Strategy₿

Managed Cloud Enterprise

Service Guide

Update Published: April 2026

Copyright Information

Trademark Information

The following are either trademarks or registered trademarks of Strategy Inc or its affiliates in the United States and certain other countries:

Dossier, Enterprise Semantic Graph, Expert.Now, Hyper.Now, HyperIntelligence, HyperMobile, HyperVision, HyperWeb, Intelligent Enterprise, Strategy, StrategyB, Strategy ONE, Strategy Mosaic, Strategy Flow, Strategy 2019, Strategy 2020, Strategy 2021, Strategy Analyst Pass, Strategy Architect, Strategy Architect Pass, Strategy AI, Strategy Auto, Strategy Cloud, Strategy Cloud Intelligence, Strategy Command Manager, Strategy Communicator, Strategy Consulting, Strategy Desktop, Strategy Developer, Strategy Distribution Services, Strategy Education, Strategy Embedded Intelligence, Strategy Enterprise Manager, Strategy Federated Analytics, Strategy Geospatial Services, Strategy Identity, Strategy Identity Manager, Strategy Identity Server, Strategy Insights, Strategy Integrity Manager, Strategy Intelligence Server, Strategy Library, Strategy Mobile, Strategy Narrowcast Server, Strategy ONE, Strategy Object Manager, Strategy Office, Strategy OLAP Services, Strategy Parallel Relational In-Memory Engine (Strategy PRIME), Strategy R Integration, Strategy Report Services, Strategy SDK, Strategy System Manager, Strategy Transaction Services, Strategy Usher, Strategy Web, Strategy Workstation, Strategy World, Usher, and Zero-Click
Intelligence.

The following design marks are either trademarks or registered trademarks of Strategy Incorporated or its affiliates in the United States and certain other countries:

Other product and company names mentioned herein may be the trademarks of their respective owners.

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

Table of Contents

Overview

The Managed Cloud Enterprise service (“MCE” or “MCE Service”) is a Software-as-a-service (“SaaS”) offering that Strategy manages on its customers’ behalf in an Amazon Web Services, Microsoft Azure, or Google Cloud Platform environment that includes access to, collectively, (a) the “Cloud Platform” version of Strategy software products (an optimized version of the Strategy software platform built specifically for deployment in an Amazon Web Services, Microsoft Azure, or Google Cloud Platform environment) licensed by the customer; (b) Cloud Support, as described below; and (c) Cloud Architecture, as described below. Strategy’s SaaS delivery model is designed to allow businesses to consume the Strategy Analytics and Mobility platform in a single tenant architecture (unless otherwise described in AI Capabilities) without the need to deploy and manage the underlying infrastructure.

MCE offers a distributed compute architecture using cloud-native services provided by either Microsoft Azure, Amazon Web Services or Google Cloud Platform. As this technology evolves, Strategy continually incorporates new services that allow for increased availability, security, or performance to ensure the latest architecture is available to our customers. At the core of the solution are Strategy Analytics and Mobility, a secure, scalable, and resilient business intelligence enterprise application platform.

MCE also includes the elements needed to operate, access, and manage the intelligence architecture. Users are provisioned with their own dedicated intelligence architecture based on reference architecture. Once provisioned, users can develop, tailor, and manage the application components to meet their respective needs. Based on this operating model, customers administer and control the Analytics and Mobility solution while Strategy maintains the supporting cloud-based infrastructure.

Cloud Support

As a Managed Cloud Enterprise service customer, you will receive “Cloud Application Support” (“Cloud Support”) in which our Cloud Support engineers will provide ongoing support over your MCE Service term to assist in maximizing the performance and agility—and minimizing the cost— of your Strategy Cloud Platform deployment. Cloud Support includes environment configuration (setting up customer accounts in a selected region and CIDR for VPC/VNETs/Subnets), enterprise data warehouse integration (including modifying the Strategy configuration for data warehouse connections and opening any connectivity for external data warehouses), authentication (SSO/OIDC), and application integration.

Additionally, Standard Support for the Cloud Platform version of Strategy Products is provided with the licenses for such Products pursuant to your contract with Strategy and our Technical Support Policies and Procedures, except that all MCE customers are entitled to four Support Liaisons (as defined in the Technical Support Policies and Procedures). Strategy Cloud Elite Support is sold to MCE Service customers as an add-on offering to standard Cloud Support. A subscription to Cloud Elite Support provides MCE Service customers, among other benefits, with enhanced initial response

times for P1 and P2 issues, four additional Support Liaisons (eight total), weekly case management meetings, and customizable system alerts. Strategy's Cloud Support Offerings are detailed below in Appendix A.

If a production outage issue occurs, Strategy reserves the right to fix the issue on behalf of the customer without pre-authorization. If a support issue is logged and determined through the diagnosis that the Root Cause Analysis (RCA) indicates the stated issue is due to a customer-specific customization of the Strategy application, the Cloud Support team will provide the customer with available options to resolve the issue. These solutions may require the purchase of Strategy Professional Services for additional assistance, depending on the complexity of the issue.

Cloud Architecture

The Cloud Architecture offered as part of the MCE Service is an optimized reference architecture providing enterprise-grade data design and governance, and consists of (a) the Cloud Architecture components required to run your SaaS environment, configured through either the Single-Instance Architecture, or a High-Availability (HA) MCE 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 MCE Service offering.

