Service Description

Content Manager Select as a Service

August 2023

Contents

This Service Description describes the components and services included in OpenText Content Manager Select as a Service (which also may be referred to as “CMSaas” or “SaaS”) and, unless otherwise agreed to in writing, is subject to the Micro Focus Customer Terms for Software-as-a-Service (“SaaS Terms”) found at https://www.microfocus.com/en-us/legal/software-licensing. Capitalized terms used but not defined herein shall have the meanings set forth in the SaaS Terms.

Standard Service Features

High Level Summary

The agreement describes the responsibilities of each support group (Micro Focus & Citadel), including the process and timeframe for delivery of their services. The objective of the OLA is to present a clear, concise, and measurable description of the services to be delivered in the delivery on Content Manager Select as a Service (CMSaaS).

The Operational Level Agreement may be updated periodically.

Intended Audience

The intended audience for this document is both Micro Focus and Citadel operational support and delivery teams responsible for the Content Manager Select as a Service (CMSaaS) product.

Solutions Overview

CMSaaS is a cloud-based solution, delivering enterprise content management as a fully managed and hosted service.

Content Manager is a governance-based enterprise content management (ECM) system designed to meet the global needs of government, regulated industry, and enterprises. CMSaaS brings corporate knowledge into a single, reliable, secure cloud which can be accessed anywhere, anytime, and from any device.

The Citadel Group Limited oversees the deployment, infrastructure, operation, availability, security and data protection and support of the service.

Micro Focus Service Operations Centre, Micro Focus Professional Services, authorized Micro Focus partners, and the Customer themselves provide product and business configuration support of the service.

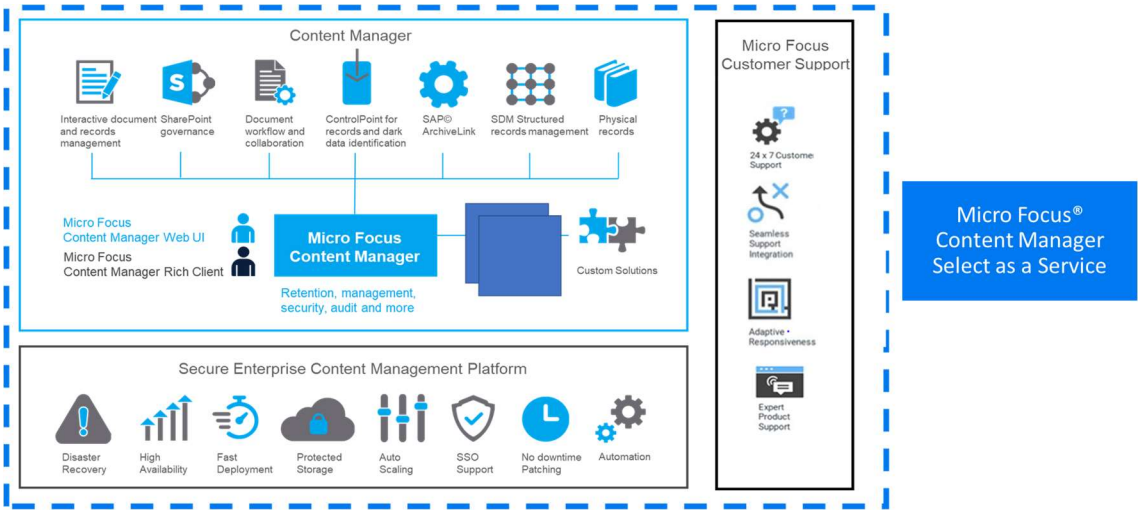


Figure 1 CMSaaS Solution Overview

Product Offerings

Standard Inclusion	Gold Edition	Platinum Edition	Titanium Edition
• 24 x 7 Customer Support • All CM add-on modules* management tools • Unlimited "Read-Only" users • Volume-Based billing for Object Storage • High-Availability (HA) • Geo-Redundant Data Protection • ISO/IEC 27001:2013 Certified	• 99.9% Availability • Disaster Recovery Instance • Recovery Point Objective < 15 minute • Recovery Time Objective < 24 hours • Maximum 1,000 Users • Suitable for SME businesses	• 99.95% Availability • Disaster Recovery Instance • Recovery Point Objective < 1 minute • Recovery Time Objective < 4 hours • Suitable for most businesses	• 99.95% Availability • Disaster Recovery Instance • Recovery Point Objective < 1 minute • Recovery Time Objective < 15 Minute • Suitable for mission critical workloads

Service Delivery Components

SaaS Delivery Components	Gold Edition	Platinum Edition	Titanium Edition
CMSaaS Production Instance (includes 1 Non-Production Instance)	√ (1000 included users)	√ (3000 included users)	√ (3000 included users)
Additional CMSaaS Non-Production Instance	O	O	O
Object Volume Packs	O	O	O
Additional Metadata / Database Storage	O	O	O
Professional Services or Premium Support (MF Professional Services / Partner Support)	O	O	O
√ = Included			
O = Optional for a fee			

Operational Services

Operational Services		
Single Sign on Support*	√	√
IP Whitelisting	√	√
Additional Remote Site Backup Service	O	O
Customer Onboarding	√	√
Citadel Business Support	√	√
24 x 7 Service Desk	√	√
Content Manager Upgrades (every 2 years)	√	
Application Management & Monitoring	√	
Application Patch Management - CM9 Critical Patches	√	
Security Management	√	√
Server Management	√	√
Storage Management	√	√
Database Management	√	√
Network Management (within CMSaaS Platform)	√	√
Disaster Recovery Management & Testing	√	√
√ = Included		
O = Optional for a fee		

Architecture Components

CMSaaS is a “multi-instance” architecture that delivers logical, single tenancy by isolating all customer data. This is achieved by utilizing an enterprise-grade cloud architecture and a dedicated database and application set per customer instance - there is no combining of data or other forms of multi-tenancy. The presentation layer is delivered through a web interface and desktop client. The desktop client is installed and configured by Customer or Customer-contracted Micro Focus partner. Micro Focus does not operate onsite components or third-party integration on behalf of Customer and will not commit to any SLO for these components.

