. Customers purchasing the MicroStrategy AI SKU will have access to Platform Analytics, which will include your usage in its reporting.

One "Question" is defined as any input action taken while using the MicroStrategy AI SKU. Below are examples of a Question:

Auto Answers (multiple consumption options):

one action submitted to MicroStrategy's Auto chatbot that returns a response constitutes consumption of one Question.

one click on auto-populated suggestions below MicroStrategy's Auto chatbot input box constitutes consumption of one Question.

any subsequent selection(s) of the recommended data analysis constitutes consumption of an additional Question.

Auto SQL:

one action submitted to MicroStrategy's Auto chatbot that returns a response constitutes consumption of one Question.

Auto Dashboard (multiple consumption options):

one action submitted to MicroStrategy's Auto chatbot that returns a response constitutes consumption of one Question.

one click on auto-populated suggestions below MicroStrategy's Auto chatbot input box constitutes consumption of one Question.

any subsequent selection(s) of the recommended data analysis constitutes consumption of an additional Question.

3.2.12 Security

Various security products are employed for vulnerability testing and timely remediation, system event logging, compliance, and system hardening. The MCG Service maintains a high-security posture in accordance with the following security standards:

3.2.12.a Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a US government-wide program that provides a standard approach to the security assessment, authorization, and continuous monitoring of cloud products and services. The governing bodies of FedRAMP include the Office of Management and Budget (OMB), US General Services Administration (GSA), US Department of Homeland Security (DHS), US Department of Defense (DoD), National Institute of Standards & Technology (NIST), and the Federal Chief Information Officers (CIO) Council.

Cloud Service Providers (CSPs) who want to offer their Cloud Service Offerings (CSOs) to the US government must demonstrate FedRAMP compliance. FedRAMP uses the NIST Special Publication 800 series and requires CSPs to receive an independent security assessment conducted by a third-party assessment organization (3PAO) to ensure that authorizations are compliant with the Federal Information Security Management Act (FISMA).

3.2.12.b National Institute of Standards and Technology (NIST)

The NIST Special Publication (SP) 800-53 security controls are generally applicable to US Federal Information Systems. Federal Information Systems typically must go through a formal assessment and authorization process to ensure sufficient protection of confidentiality, integrity, and availability of information and information systems. The MCG Service follows NIST SP 800-53 to implement security controls for the FedRAMP Moderate offering.

The NIST Cybersecurity Framework (CSF) is supported by governments and industries worldwide as a recommended baseline for use by any organization, regardless of its sector or size. Since 2016, Federal Information Security Modernization Act (FISMA) metrics have been organized around the CSF and agencies are now required to implement this framework (CSF) under the Cybersecurity Executive Order.

3.2.12.c Federal Information Processing Standards (FIPS) 199

FIPS 199 provides guidelines on determining the potential impact on organizational operations and assets, and individuals through a formula that examines three security objectives: confidentiality, integrity, and availability. FIPS 199 requires Federal agencies to assess their information systems in each of the categories of confidentiality, integrity, and availability, rating each system as “Low (L)”, “Moderate (M)” or “High (H)” impact in each category. The most severe rating from any category becomes the information system’s overall security categorization. The MCG Service is classified as a Moderate (M) impact system, in accordance with FIPS 199.

3.2.12.d Federal Information Processing Standards (FIPS) 200

FIPS Publication 200–*“Minimum Security Requirements for Federal Information and Information Systems”* is a mandatory federal standard developed by NIST in response to FISMA. To comply with the federal standard, organizations must first determine the security category of their information system in accordance with FIPS Publication 199–*“Standards for Security Categorization of Federal Information and Information Systems”*; derive the information system impact level from the security category in accordance with FIPS 200; and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. FIPS 200 follows FIPS 199's categorization system by specifying 17 areas of cybersecurity where minimum security requirements are specified, including access control, incident response, and risk assessment, among others.

3.2.12.e Federal Information Processing Standards (FIPS) 140-2

FIPS 140-2 defines the requirements and standards for cryptography modules that include both hardware and software components. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels (Level 1 to Level 4) intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management, etc. The MCG Service follows and implements FIPS 140-2 validated encryption guidelines to ensure secure communication between all internal and external applications.