Cloud Infrastructure

Our MCE Service offers a single-tenant platform architecture built based on industry, best practices for security, compliance, and availability. All offerings are fully managed cloud environments with 24/7 availability and separate metadata servers, load balancers, firewalls, data egress, and other services to ensure ease of use. This cloud infrastructure ("Additional SaaS Components") is available in several configurations, as described below:

A. The cloud infrastructure provided with the Cloud Architecture - Tier 1 operating environment (designated on an order as "Cloud Platform for AWS-Tier 1-MCE" or "Cloud Platform for Azure-Tier 1-MCE" or "Cloud Platform for GCP – Tier 1 – MCE") includes the following components:
   - one (1) production instance with up to 256 GB RAM;
   - one (1) non-production instance with up to 128 GB RAM; and
   - one (1) non-production Windows instance (Utility Box) with up to 32 GB RAM

B. The cloud infrastructure provided with the Cloud Architecture - Tier 2 operating environment (designated on an order as "Cloud Platform for AWS-Tier 2-MCE" or "Cloud Platform for Azure-Tier 2-MCE" or "Cloud Platform for GCP – Tier 2 – MCE") includes the following components:
   - two (2) production instances (HA) with up to 512 GB RAM each;
   - one (1) non-production instance with up to 256 GB RAM; and
   - one (1) non-production Windows instance (Utility Box) with up to 32 GB RAM.

C. The cloud infrastructure provided with the Cloud Architecture - Tier 3 operating environment (designated on an order as “Cloud Platform for AWS-Tier 3-MCE” or “Cloud Platform for Azure-Tier 3-MCE” or “Cloud Platform for GCP – Tier 3 – MCE”) includes the following components:
   - two (2) production instances (HA) with up to 1 TB RAM each;
   - one (1) non-production instance with up to 512 GB RAM; and
   - one (1) non-production instance with up to 256 GB RAM; and
   - two (2) non-production Windows instances (Utility Box) with up to 64 GB RAM each.

D. The cloud infrastructure provided with the Cloud Architecture - Tier 4 operating environment (designated on an order as “Cloud Platform for AWS-Tier 4-MCE” or “Cloud Platform for Azure-Tier 4-MCE” or “Cloud Platform for GCP – Tier 4 – MCE”) includes the following components:
   - two (2) production instances (HA) with up to 2 TB RAM each;
   - one (1) non-production instance with up to 1 TB RAM; and
   - one (1) non-production instance with up to 512 GB RAM; and
   - two (2) non-production Windows instances (Utility Box) with up to 64 GB RAM each.

E. Cloud Architecture - Standard offering (designated on an order as “Cloud Architecture - AWS” or “Cloud Architecture - Azure) includes the following components:
   - one (1) production node with up to 512 GB RAM;
   - one (1) non-production development node with up to 64 GB RAM; and
   - one (1) non-production Windows instance (Utility Box) with up to 32 GB RAM.

Additional nodes are also available to purchase through the execution of an order as an add-on to this offering. Each additional node purchased is for use in either production or non-production environments and includes up to 512 GB RAM. A customer may purchase additional nodes to create a HA production instance (inclusive of a high-performance file system) or for use as separate, standalone environments for quality assurance or development.

F. The Cloud Architecture - Small offering (designated on an order as “Cloud Architecture - AWS Small” or “Cloud Architecture – Azure Small”) is available for purchase by certain small to medium-sized customers with less complex requirements and includes the following components:
   - one (1) production node with up to 128 GB RAM; and
   - one (1) non-production Windows instance (Utility Box) with up to 16 GB RAM.

G. The Cloud Architecture - GCP standard offering (designated on an order as “Cloud Architecture – GCP”) includes the following components:
   - one (1) node with up to 640 GB RAM; and
   - one (1) non-production Windows instance (Utility Box) with up to 32 GB RAM.

Additional GCP nodes are also available to purchase through the execution of an order as an add-on to this offering. Each additional node purchased includes up to 640 GB RAM. A customer may purchase additional nodes to create a HA production instance (inclusive of a high-performance file system) or for use as separate, standalone environments for quality assurance or development.

H. The Cloud Architecture – GCP Small offering (designated on an order as "Cloud Architecture – GCP Small") is available for purchase by certain small to medium-sized customers with less complex requirements and includes the following components:

- one (1) node with up to 128 GB RAM; and
- one (1) non-production Windows instance (Utility Box) with up to 16 GB RAM.

These offerings are procured on your behalf from Microsoft Azure, Amazon Web Services, or Google Cloud Platform to host the Strategy Cloud Platform in an MCE and will be operated out of a mutually determined data center location. As part of these additional SaaS components, we will also provide you with Cloud Environment Support for your instance-based deployments and container-based deployments, as further described in this Guide, which includes support of your Strategy Cloud Platform managed by Strategy experts in the MCE. Such support also includes 24/7/365 system monitoring and alerting, daily backups for streamlined disaster recovery, updates and quarterly system reviews, and annual compliance checks and security certifications. Additionally, all MCE customers will receive up to 1 TB per month of data egress at no additional charge. As part of the MCE quarterly service review, we will advise you if your monthly data egress usage is close to or exceeds 1 TB for each MCE environment. Environments showing consistent high usage may be subject to overage charges or tier adjustments.