A CMSaaS instance is an entirely discrete Content Manager environment consisting of two or more application nodes and a single database and document store which stores all data and content for the instance.

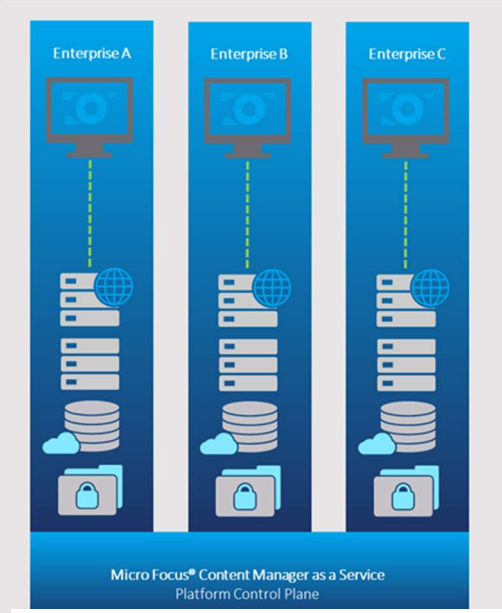


Figure 2 CMSaaS Multi-Instance Architecture

Figure 3 Multi-Tenant vs Multi-Instance Architecture

Technical Components

CMSaaS offers a hosted solution built on OpenText Content Manager and Microsoft Azure IaaS and PaaS (collectively, “Azure”) to offer a secure, highly available and scalable records management solution.

The solution is deployed a multi-layer n-tiered architecture with security, presentation application and data components comprising one or more tiers respectively, as shown in Figure 4, below. Each of the layers sits within its own subnet and Network Security Group to provide defense in depth with only explicitly allowed traffic reaching each layer as needed. Each layer also sits within its own Azure VM ScaleSet which allows the infrastructure to automatically scale up and down based on end user traffic and performance requirements.

Ingress traffic must pass through the Web Application Gateway with Web Application Firewall which is configured to block most common attack vectors. Web traffic is routed to the Web Application Proxy to perform a pre-authentication check. Unauthenticated traffic is directed to the CMSaaS ADFS which in turn redirects traffic to the Customers IdP for authentication against the Customers Active Directory and Multi-factor authentication agent.

Appropriately authorized web traffic is then permitted to reach the CMSaaS Web Server which in turn makes internal service calls to the CMSaaS Workgroup Servers and Search Servers as required. Thick client traffic will be pre-authenticated internally on the Customer’s network and carry an appropriate authorization token across the TLS encrypted link to the Workgroup Servers.

CMSaaS is designed to take advantage of the reliability and redundancy of the Azure PaaS services where possible and uses Azure SQL for the Content Manager relational metadata store. In the configuration used by CMSaaS, Azure SQL provides a highly available and geo-redundant relation metadata store with transparent data encryption to ensure that data is encrypted at rest.

The service is built from Microsoft-provided base images and scripted to the running state using Desired State Configuration (PowerShell DSC) and custom automation playbooks.

Content Manager Version 9.2 added direct support for Azure Blob storage accounts and CMSaaS utilizes this for the document storage layer. This allows the CMSaaS solution to leverage highly scalable geo-replicated storage on the Azure platform.

The solution maintains data sovereignty with two verifiable Azure Regions within Australian borders, Australia East (Sydney region) and Australia South East (Melbourne region). The Australia East is the primary region while Australia South East is configured as the DR location in the event of a catastrophic region outage in the primary location.