3.3 Cloud Shared Services Components

As part of the MCG Service's platform architecture and in support of the MCG Service, we incorporate other solutions to assist in the management, deployment, and security of the environment, and to complete operational tasks. These solutions include management and detection response, cloud security posture management, compliance with FedRAMP, NIST SP 800-53, and CIS Foundations Benchmarks, adherence to AWS Foundational Security Best Practices, application and infrastructure monitoring, alerting and on-call management, and workflow and continuous integration tools.

4. Service Availability

The MCG Service offers a service level agreement of 99.9% availability for highly available environments and 99% availability for non-highly available environments. Availability is calculated per calendar month as follows:

$$\left\lceil \frac{\text{Total Minutes * \# of Production Instances - Unavailability}}{\text{Total Minutes * \# of Production Instances}} \right)^{*\,100}$$

4.1 Service Definition

"Total Minutes": the total number of minutes in a calendar month.

"Production Instance": an MCG Intelligence Architecture that users are running in production, in support of an operational business process.

"Unavailability": for each Production Instance, the total number of minutes in a calendar month during which (1) the Production Instance(s) has no external connectivity; (2) the Production Instance(s) has external connectivity but is unable to process requests (i.e., has attached volumes that perform zero read-write IO, with pending IO in the queue); or (3) all connection requests made by any component of the Production Instance(s) fail for at least five consecutive minutes. "Unavailability" does not include minutes when the MCG Service is unavailable due to issues related to applications built on the MicroStrategy software platform, including project, report, and document issues; migration problems related to user design; ETL application problems; improper database logical design and code issues; downtime related to scheduled maintenance; downtime experienced as a result of user activity; general internet unavailability; and other factors out of MicroStrategy's reasonable control.

"Total Unavailability": the aggregate unavailability across all Production Instances.

For any partial calendar month during which customers subscribe to the MCG Service, availability will be calculated based on the entire calendar month, not just the portion for which they subscribed.

4.2 Service Remedies

If the availability standard of 99.9% (for highly-available Systems) and 99% (for non-|available Systems) is not met in any given calendar month, customers may be eligible for a Service Credit, according to the definitions below. Each Service Credit will be calculated as a percentage of the total fees paid by customers for the MCG Service, managed by MicroStrategy within the calendar month that a Service Credit has been accrued. This is the exclusive remedy available to customers in the event MicroStrategy fails to comply with the service level requirements set forth in the availability designed in Section 4. 4.

4.3 Service Credits

Highly Available System:

- Availability less than 99.9% but equal to or greater than 99.84%: 1% Service Credit
- Availability less than 99.84% but equal to or greater than 99.74%: 3% Service Credit
- Availability less than 99.74% but equal to or greater than 95.03%: 5% Service Credit
- Availability less than 95.03%: 7% Service Credit

Non- Highly Available System:

- Availability less than 99% but equal to or greater than 98.84%: 1% Service Credit
- Availability less than 98.84% but equal to or greater than 98.74%: 3% Service Credit
- Availability less than 98.74% but equal to or greater than 94.03%: 5% Service Credit
- Availability less than 94.03%: 7% Service Credit

4.4 Service Credits Procedure

To receive a Service Credit, customers must submit a MicroStrategy case on or before the 15th day of the calendar month following the calendar month in which the Service Credit allegedly accrues that includes the following information: (a)the words "SLA Credit Request" in the "Case Summary/ Error Message" field; (b) a detailed description of the event(s) that resulted in unavailability; (c) the dates, times, and duration of the unavailability; (d) the affected system or component ID(s) provided to customers by MicroStrategy during onboarding and Intelligence Architecture delivery activities; and

(e) a detailed description of the actions taken by users to resolve the unavailability. Once MicroStrategy receives this claim, MicroStrategy will evaluate the information provided and any other information relevant to determining the cause of the Unavailability (including, for example, information regarding the availability performance of the Intelligence Architecture, third-party software or services, dependencies on customer-hosted or subscribed software or services, operating system, and software components of the MCG Service). Thereafter, MicroStrategy will determine in good faith whether a Service Credit has accrued and will notify customers of its decision. If MicroStrategy determines that a Service Credit has accrued, then at its discretion, it will either (1) apply the Service Credit to the next MCG Service invoice sent or (2) extend the MCG Service Term for a period commensurate to the Service Credit amount. Customers may not offset any fees owed to MicroStrategy with Service Credits.