MCE Architecture

Customers who purchase either the AWS, Azure, or GCP Cloud Architecture – Standard or Cloud Architecture – Tier 1 offering of Strategy's MCE Architecture will receive one Production instance, one non-Production instance, and one Windows instance from either Microsoft Azure or Amazon Web Services or GCP. Each instance consists of a single server for Strategy Intelligence Server, Web, Library, Mobile, and Collaboration. There is also a database for the Strategy metadata, statistics, insights, and collaboration services. The MCE Architecture is built to scale to thousands of end users. Deployments post June 2025 leverage container-based architecture. Some of the benefits of the two are highlighted below:

Category	Container-Based Deployment	Instance-Based Deployment
Provisioning & Security	New provisioning console with MFA for secure, streamlined access and management.	Traditional provisioning with no MFA options for customers.
Maintenance & Updates	Monthly updates combined with maintenance — fewer events and shorter downtime.	Separate maintenance and update cycles — more frequent events and longer downtime.
Disaster Recovery	Enhanced DR with shorter targets: RTO ~4 hours / RPO ~4 hours, enabling faster recovery.	Longer recovery targets: RTO ~6 hours / RPO ~24 hours.
Scalability	Horizontal scaling enables seamless capacity expansion, with vertical scaling requiring minimal downtime.	Primarily vertical scaling, typically requiring downtime.
Operational Flexibility	Rolling updates and restarts support configuration changes (License Key, SSO, etc.) with minimal downtime.	Many configuration changes require longer planned downtime.

High-Availability MCE Architecture

Strategy's High-Availability MCE Architecture consists of a HA Cloud Architecture spanned across multiple Availability Zones. Strategy Metadata database is also HA through a multi-Availability Zone architecture offered by cloud service providers. The High-Availability MCE Architecture is included in the Cloud Architecture Tier 2, Tier 3, and Tier 4 offerings. MCE customers may move to the next available Tier if additional non-production instances are required, listed under the Cloud Architecture section.

Cloud Environment Support

As part of the Cloud Architecture, Strategy will provide Cloud Environment Support to you by maintaining your environments for the total number of instances purchased as part of an MCE Service subscription, including the following:

Service Availability

Service availability for both production and non-production instances is 24/7 by default. However, non-production instances may also be set to a minimum of 12/5 (aligned to the customer's local time zone). These parameters can be adjusted based on mutual agreement.

Root Cause Analysis (RCA)

For production outages, an RCA can be requested by the customer. Customers will receive the RCA report within ten (10) business days of the request.

Cloud Support will cover all aspects regarding the diagnosis of the RCA. It may also cover product defects, security updates, operating system updates, and changes. As

noted, if an RCA determines an issue to be created by a customer-specific customization, Strategy will provide options outside of Cloud Support, such as Professional Services engagements, to remedy the issue.

24/7 Cloud Support Hotline

For Production instance outages where system restoration is paramount, a global cloud team is mobilized for prompt resolution. The Strategy Cloud team functions around the clock to support customers and maintain service SLAs.

24/7 Monitoring and Alerting

Key system parameters are monitored for all production and non-production instances. Strategy has alerts on CPU utilization, RAM utilization, disk space, application-specific performance counters, VPN Tunnel, and ODBC warehouse sources monitoring. As part of Strategy's Cloud Elite Support Offering, customers are eligible to receive system alert notifications.

Backups

Daily backups are performed for all customer systems, including system state and metadata. By default, MCE customers will have a thirty (30) day backup retention period, and a monthly backup archive for the preceding eleven (11) months. All backups are inclusive of metadata, cubes, caches, images, and plugins. Please reach out to your Account Executive for additional cost estimates if you have additional backup requirements.

Platform Analytics

Strategy Platform Analytics is set up for all Strategy customers on MCE and maintained to allow for instant access to system performance metrics. Strategy will monitor the MCE Service-based data repository and/or cube memory requirement of the Platform Analytics database. In the event the space availability is less than 20% of the allocated storage, after receiving the customer's consent, Strategy will purge older data from the MCE 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 MCE Service, including increases to the data repository and/or cube memory requirements.

Maintenance

Maintenance windows are scheduled monthly to allow for third-party security updates to be applied to the MCE platform. During these scheduled interruptions, the MCE 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, Strategy 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 24-to 48-hour notice before applying a remedy. MCE customers are required to adhere to their monthly

maintenance window. If the assigned window is not suitable, please contact your Customer Success Manager (CSM).

Quarterly Service Reviews

The assigned designated Customer Success Manager (CSM) for your MCE will conduct the Quarterly Service Reviews (QSR) with the business and technical contacts on a quarterly cadence. This may include an overview of system resources and recommendations based on observed trends.

Infrastructure Availability

The MCE Service is architected to withstand the failure of an individual service to maintain availability. For HA environments, this is achieved by utilizing underlying application features and building on best practices. Strategy Cloud also utilizes the advantages of Availability Zones (“AZ”) in AWS, Azure, and GCP.

Intra-Region Fail-Over (HA)

For Tier 2 and above, production environments are deployed across multiple Availability Zones. This provides physical separation of compute and data and allows the service to continue running if one AZ becomes unavailable.

Instance-based deployments

In the event of an AZ failure, the remaining Instance continues to run, and data remains intact (RDS and EFS are resilient across AZs). There is no data loss and no recovery downtime. Capacity may be temporarily reduced until the failed instance is replaced.

Tier 1 will have an RPO (Recovery Point Objective) of 24 hours and an RTO (Recovery Time Objective) of 48 hours.

Container-based deployments

For container-based deployments in all Tiers, failover is automatic. If capacity is available in a third AZ, replacement workloads are started there. Some active sessions or jobs on the affected AZ may be interrupted, but services are restored automatically without manual intervention.