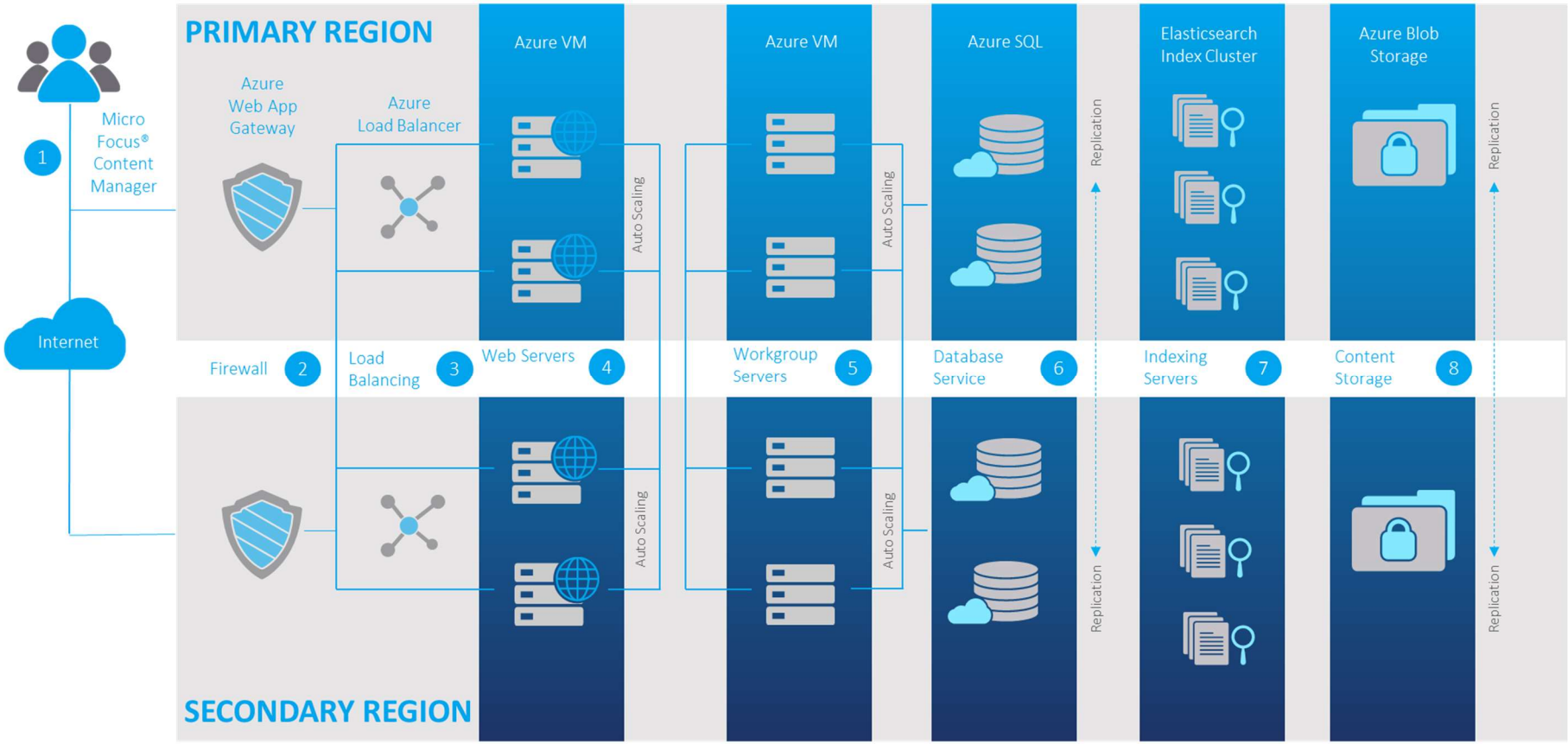


Figure 4 CMSaaS Instance Technical Architecture

Application Administration

Customer accesses CMSaaS using a Content Manager Client application (desktop or web client) and the service URLs provided to them. Once securely logged in, Customer can perform administrative tasks such as adding and deleting users and other objects within the CM Locations Directory, managing Record Types, Business Classification Schemes, Retention and Disposal Schedules, and configuring / administering all other system objects and configuration items.