5. Terms Applicable to Processing Personal Data

This Section will apply only to the extent there is no other executed agreement in place regarding the same subject between MicroStrategy and the customer (Customer), including any order(s) and/or a master agreement between the customer and MicroStrategy (collectively, the Governing Agreement), and shall be considered a Data Protection Agreement (DPA).

5.1 Definitions

“Applicable Data Protection Law” shall include and means all applicable laws and regulations where these apply to MicroStrategy, its group, and third parties who may be utilized in respect of the performance of the MCG Service relating to the processing of personal data and privacy, including, without limitation, the California Consumer Protection Act (Cal. Civ. Code §§ 1798.100 et. seq.), including as modified by the California Privacy Rights Act, together with any applicable implementing regulations (CCPA), and any similar law of any other state related to the processing of personal data.. The terms “Business”, “Service Provider,” “Supervisory Authority,” “process,” “processing,” and “personal data” shall be construed in accordance with their meanings as defined under Applicable Data Protection Law.

“Customer Group” shall include and mean Customer and any affiliate, subsidiary, subsidiary undertaking, and holding company of Customer (acting as a Controller) accessing or using the MCG Service on Customer’s behalf or through Customer’s systems or who is permitted to use the MCG Service pursuant to the Governing Agreement between Customer and MicroStrategy, but who has not signed its own Order Form with MicroStrategy.

“MCG Service” means the MicroStrategy Cloud for Government service, the platform-as-a-service offering that we manage as a unique FedRAMP certified offering that includes access to, collectively: (a) the“Cloud Platform” version of our Products (an optimized version of the MicroStrategy software platform built specifically for deployment in an Amazon Web Services GovCloud environment licensed by the Customer; and (b) the Additional SaaS Components (as defined in the MicroStrategy Software License and Service Agreement) Customer has purchased for use with such Products.

“External Service Provider” shall include and mean any third party appointed by MicroStrategy to process personal data.

“Security Incident” means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any personal data. For the avoidance of doubt, an unsuccessful attempt that does not result in the unauthorized access to personal data or to any of MicroStrategy’s or any External Service Provider’s equipment or facilities storing personal data including, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents shall not be considered a Security Incident.

5.2 Data Processing

MicroStrategy will process, as a Service Provider, the personal data that is uploaded or transferred to the MCG Service as instructed by Customer or provided by Customer as Controller in accordance with Customer’s documented instructions. Customer authorizes MicroStrategy, on its own behalf and on behalf of the other members of the Customer Group, to process personal data during the term of this DPA as a Service Provider for the purpose set out in the table set forth below.

Personal Data in relation to MCG Service

Subject matter of processing	Storage of data, including without limitation personal data, provided by Customer for its business purpose
Duration of processing	MCG Service Term
Nature of processing	Storage, back-up, recovery, and processing of personal data in connection with the MCG Service
Purpose of processing	Provision of the MCG Service
Type of personal data	The personal data uploaded for processing through the MCG Service
Categories of data subject	Employees of the Customer and Customer's customers, prospects, business partners and vendors, and employees or agents of the Customer, including those who have been authorized to use the MCG Service

The parties agree that this DPA is Customer's complete and final documented instruction to MicroStrategy in relation to Customer Data. Additional instructions outside the scope of this DPA (if any) require a prior written agreement between MicroStrategy and Customer, including an agreement on any additional fees payable by Customer to MicroStrategy for carrying out such instructions. Customer shall ensure that its instructions comply with all rules and regulations applicable in relation to Customer Data and that the processing of Customer Data in accordance with Customer's instructions will not cause MicroStrategy to be in breach of Applicable Data Protection Law. MicroStrategy will not process Customer Data outside the scope of this DPA.