Inter-Region Disaster Recovery (DR)

Strategy’s MCE offering does not provide region failover in its standard offering. However, customers do have the option to purchase Inter-Region failover as an add-on to the standard offering at an additional cost. Strategy recommends having a secondary data warehouse site available for Inter-Region failover when considering a disaster recovery purchase. Strategy provides the following options for Inter-region:

Instance-Based Deployments

Hot-Cold: A failover environment is pre-provisioned in the secondary region but remains shut down until a disaster occurs in the primary region. Provides a targeted RPO of 24 hours and RTO of 6 hours.

Hot-Warm: A failover environment is pre-provisioned in the secondary region and refreshed daily with metadata. The environment is shut down after each refresh. Provides a targeted RPO of 24 hours and RTO of 4 hours.

Container-Based Deployments

Hot-Cold: A failover environment is provisioned in the secondary region only after a disaster occurs in the primary region. Provides a targeted RPO of 4 hours and RTO of 4 hours.
Hot-Warm: A failover environment is provisioned in the secondary region upon disaster. Provides a targeted RPO of 30 minutes and RTO of 2 hours.

Updates and Upgrades

Strategy is committed to providing the latest updates with security fixes, therefore all customers are required to take advantage of the fixes and new features. For each Product license, we will deliver to you every quarter for instance-based deployments and every month for container-based deployments at no charge and at your request, an update and/or upgrade as part of the Technical Support Services subscription. Major upgrades are completed in a free parallel environment for up to 30 days to allow for customer testing for instance-based deployments while it will be in place for container-based deployments. Updates may not include new separately marketed products. Customers requiring longer than 30 days to complete the upgrade should contact their Account Executive.

Your Customer Success Manager (CSM) will work with you each quarter and/or month to schedule the updates. These updates are seamless and carry over all customizations in your Strategy environment. The customer is responsible for ensuring SDK Mobile apps are recompiled to comply with newer versions of Strategy. Customers are also encouraged to perform regression testing on the updated environment, along with data validation and testing other custom workflows.

Roles and Responsibilities

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

Non-Migrated Strategy Components

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

- Strategy Narrowcast Server replaced with Distribution Services
- Strategy Enterprise Manager replaced with Platform Analytics
- Legacy Office plugin (non-365 version)

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

- IIS web server to support MDX

- Customizations not in plugin form

Distribution Services

All Strategy Cloud customers are required to use their own SMTP server for delivery of email and history list subscriptions. File subscriptions are pushed to an Amazon S3 bucket, Azure BLOB Storage, or Google Cloud Storage, provided to the customer as part of the MCE infrastructure. Customers may pull file subscriptions from the storage locations provided during the onboarding process with their Customer Success Manager (CSM). Our Professional Services team is available to assist with any customizations that may be required to move File subscriptions from Amazon S3, AZURE Blob Storage, or Google Cloud Storage to the desired location.

MCE Migration Licensing

As part of the MCE Service, two additional administrative accounts are provisioned automatically within your dedicated MCE environment at no additional charge, exclusively for Cloud operations and maintenance purposes. These accounts are environment-specific and are never shared across other MCE environments. The first is the 'mstr' account. The second is a cloud provider-specific administrator account: 'Cxxx-administrator' or 'Wxxx-administrator' for AWS, 'Axxx-administrator' or 'Kxxx-administrator' for Azure, or 'Gxxx-administrator' for GCP.

The 'mstr' account must never be deleted, as it is required for ongoing Cloud operations and maintenance.

AI Capabilities

The “AI Power User,” “AI Consumer User,” “AI Architect User,” “Strategy AI,” and “Strategy 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 Strategy 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. You must use our AI capabilities only for the intended purpose set forth in this Guide and in the Strategy AI Security Whitepaper, available here: Strategy AI Security Whitepaper. To the extent your use of our AI offerings could potentially be classified as high risk under the EU AI Act or other applicable laws and regulations governing AI, such use is undertaken solely at your own risk and you must comply with all applicable laws and regulations governing its use and Strategy has no responsibility or liability for any loss, damage, claim, cost, or other consequence arising from or related to such use.

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 Strategy AI SKU

- For each Strategy 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 Strategy AI SKU quantity for a subsequent Use Period, each at the then current list price for such Strategy, 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. Strategy 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 Strategy 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 Strategy AI SKU. Below are examples of a Question:
    - Auto Answers (multiple consumption options):
        - One action submitted to Strategy's Auto chatbot that returns a response constitutes consumption of one Question.
        - One click on auto-populated suggestions below Strategy'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 Strategy's Auto chatbot that returns a response constitutes consumption of one Question.
    - Auto Dashboard (multiple consumption options):
        - One action submitted to Strategy's Auto chatbot that returns a response constitutes consumption of one Question.
        - One click on auto-populated suggestions below the Strategy'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.

Agent Activation

For configurations that include any combination of “AI Power User,” “AI Consumer User,” or “AI Architect User,” customers may request additional advisory assistance related to getting started with their Agentic features (Agent Activation Advisory). Agent Activation Advisory assistance can be requested only once and is limited to the following 2 Agents, as detailed below:

- 1 Structured Agent includes: 2 datasets, 15 attributes per dataset, 15 metrics per dataset, 5 derived metrics, 1 language, and up to 5M rows per dataset.
- 1 Unstructured Agent includes: up to 3 PDF/Doc files with up to 250 pages per document.

If additional advisory services are needed, Strategy will provide options outside of Cloud Support, such as Professional Services engagements.