CMSaaS Order to Cash Process

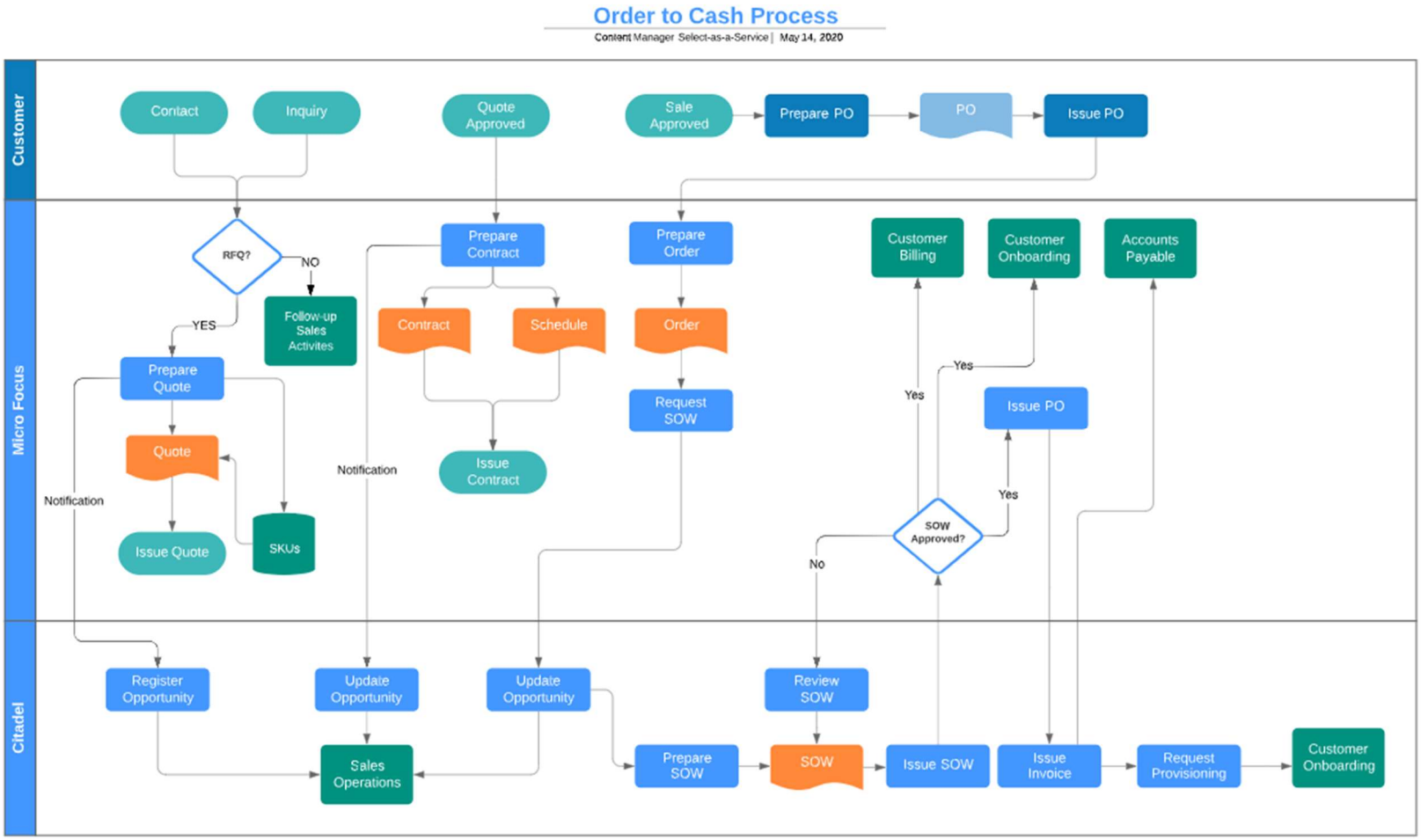


Figure 5 CMSaaS Order to Cash Workflow Overview

CMSaaS Customer Onboarding

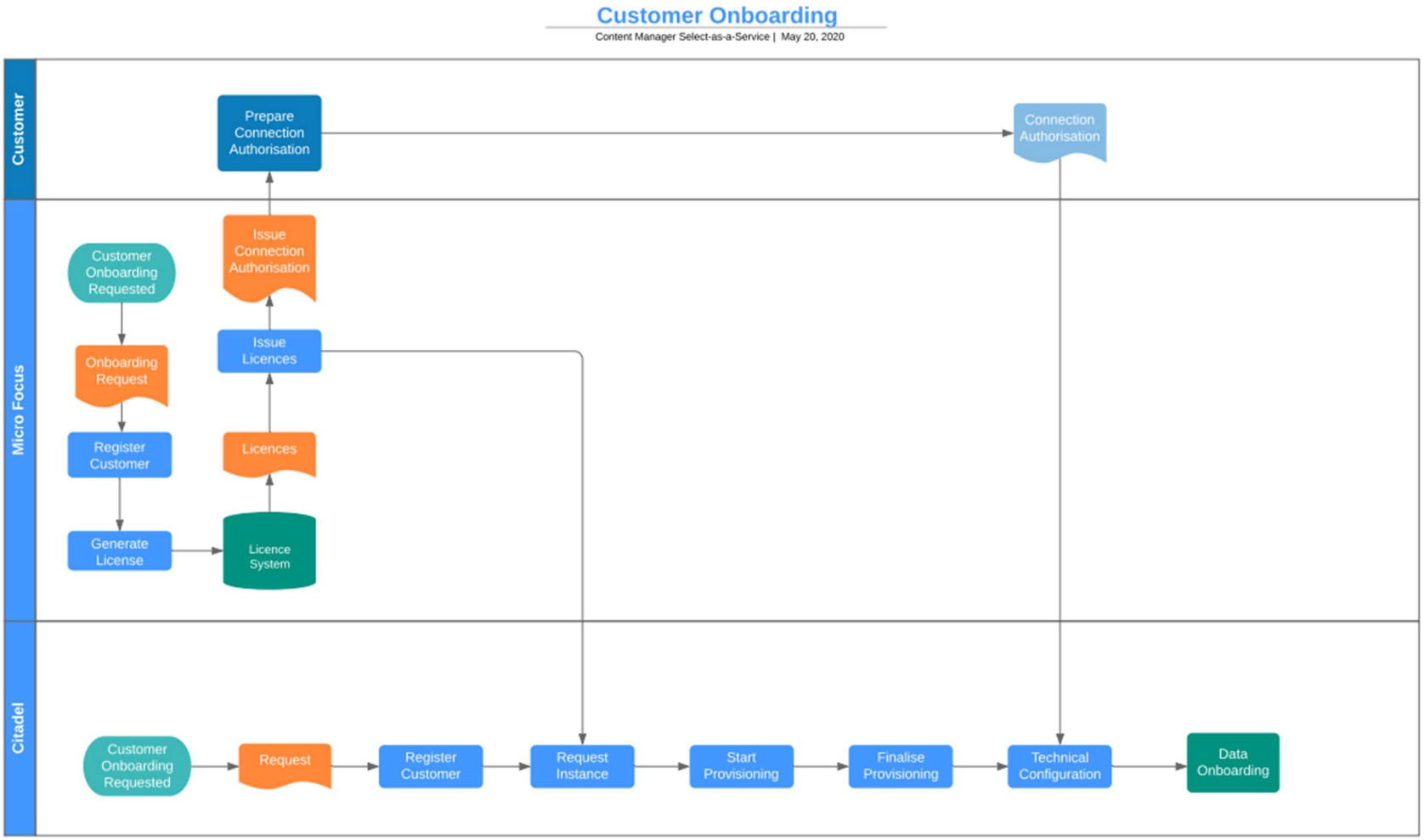


Figure 6 CMSaaS Customer Onboarding Workflow Overview

CMSaaS Customer Data Onboarding

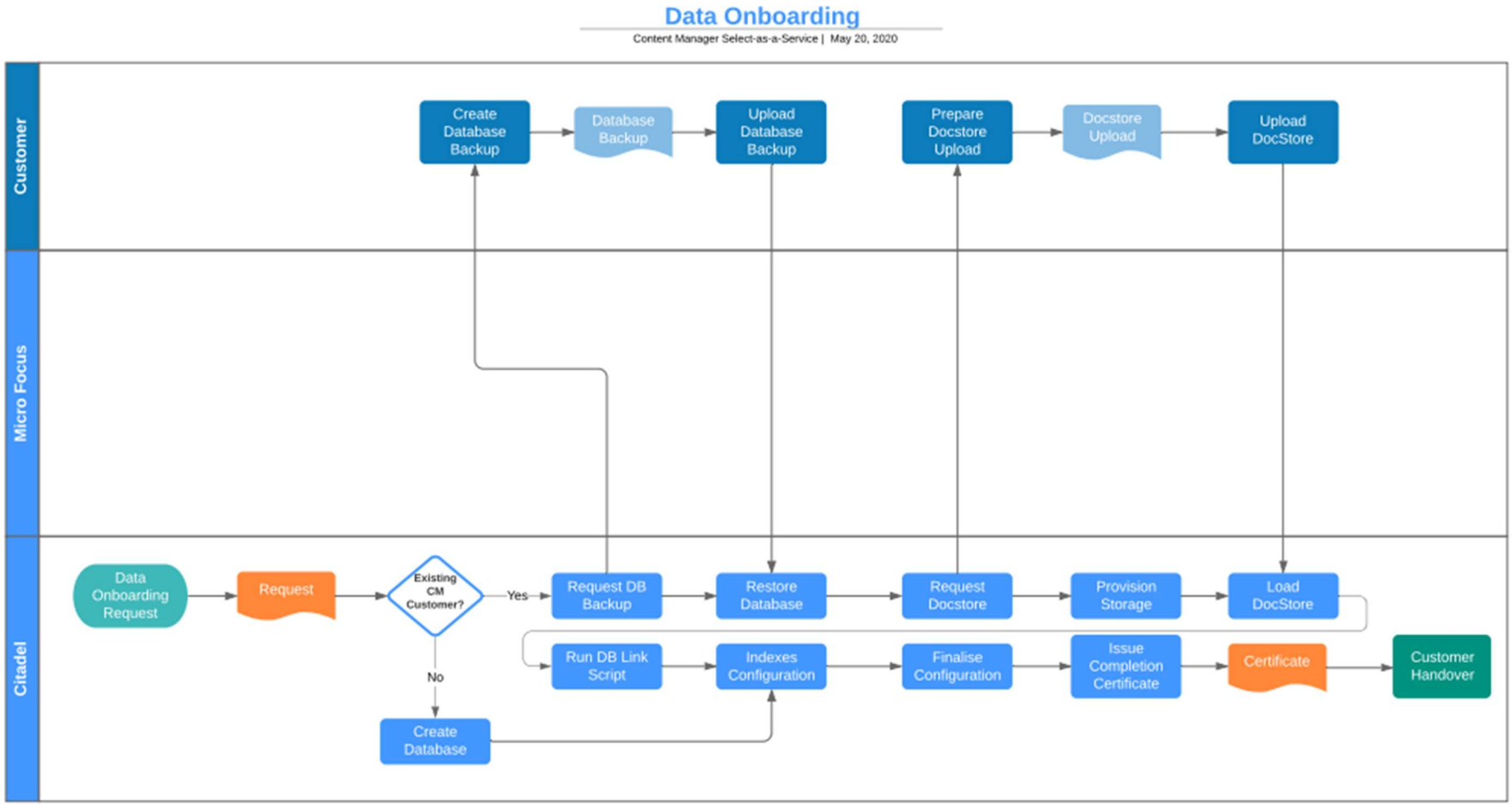
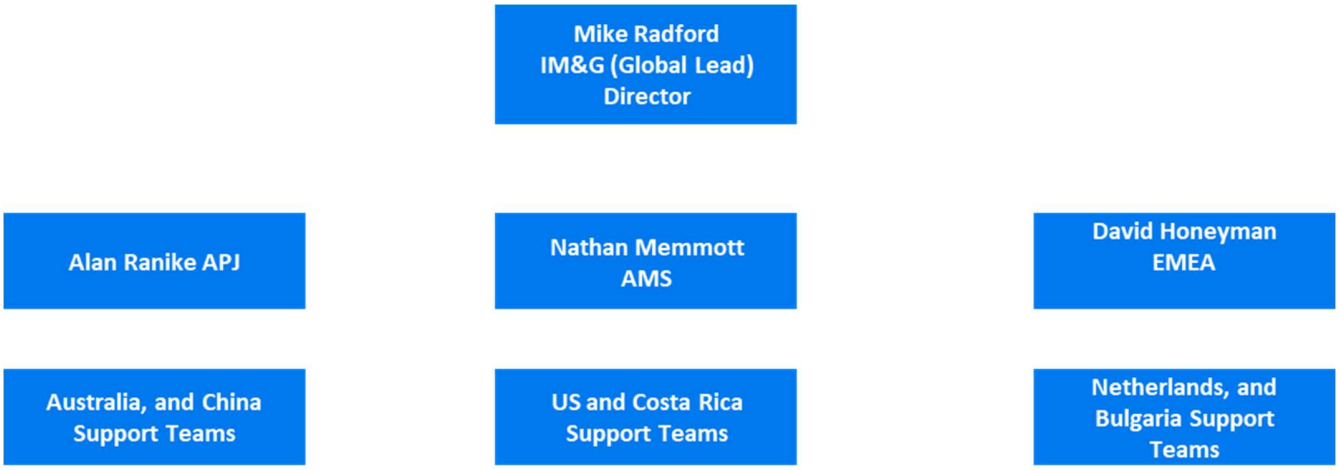