MicroStrategy will:

1. Process Customer Data only on documented instructions from Customer (unless MicroStrategy or the relevant External Service Provider (see Section 5.4 below) is required to process Customer Data to comply with applicable laws, in which case MicroStrategy will notify Customer of such legal requirement prior to such processing unless such applicable laws prohibit notice to them on public interest grounds);
2. Immediately inform the Customer in writing if, in its reasonable opinion, any instruction received from them infringes any Applicable Data Protection Law;
3. Ensure that any individual authorized to process Customer Data complies with Section 5.2(1);
4. At the option of Customer, delete or return to Customer all Customer Data after the end of the provision of the MCG Service, relating to processing, and delete any remaining copies. MicroStrategy will be entitled to retain any Customer Data which it has to keep in order to comply with any applicable law or which it is required to retain for insurance, accounting, taxation, or record-keeping purposes. Section 5.3 will continue to apply to retained Customer Data.

MicroStrategy will not_"sell" Customer personal data as that term is defined in the CCPA, nor will it retain, use, or disclose Customer personal data for any purpose other than for the specific purpose of performing the services specified in the Governing Agreement, or as otherwise permitted by the CCPA or its implementing regulations. MicroStrategy certifies that it understands the restrictions and obligations under the CCPA, including the restrictions and obligations in the previous sentence, and will comply with CCPA. In addition, MicroStrategy will comply with any applicable amendments to the CCPA or its regulations.

5.3 Confidentiality

MicroStrategy will not disclose Customer personal data to any government or any other third party, except as necessary to comply with the law or a valid and binding order of a government or law enforcement agency (such as a subpoena or court order). If a government or law enforcement agency sends MicroStrategy a demand for Customer personal data, MicroStrategy will attempt to redirect the government or law enforcement agency to request that data directly from the Customer. As part of this effort, MicroStrategy may provide Customer's basic contact information to the government or law enforcement agency. If compelled to disclose Customer personal data to a government or law enforcement agency, then MicroStrategy will give the Customer reasonable notice of the demand to allow the Customer to seek a protective order or other appropriate remedy, unless MicroStrategy is legally prohibited from doing so. MicroStrategy restricts its personnel from processing Customer personal data without authorization by MicroStrategy and imposes appropriate contractual obligations upon its personnel, including, as appropriate, relevant obligations regarding confidentiality, data protection, and data security. its personnel from processing Customer personal data without authorization by MicroStrategy and imposes appropriate contractual obligations upon its personnel, including, as appropriate, relevant obligations regarding confidentiality, data protection, and data security.

5.4 Third-Party Processing

Customer authorizes MicroStrategy to engage its own affiliated companies for the purposes of providing the MCG Service. In addition, Customer agrees that MicroStrategy may use External Service Providers to fulfill its contractual obligations under this DPA or to provide certain services on its behalf. The MicroStrategy websites at https://community.microstrategy.com/s/article/MCG-External-Service-Providers list External Service Providers that are currently engaged to carry out specific processing activities on Customers' behalf. To the extent MicroStrategy engages a third-party External Service Provider to provide the MCG Service, MicroStrategy will (i) restrict the External Service Provider's access to Customer personal data to provide the MCG Service to Customer and will prohibit the External Service Provider from accessing Customer personal data for any other purpose; (ii) will enter into a written agreement with the External Service Provider; and (iii) to the extent the External Service Provider is performing the same data processing services that are being provided by MicroStrategy under this DPA, impose on the External Service Provider substantially similar terms to those imposed on MicroStrategy in this DPA.

5.5 Security of Data Processing

MicroStrategy shall, taking into account the state-of-the-art, the costs of implementation and the nature, scope, context and purpose of the processing, implement appropriate technical and organizational measures designed to provide a level of security appropriate to the risk.