Security

Various security tools are employed to perform penetration testing and remediation, system event logging, and vulnerability management. The MCE Service maintains a high security posture in accordance with the following security standards:

Service Organization Controls (SSAE-18)

SSAE-18 is the service organization auditing standard maintained by the AICPA. It evaluates Service Organization Controls over the security, availability, and processing integrity of a system and the confidentiality and privacy of the information processed by the system. Our MCE Service maintains a SOC2 Type 2 report.

Health Insurance Portability and Accountability Act (HIPAA)

Controls designed to protect health information.

Payment Card Industry Data Security Standards (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information. MCE maintains an SAQ-D for Service Providers.

International Organization for Standardization (ISO 27001-2)

International Organization for Standardization (ISO 27001-2) is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance.

MCE Security Scans

Strategy will conduct a security review on all custom components provided by the customers, such as plugins, drivers, etc. Customer is responsible for the remediation of all security findings.

Cloud Shared Services Components

As part of the MCE Service’s platform architecture and in support of the Cloud Environment, we incorporate third-party solutions to assist in the management,

deployment, and security of the infrastructure, and to complete operational tasks. These include management and detection response solutions, cloud security posture management solutions, application/infrastructure monitoring, alerting and on call management solutions, and workflow and continuous integration tools.

Service Availability

MCE offers a service level agreement of 99.9% for HA production environments and 99% service level for single instance non-HA production environments. Availability is calculated per calendar month as follows:

$$\left[\left(\frac{\text{Total Minutes} * \#\text{ of Production Instances} - \text{Unavailability}}{\text{Total Minutes} * \#\text{ of Production Instances}} \right) * 100 \right]$$

Service Definition

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

"Production Instance": an MCE 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 MCE is unavailable due to issues related to applications built on the Strategy 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 Strategy's reasonable control.

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

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

Service Remedies

If the availability standard of 99.9% (for HA Production Instances) and 99% (for non-HA Production Instances) 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 MCE Service, managed by Strategy, within the calendar month that a Service Credit has been accrued. This is the exclusive remedy available to customers in the event Strategy fails to comply with the service level requirements set forth in the availability designed in the Service Availability section.

Service Credits

HA Production Instance:

- 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-HA Production Instance:

- 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

Service Credits Procedure

To receive a Service Credit, customers must submit a Strategy 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 Strategy during onboarding and Intelligence Architecture delivery activities; and (e) a detailed description of the actions taken by users to resolve the unavailability.

Once Strategy receives this claim, Strategy 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 MCE). Thereafter, Strategy will determine in good faith whether a Service Credit has accrued and will notify customers of its decision. If Strategy determines that a Service Credit has accrued, then at its discretion, it will either (1) apply the Service Credit to the next MCE Service invoice sent or (2) extend the MCE Service Term for a period commensurate with the Service Credit amount. Customers may not offset any fees owed to Strategy with Service Credits.

Exclusions

In the context of Strategy MCE services delivered via a SaaS model, the following are considered exclusions for service as it concerns all matters of impacts to availability:

1. **Scheduled Maintenance**: Service interruptions during scheduled maintenance, announced in advance, are excluded from the SLA.
2. **Customer Configurations**: Service issues caused by customer actions, such as misconfigurations or excessive API requests, are not covered. Issues related to applications built on the Strategy software platform, including project, report, and document issues; migration problems related to user design; downtime experienced as a result of user activity.
3. **ETL Application:** Outages caused through degradation or failure of ETL processes in the application.
4. **Database Issues and Configuration:** Improper database logical design and code issues.
5. **Hyperscaler or other Third-party Services**: Downtime related to third-party services or dependencies outside control is excluded.
6. **Force Majeure**: Events beyond control of Strategy, such as natural disasters or government actions, do not qualify for SLA coverage.
7. **Unauthorized Access**: Issues not originated by Strategy like unauthorized access or credential compromised
8. **Customer-Based Migration Issues:** Migration problems and outages related to customer or user design.
9. **SSO or other Custom Security Configuration or Policies**: Implementation and management of custom security policies and compliance measures outside the pre-configured, standard security settings are not included.
10. **Network Connectivity Issues**: Issues related to the customer's internal network or internet connectivity, including VPN configurations and local firewall settings, fall under the customer's responsibility.

These exclusions ensure a clear boundary of responsibilities and help manage expectations for the scope and limits of Strategy MCE services within a SaaS delivery model.

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 Strategy and the customer ("Customer"), including any order(s) and/or a master agreement between the customer and Strategy (collectively, the "Governing Agreement"), and shall be considered a Data Processing Addendum (DPA). Except as amended by this DPA, the Governing Agreement will remain in full force and effect.

Definitions

"Customer Group" means Customer and any affiliate, subsidiary, subsidiary undertaking and holding company of Customer (acting as a Controller) accessing or using the MCE Service on Customer's behalf or through Customer's systems or any other third party who is permitted to use the MCE Service pursuant to the Governing Agreement between Customer and Strategy, but who has not signed its own Order Form with Strategy.

“Data Privacy Framework” means, as relevant, (i) the EU-US Data Privacy Framework as administered by the US Department of Commerce and approved by the European Commission as ensuring an adequate level of protection for Personal Data for the purposes of Article 45 GDPR; (ii) the UK Extension to the EU-US Data Privacy Framework approved by the competent authority of the United Kingdom as ensuring an adequate level of protection for Personal Data for the purposes of Article 45 UK GDPR; and (iii) the Swiss-US Data Privacy Framework as administered by the US Department of Commerce and approved by the Swiss Federal Administration as ensuring an adequate level of protection for Personal Data for the purposes of applicable Swiss data protection laws, in each case as in force, amended, consolidated, re-enacted or replaced from time to time.