Figure 7 CMSaaS Customer Data Onboarding

Support Operating Models

CMSaaS Support Organization



Citadel CMSaaS Support Organization

The diagram illustrates the Citadel CMSaaS Support Organization that will deliver the day-to-day operational support to the CMSaaS offering.

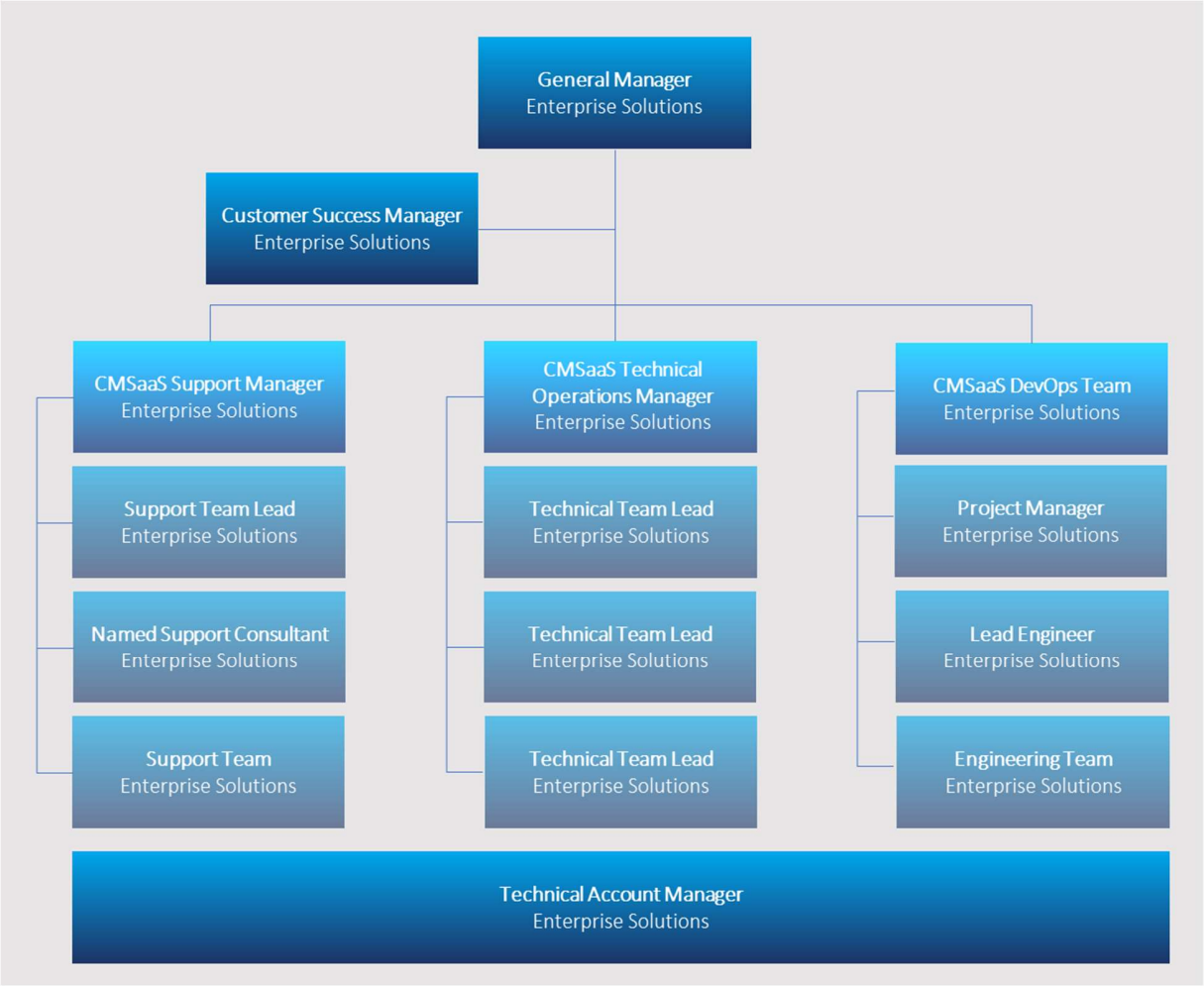
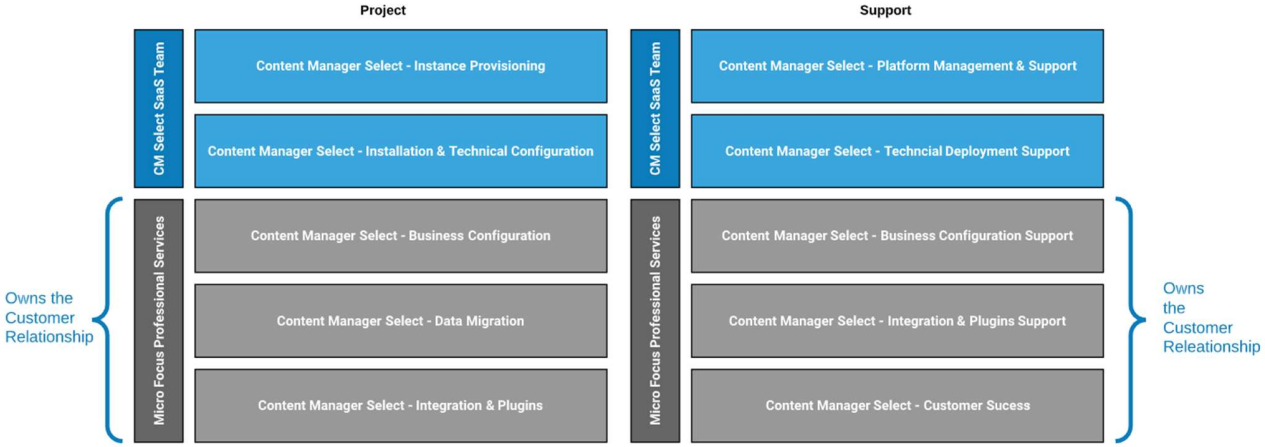