Customer may elect to implement appropriate technical and organizational measures in relation to Customer personal data, directly from MicroStrategy's External Service Provider. Such appropriate technical and organizational measures include:

1. Pseudonymization and encryption to ensure an appropriate level of security;
2. Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services provided by Customer to third parties;
3. Measures to allow Customer to backup and archive appropriately to restore availability and access to Customer personal data in a timely manner in the event of a physical or technical incident; and
4. Processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

5.6 Security Breach Notification

MicroStrategy will, to the extent permitted by law, notify Customer without undue delay after becoming aware of any actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Data by MicroStrategy or MicroStrategy's External Service Provider(s) (a Security Incident). If such a Security Incident is caused by a violation of the requirements of this DPA by MicroStrategy, MicroStrategy will make reasonable efforts to identify and remediate the cause of such breach, including steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Customer agrees that an unsuccessful Security Incident will not be subject to Section 5.6. An unsuccessful Security Incident is one that results in no actual unauthorized access to Customer Data or to any of MicroStrategy's or MicroStrategy's External Service Provider's equipment or facilities storing Customer Data and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-in attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents; and MicroStrategy's obligation to report or respond to a Security Incident under this Section 5.6 is not, and will not, be construed as an acknowledgment by MicroStrategy of any fault or liability of MicroStrategy with respect to the Security Incident.

Notification(s) of Security Incidents, if any, will be delivered to Customer by any means MicroStrategy selects, including via email. It is Customer's responsibility to ensure that they provide MicroStrategy with accurate contact information and secure transmission at all times.

The information made available by MicroStrategy is intended to assist Customer in complying with their obligations under Applicable Data Protection Law in respect of data protection impact assessments and prior consultation.

5.7 Assessments

MicroStrategy does not allow clients to conduct audits or reviews of our systems or facilities, as doing so would be disruptive to our business operations. Allowing a single client to conduct audits on our systems could compromise other clients' confidentiality. However, we will answer questions about our security program and controls and provide an annual certification (Eg; ISO, SOC II Type II, Pen-test reports) or other assurances regarding our continued compliance.