“**EU/UK Privacy Laws**” means, as applicable: (a) the General Data Protection Regulation 2016/679 (the “**GDPR**”); (b) the Privacy and Electronic Communications Directive 2002/58/EC; (c) the UK Data Protection Act 2018, the UK General Data Protection Regulation as defined by the UK Data Protection Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (together with the UK Data Protection Act 2018, the “**UK GDPR**”), and the Privacy and Electronic Communications Regulations 2003; and (d) any relevant law, directive, order, rule, regulation or other binding instrument which implements any of the above, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

“**Personal Data**” means any information that Strategy processes on behalf of Customer to provide the Services that is defined as “personal data” or “personal information” under any Privacy Law. “**Privacy Laws**” means, as applicable, EU/UK Privacy Laws, US Privacy Laws, and any similar law of any other jurisdiction which relates to data protection, privacy, or the use of Personal Data, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

“**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 Strategy’s or
Strategy’s Sub-Processors’ equipment or facilities storing Personal Data, including, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful logon 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.

“Sub-Processor” means any third party appointed by Strategy to process personal data.

“**Third Country**” means any country or territory outside of the scope of the data protection laws of the European Economic Area or the UK, as relevant, that has not been approved as providing adequate protection for Personal Data by the relevant competent authority from time to time.

“**US Privacy Laws**” means, as applicable, the California Consumer Privacy Act, Colorado Privacy Act, Connecticut Data Privacy Act, Delaware Personal Data Privacy Act, Florida Digital Bill of Rights,
Indiana Consumer Data Protection Act, Iowa Consumer Data Protection Act, Montana Consumer Data Privacy Act, Oregon Consumer Privacy Act, Tennessee Information

Protection Act, Texas Data Privacy and Security Act, Utah Consumer Privacy Act, and Virginia Consumer Data Protection Act, and any similar law of any other state related to the processing of Personal Data.

Data Processing

As a Processor, Strategy will process the Personal Data that is uploaded or transferred to the MCE Service as instructed by Customer or provided by Customer as Controller in accordance with Customer's documented instructions. Customer authorizes Strategy, on its own behalf and on behalf of the other members of its Customer Group, to process Personal Data during the term of this DPA as a Processor for the purpose set out in the table below.

Personal Data in relation to MCE Service	
Subject matter of processing	Storage of data, including, without limitation Personal Data, provided by Customer for its business purpose
Duration of processing	MCE Service Term and 90 days following expiry of such term
Nature of processing	Storage, back-up, recovery, and processing of Personal Data in connection with the MCE Service.
Purpose of processing	Provision of the MCE Service
Type of personal data	The Personal Data uploaded or transferred for processing through the MCE Service by the Customer
Categories of data subject	Employees or agents of the Customer and Customer's customers, prospects, business partners, vendors, and those individuals who have been authorized to use the MCE Service by the Customer

Strategy may aggregate and/or anonymize Personal Data such that it no longer constitutes Personal Data under Privacy Laws and process such data for its own purposes. To the extent Strategy receives de-identified data (as such term is defined under applicable US Privacy Laws) from Customer, Strategy shall: (i) take commercially reasonable measures to ensure that the data cannot be associated with an identified or identifiable individual; (ii) publicly commit to maintain and use the data only in a de-identified form and not attempt to re-identify the data; and (iii) otherwise comply with applicable US Privacy Laws with respect to such de-identified data. Customer will take all measures possible to avoid transferring or providing us with any access to any Personal Data to the extent possible while continuing to use the MCE Service.
In processing Personal Data under the Agreement, Strategy will:

1. only process Personal Data on documented instructions from Customer which the Parties agree that this DPA is Customer's complete and final documented instruction to Strategy in relation to Personal Data (which the parties agree are reflected in full in this DPA), for the limited and specific purpose described in the table above, and at all times in compliance with Privacy Laws, unless required to process such Personal Data by applicable law to which Strategy is subject; in such a case, Strategy shall

inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

2. notify Customer without undue delay if it: (i) makes a determination that it can no longer meet its obligations under applicable US Privacy Laws or (ii) believes that instruction of Customer, infringes applicable Privacy Laws;
3. to the extent required by Privacy Laws, and upon reasonable written notice that Customer reasonably believes Strategy is using Personal Data in violation of Privacy Laws or this DPA, grant Customer the right to take reasonable and appropriate steps to help ensure that Strategy uses the Personal Data in a manner consistent with Customer's obligations under Privacy Laws, and stop and remediate any unauthorized use of the Personal Data; and
4. require that each employee or other person processing Personal Data is subject to an appropriate duty of confidentiality with respect to such Personal Data.
5. To the extent required by applicable Privacy Laws, Strategy will not:
   a) sell the Personal Data or sharing the Personal Data for cross-context behavioral advertising purposes;
   b) retain, use, or disclose the Personal Data outside of the direct business relationship between Strategy and Customer and for any purpose other than for the specific purpose of performing the Services; and
   c) combine the Personal Data received from, or on behalf of, Customer with any Personal Data that may be collected from Strategy's separate interactions with the individual(s) to whom the Personal Data relates or from any other sources, except to perform a business purpose or as otherwise permitted by Privacy Laws.