Figure 8 Citadel CMSaaS Support Organization Structure

Direct Professional Service / Partner Delivery Model



Stage	Task	MF PS / Partner Team	CMSaaS Platform Service Team
CMSaaS – Review, Planning and Design / SaaS Pathways Consulting	Undertake all readiness activities in preparing the customer and data to be migrated to CMSaaS	Responsible	Supporting
CMSaaS - Instance Provisioning	Provision of the base CMSaaS instance as per the approved Order (Automated)		Responsible
CMSaaS - Installation and Technical Provisioning	Content Manager installation encompassing all components including Web Client, Thick Client, Service API (Semi-Automated)		Responsible
	CMSaaS Authentication Configuration. MF PS / Partner provides the Federation Metadata endpoint for the customers Identity Provider.	Supporting	Responsible
	Base Database Configuration. For existing CM customers, MF PS / Partner will upload the DB backup to CMSaaS to be restored by the CMSaaS Platform Team		Responsible
	Document Store Creation		Responsible
	Document Store Upload	Responsible	Supporting
	Enterprise Studio Setup License CM Instance Configure ADFS within Enterprise Studio Setup Event Processing Setup Workgroup Server (https with Certificate)		Responsible

Direct Support Model

The following diagram illustrates at a high-level (to be replaced once full RACI has been developed) the Core responsibility of each team within the joint CMSaaS Support Organization.

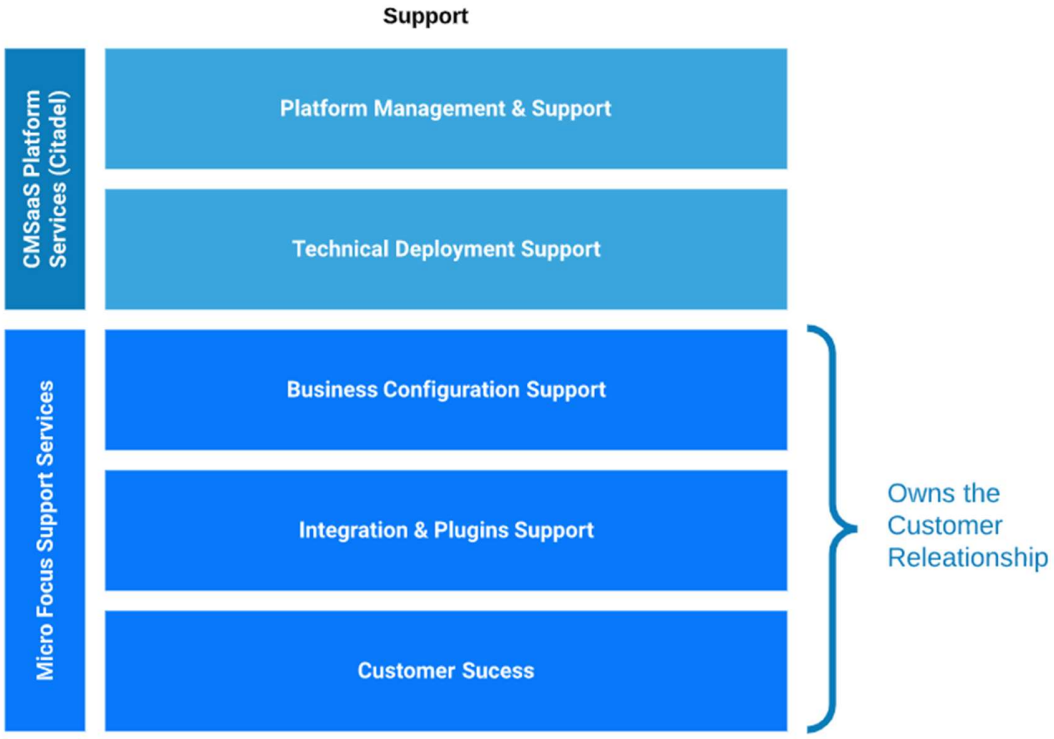


Figure 9 CMSaaS RACI Overview

The following diagram illustrates the support model for the CMSaaS product where the customer has purchased the CMSaaS directly through Micro Focus and Micro Focus is providing direct support.