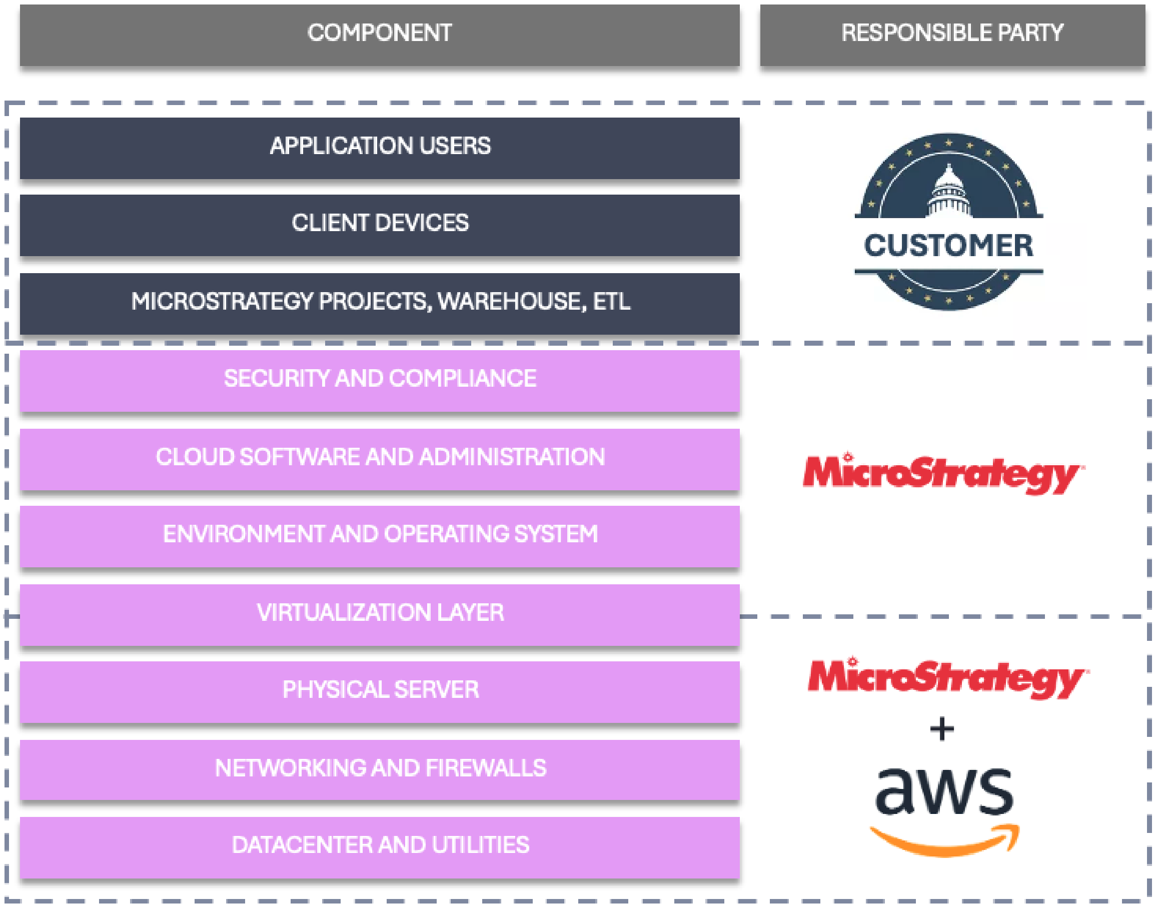
5.8 Return or Deletion of Customer Data

Due to the nature of the MCG Service, MicroStrategy's External Service Provider provides Customer with controls that Customer may use to retrieve or delete Customer Data. Up to the termination of the master agreement between Customer and MicroStrategy (Governing Agreement), Customer will continue to have the ability to retrieve or delete Customer Data in accordance with this section. For 30 days following that date, Customer may retrieve or delete any remaining Customer Data from the MCG Service, subject to the terms and conditions set out in the Governing Agreement, unless (i) it is prohibited by law or the order of a governmental or regulatory body, (ii) it could subject MicroStrategy or its External Service Providers to liability, or (iii) Customer has not paid all amounts due under the Governing Agreement. No later than the end of this 90-day period, Customer will close all MicroStrategy accounts. MicroStrategy will delete Customer Data when requested by Customer through the MCG Service controls provided for this purpose.

	MCG Support
Issue resolution by dedicated Cloud Technical Account Manager	Yes
Number of designated Support Liaisons	4
Initial response times for P1 and P2 issues **priority definitions as provided in the Technical Support Policy and Procedures	P1 < 2hr P2 < 2hr
P1 and P2 issues updates	As status changes
Case management meetings	No
System alert notifications	No
Quarterly service reporting	Via email
Location based 24x7 support	Yes

Appendix B – RACI Diagram

The RACI (Responsible, Accountable, Consulted, Informed) Table below in Appendix B highlights the roles and responsibilities of customers and MicroStrategy. Please note that some responsibility relies on Cloud service providers and, therefore, MicroStrategy will comply with cloud providers Service Level Agreement for service availability.



Activity	Description	MCG	Customer
Cloud Platform			
Environment Build	Automated build, security boundaries, etc.	RA	CI
Infrastructure Maintenance	Monthly/Emergency Maintenance Windows, OS Updates	RA	I
Environment Resizing	Upsizing/Downsizing of the VMs	RA	CI
Infrastructure Management	All cloud components such as VMs, Storage, DBMS (for MD/PA)	RA	
Backups	Compute Nodes, cache/cubes files, MD Repository, ODBC and Config files	RA	
Restores	Compute Nodes, cache/cubes files, MD Repository, ODBC and Config files	RA	CI
24x7 Support		RA	
Security & Compliance			
FedRAMP Moderate	Certifications with 3rd party audit	RA	I
FIPS 140-2	Certifications with 3rd party audit	RA	I
FIPS 200	Certifications with 3rd party audit	RA	I
FIPS 199	Certifications with 3rd party audit	RA	I
NIST Special Publication (SP) 800-53	Certifications with 3rd party audit	RA	I
NIST Cybersecurity Framework (CSF)	Certifications with 3rd party audit	RA	I
ISO27001	Certifications with 3rd party audit	RA	I
SOC2/Type 2	Certifications with 3rd party audit	RA	I