Customer Obligations

Customer shall comply with all Privacy Laws in providing Personal Data to Strategy in connection with the Services. Customer represents and warrants that:
a) the Privacy Laws applicable to Customer do not prevent Strategy from fulfilling the instructions received from Customer and performing Strategy's obligations under this DPA;
b) all Personal Data was collected and at all times processed and maintained by or on behalf of Customer in compliance with all Privacy Laws, including with respect to any obligations to provide notice to and/or obtain consent from individuals; and
c) Customer has a lawful basis for disclosing the Personal Data to Strategy and enabling Strategy to process the Personal Data as set out in this DPA.
Customer shall notify Strategy without undue delay if Customer makes a determination that the processing of Personal Data under the Agreement does not or will not comply with Privacy Laws, in which case, Strategy shall not be required to continue processing such Personal Data.
5.4 Sub-Processing
To the extent Strategy engages any Sub-Processors to process Personal Data on its behalf:

a) Customer hereby grants Strategy general written authorization to engage the Sub-Processors set out on the Strategy's website, currently at: https://community.strategy.com/article/strategy-sub-processors (as such website addresses may be amended or replaced from time to time), subject to the requirements of this section.

b) If Strategy appoints a new Sub-Processor or intends to make any changes concerning the addition or replacement of any Sub-Processor which will process Personal Data that Strategy is processing on behalf of Customer, Strategy shall update the websites set out in Section 5.4(a) above and inform Customer of such update via e-mail if the new or replacement Sub-Processor will process any Personal Data. If Customer fails to object to the appointment or replacement within thirty (30) days of its posting on reasonable and documented grounds related to the confidentiality or security of Personal Data or the subcontractor's compliance with Privacy Laws, Strategy may proceed with the appointment or replacement. If Customer reasonably objects to a new Sub-Processor, Customer shall inform Strategy in writing within thirty (30) days following the update of the applicable Sub-Processor list and such objection shall describe Customer's legitimate reasons for objection. Strategy shall have the right to cure any objection by, in its sole discretion, either choosing to (i) take any corrective steps requested by Customer in its objection (which steps will be deemed to resolve Customer's objection) and proceed to use the Sub-Processor or (ii) suspend and/or terminate any product or service that would involve the use of the Sub-Processor.

c) Strategy shall engage Sub-Processors only pursuant to a written agreement that contains obligations on the subcontractor which are no less onerous on the relevant subcontractor than the obligations on Strategy under this DPA.

d) In the event Strategy engages a Sub-Processor to carry out specific processing activities on behalf of Customer pursuant to EU/UK Privacy Laws, where that Sub-Processor fails to fulfil its obligations, Strategy shall remain fully liable under applicable EU/UK Privacy Laws to Customer for the performance of that Sub-Processor's obligations.

Transfers of Personal Data

Customer acknowledges and agrees that Strategy may appoint an affiliate or third-party Sub-Processor to process the Personal Data in a Third Country, in which case, Strategy shall ensure that any Personal Data transferred to such affiliate or third-party shall be done so pursuant to a valid data transfer mechanism under EU/UK Privacy Laws, such as the Data Privacy Framework (if applicable) or the standard contractual clauses for the transfer of Personal Data to third countries.

Security of Data Processing

Strategy 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 also elect to implement appropriate technical and organizational measures in relation to Customer Personal Data, directly from Strategy's Sub-Processor. Such appropriate technical and organizational measures include:

a) Pseudonymization and encryption to ensure an appropriate level of security;

b) Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services provided by Customer to third parties;

c) Measures to allow Customer to backup and archive appropriately to restore availability and access to CustomerPersonal Data in a timely manner in the event of a physical or technical incident; and
d) Processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

Security Breach Notification

To the extent required by Privacy Laws, Strategy shall without undue delay notify Customer of any Security Incident, with further information about the Security Incident provided in phases as more details become available. For the avoidance of doubt, Strategy's obligation to report or respond to a Security Incident, including without limitation, under this section, is not and will not be construed as an acknowledgement by Strategy of any fault or liability of Strategy with respect to the Security Incident.

Audit

Upon reasonable request of Customer, Strategy shall make available to Customer such information in its possession as is reasonably necessary to demonstrate Strategy's compliance with its obligations under this DPA, and allow for and contribute to audits by providing written responses to questionnaires and copies of relevant documents. As an alternative to an audit performed by the Customer, to the extent permitted by Privacy Laws, Strategy may arrange for a qualified and independent auditor to conduct, at Customer's expense, an assessment of Strategy's policies and technical and organizational measures in support of its obligations under Privacy Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessment, and will provide a report of such assessment to Customer upon reasonable request. Notwithstanding the foregoing, in no event shall Strategy be required to give Customer access to information, facilities, documents or systems to the extent doing so would cause Strategy to be in violation of confidentiality obligations owed to other customers or its legal obligations.

Customer acknowledges and agrees that our rights to audit our Sub-Processors referred to in the Transfers of Personal Data section above will be subject to the terms we have in place with each such Sub-Processor and will likely involve: (i) using external auditors to verify the adequacy of security measures including the security of the physical data centers from which the Sub-Processor provides the Services; (ii) ISO 27001 standards or other such alternative standards that are substantially equivalent to ISO 27001; and (iii) the generation of an audit report ("**Report**"), which will be the Sub-Processor's confidential information or otherwise be made available subject to a mutually agreed upon non-disclosure agreement covering the Report ("**NDA**"). Strategy may not be able to disclose such Report to Customer without permission from the Sub-Processor. At Customer's reasonable written request during the exercise of its audit rights under the Independent Determination section below, Strategy will request the permission to provide Customer with a copy of such Report so that Customer can reasonably verify the Sub-Processor's compliance with its security obligations, provided that Customer acknowledges that the Sub-Processor may require Customer to enter into an NDA with such Sub-Processor before releasing the same.