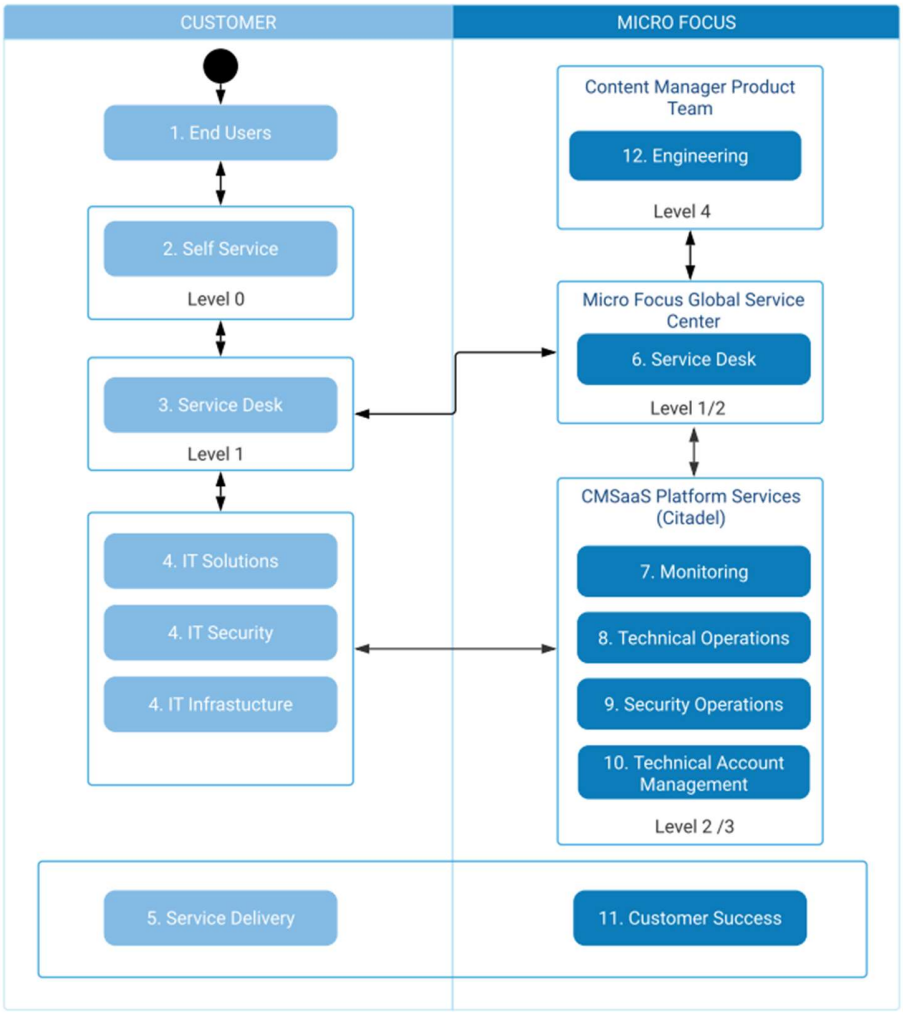


Figure 10 High Level Micro Focus Direct Support Model

The following table outlines the support levels and responsibilities from the Customer, Micro Focus and Citadel referencing the diagram above:

Ref	Role	Support Level	Responsible Organization	Responsibilities
1	End User	Level 0	Customer	Customer end users of Content Manager

Ref	Role	Support Level	Responsible Organization	Responsibilities
2	Self Service	Level 0	Customer	Customer maintained Content Manager knowledge base for Level 0 Self Service Support
3	Service Desk	Level 1	Customer	Provides Level 1 Support to all Customer entities for Content Manager
4	ICT	Level 2	Customer	Provides support for Customer-controlled support systems and services delivered by the Customer e.g., network, desktop etc.
5	Service Delivery	Escalation	Customer	Responsible for managing the service delivery of the services for the Customer.
6	Service Desk	Level 2	Micro Focus	Provides Level 2 support for CMSaaS, experts in the Content Manager implementation, responsible for the management of the incident though to resolution. Coordinates support activities with all parties.
7	Monitoring	Event Management	Citadel	CMSaaS automated system fault identification, notification, and rectification
8	Technical Operations	Level 2/3	Citadel	Responsible for operation support and maintenance (patching, backups etc.,) of the CMSaaS environment including Level 3 cloud infrastructure support
9	Security Operations	Level 2/3	Citadel	Responsible for the proactive and reactive security management of the system including Information Security Compliance Management
10	Technical Account Management	TAM	Citadel	Responsible for helping customers and Micro Focus to build relationships and help them achieve their technical goals including assistance with overcome technical challenges.

Ref	Role	Support Level	Responsible Organization	Responsibilities
11	Customer Success	Escalation	Citadel	Responsible for managing the CMSaaS service delivery to the Micro Focus and the Customer
12	Engineering Services	Level 3/4	Micro Focus (Application) and Citadel (Platform)	Responsible for the development of bug fixes and new features in CMSaaS.

Partner-Led Direct Support Model

The following diagram illustrates the applicable support models for the CMSaaS offering where a Micro Focus Partner is owning the direct customer relationship with the Customer.