GDPR	Certifications with internal audit	RA	I
PCI	Certifications with internal audit	RA	I
HiPAA	Certifications with 3rd party audit	RA	I
24x7 Security Incident Event Management	Security logs sent to SIEM for automatic analyses	RA	I
Vulnerability Management	Scanning, remediation following the NIST standards	RA	I
Penetration Testing	Quarterly environmental external scanning	RA	I
Data Encryption at Rest	AES 256 encryption on storage volumesa dn MD DB	RA	I

Monitoring

Cloud Infra Components	VMs, Storage, DBMS (for MD/PA), Network components	RA	I
Application Services	MIcroStrategy Components like I-Server, WebApps, etc	RA	I
Data Connectivity	VPN, PrivateLink,	RA	CI
Intrusion Detection	SIEM	RA	I
Networking Connections	On-Prem Connectivity for internal access	RA	CI

Networking

Logging	VPC flow logs etc	RA	
Data source and Databases connections	Deployment/configuration of VPN Tunnels, Private Links, Express route, etc.	RA	RA
Networking Connections	On-Prem Connectivity for internal access	RA	RA

MicroStrategy Application Administration

Reference Architecture	MicroStrategy Cloud Environment Architecture	RA	I
Upgrades	Platform Upgrades via parallel environments	R	ACI
Updates	Over the top Updates - no prarallel environment required	R	AI
Post Upgrade QA (Availability of the Services)	Testing and Validation of Services health/availability	RA	CI
Post Upgrade Regression Testing	Customer Regression and functional tests/certifications	I	RA
Customer Data	Customer Data		RA
MicroStrategy Project Development	Content building and delivery		RA
MicroStrategy Project and I-Server Configuration	Project and I-Server specific settings		RA
Customizations	custom workflows, plugins/SDK Customizations, MicroStrategy Webapps Customizations	CI	RA
MicroStrategy Application User Permissions	Customer controls who has access to what reports		RA
Authentication set up	SSO Authentication Methods	R	ACI
Metadata Modelling	Building rules		RA
Platform Analytics	Initial configuration only + Monitoring of availability of the services	RA	
SMTP Server for Distribution Services	Your MCG's DS sent via your own SMTP server	CI	RA
File Subscriptions	Customer configures to send content to files on disk (S3)	RA	CI
Plugins		N/A	N/A

Pre-Prods/POC

Project Management	Aligning internal resources to complete activities. Highlighting areas of customer responsibility (SE led)	RA	CI

Build Environment (Vanilla)	Based on the platform and region of choice	RA	CI
MicroStrategy MD Restore	Restore MD and other artefacts	RA	CI
Environment Configuration	I-Server Settings, URL customization, Authentication setup, Webapps Deploy, Custom ODBC Drivers	RA	CI
Customizations	custom workflows, plugins/SDK Customizations, MicroStrategy Webapps Customizations	N/A	N/A
Testing	Testing to ensure success criteria is met (SE led with customer)	CI	RA

Migrations

Project Management	Aligning internal resources to complete activities. Highlighting areas of customer responsibility	R	ACI
Application Upgrade	Upgrade of MD and other arefacts to the latest version	RA	CI
MicroStrategy MD Restore/Refresh	Restore/Refresh MD and other artefacts	RA	CI
Environment Configuration	I-Server Settings, URL customization, Authentication setup, Webapps Deploy, Custom ODBC Drivers	RA	CI
Networking Connections	On-Prem Connectivity for internal access	RAC	ACI
Customizations	custom workflows, plugins/SDK Customizations, MicroStrategy Webapps Customizations	N/A	N/A
Post Upgrade QA (Availability of the Services)	Testing and Validation of Services health/availability	RA	CI
Post Upgrade Regression Testing	Customer Regression and functional tests/certifications	CI	RA