Independent Determination

Customer is responsible for reviewing the information made available by Strategy and its Sub-Processor relating to data security and making an independent determination as to whether the MCE Service meets Customer's requirements and legal obligations, as well as Customer's obligations under this DPA.

Assistance

To the extent required by Privacy Laws, and taking into account the nature of the processing, Strategy shall, in relation to the processing of Personal Data and to enable Customer to comply with its obligations which arise as a result thereof, provide reasonable assistance to Customer, through appropriate technical and organizational measures, in: responding to requests from individuals pursuant to their rights under Privacy Laws, including by providing, deleting, or correcting the relevant Personal Data, or by enabling the Customer to do the same, insofar as this is possible;

a) responding to requests from individuals pursuant to their rights under Privacy Laws, including by providing, deleting, or correcting the relevant Personal Data, or by enabling the Customer to do the same, insofar as this is possible;
b) implementing reasonable security procedures and practices appropriate to the nature of the Personal Data to protect the Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure;
c) notifying relevant competent authorities and/or affected individuals of any Security Incident;
d) conducting data protection impact assessments and, if required, prior consultation with relevant competent authorities; and
e) entering into this DPA.

Return or Deletion of Customer Data

Due to the nature of the MCE Service, Strategy's Sub-Processor provides Customer with controls that Customer may use to retrieve Customer Data in the format in which it was stored as part of the MCE Service or delete Customer Data. Up to the termination of the Governing Agreement between Customer and MicroStrategy, Customer will continue to have the ability to retrieve or delete Customer Data in accordance with this section For 90 days following that date, Customer may retrieve or delete any remaining Customer Data from the MCE 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 Sub-Processors 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 MCE Service controls provided for this purpose.

Appendix A - Cloud Support Offerings

Support Detail	Cloud Support	Cloud Elite Support
Designated Customer Success Manager (CSM)	Yes	Yes
Number of designated Support Liaisons	4	8
Architect Education Passes	0	8
Initial response times for P1 and P2 issues*	P1 < 2hr P2 < 2hr	P1 < 15 minutes P2 < 1 hour
P1 and P2 issues updates	As status changes or daily	P1 every 1 hour P2 as status changes or twice a day
Case management meetings	No	Weekly
System alert notifications	No	Yes
Quarterly service reporting	Via email	Via meeting
Location-based 24/7 support	No	Yes

*Priority definition as provided in the Technical Support Policy and Procedures.

Appendix B - RACI Diagram

ACTIVITY	DESCRIPTION	MCE STANDARD	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 Instances, cache/cubes files, MD Repository, ODBC, and Config files	RA	
Restores	Compute Instances, cache/cubes files, MD Repository, ODBC and Config files	RA	CI
24/7 Support		RA	
Security & Compliance			
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
24/7 Security Incident Event Management	Security logs sent to SIEM for automatic analysis	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 volumes and MD DB	RA	I
Monitoring			
Cloud Infrastructure Components	VMs, Storage, DBMS (for MD/PA), Network components	RA	I
Application Services	Strategy Components like I-Server, WebApps, etc.	RA	I
Data Connectivity	VPN, PrivateLink	RA	CI
Intrusion Detection	SIEM	RA	I
Logging	Load balancer logs, etc.	RA	
Data source and Databases connections	Deployment/configuration of VPN Tunnels, Private Links, Express route, etc.	RA	RA

Strategy Application Administration			
Reference Architecture	MCE Architecture	RA	I
Upgrades	Platform Upgrades via parallel environments	R	ACI
Updates	Over the top Updates - no parallel environment required	R	ACI
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
Strategy Project Development	Content building and delivery		RA
Strategy Project and I-Server Configuration	Project and I-Server specific settings		RA
Customizations	Custom workflows, plugins/SDK Customizations, Strategy Webapps Customizations	CI	RA
Strategy Application User Permissions	Customer controls who has access to what reports		RA
Authentication set up	SSO and OIDC Supported 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 MCE's DS sent via your own SMTP server	CI	RA
File Subscriptions	Customer configures to send content to files on disk (Blob or	RA	CI

	Amazon S3, or Google Cloud Storage)		
Plugins		CI	RA
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
Strategy MD Restore	Restore MD and other artifacts	RA	CI
Environment Configuration	I-Server Settings, URL customization, Authentication setup, Webapps Deploy, Custom ODBC Drivers	RA	CI
Networking Connections	On-Premise Connectivity for internal access	RAC	ACI
Customizations	Custom workflows, plugins/SDK Customizations, Strategy Webapps Customizations	CI	RAC
Testing	Testing to ensure the success criteria are met (SE led with the 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 artifacts to the latest version	RA	CI
Strategy MD Restore/Refresh	Restore/Refresh MD and other artifacts	RA	CI
Environment Configuration	I-Server Settings, URL customization, Authentication setup, Webapps Deploy, Custom ODBC Drivers	RA	CI
Networking Connections	On-Premise Connectivity for internal access	RAC	ACI

Customizations	Custom workflows, plugins/SDK Customizations, Strategy Webapps Customizations	CI	RAC
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

Strategy₿