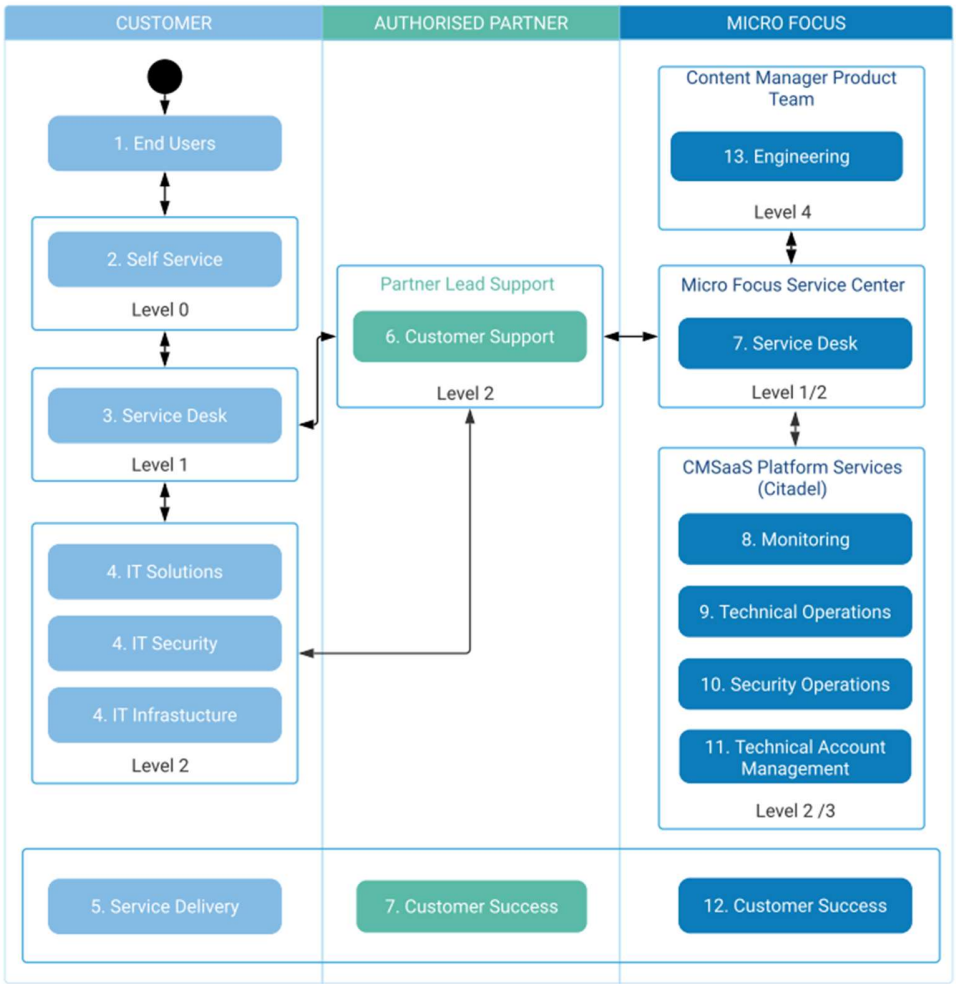


Figure 11 High Level Partner-Led Support Model

The following table outlines the support levels and responsibilities from the Customer, Authorised Partner, Micro Focus and Citadel referencing the diagram above:

Ref	Role	Support Level	Responsible Organization	Responsibilities
1	End User	Level 0	Customer	Customer end users of Content Manager
2	Self Service	Level 0	Customer	Customer maintained Content Manager knowledge base for Level 0 Self Service Support
3	Service Desk	Level 1	Customer	Provides Level 1 Support to all Customer entities for Content Manager
4	ICT	Level 2	Customer	Provides support for Customer-controlled support systems and services delivered by the Customer e.g., network, desktop etc.
5	Service Delivery	Escalation	Customer	Responsible for managing the service delivery of the services for the Customer.
6	Customer Support	Level 2	Authorized Partner	Provides Level 2 support for CMSaaS, experts in the Content Manager implementation, responsible for the management of the incident though to resolution. Coordinates support activities with all parties.
7	Service Desk	Level 2	Micro Focus	Provides Level 2 support for CMSaaS, experts in the Content Manager product, responsible management of the incident though to resolution within Micro Focus. Coordinates support activities with all internal parties.
8	Monitoring	Event Management	Citadel	CMSaaS automated system fault identification, notification, and rectification

Ref	Role	Support Level	Responsible Organization	Responsibilities
9	Technical Operations	Level 2/3	Citadel	Responsible for operation support and maintenance (patching, backups etc.) of the CMSaaS environment including Level 3 cloud infrastructure support
10	Security Operations	Level 2/3	Citadel	Responsible for the proactive and reactive security management of the system including Information Security Compliance Management
11	Technical Account Management	TAM	Citadel	Responsible for helping customers, Authorised Partners, and Micro Focus to build relationships and help them achieve their technical goals including assistance with overcome technical challenges
12	Customer Success	Escalation	Citadel	Responsible for managing the CMSaaS service delivery to the Authorised Partner, Micro Focus and the Customer
13	Engineering Services	Level 3/4	Micro Focus (Application) and Citadel (Platform)	Responsible for the development of bug fixes and new features in CMSaaS.

Citadel Support Services

Citadel Service Management

It is important that the management of availability, performance and service levels considers the overall environment (including application, infrastructure, and network). Whilst Citadel does not have direct control over some of these elements (e.g., Network Connectivity to Content Manager Select as a Service, this is the responsibility of the Customer), Citadel maintains a holistic view of the application and are proactive in identifying issues and engaging with the relevant parties to ensure that all information is available to assist in resolving issues.

Citadel's Customer Success Framework aims to contribute to the solid governance practices of the Customer. It integrates ongoing account and relationship management to include the relationship between the Customer, Micro Focus and Citadel.

Citadel Included Services

The following services are provided in the delivery of CMSaaS.

Service	Description
Service Desk	• Support Enquiries • Incident Management • Problem Management • Request Fulfilment • Change Management • Event Management • Fault Rectification
IT Operations	• Asset/Records Management • License Management • Vendor and 3rd Party Escalation
Service Management	• Service Breach Escalation • Service Delivery Management • Continual Service Improvement • Monthly Service Reporting • Quarterly Contract Performance Review
Micro Focus Content Manager Support*	• Level 2 and 3 Content Manager Product Support • Management of Micro Focus vendor support escalations • Optional where neither Micro Focus or Authorized Partner is providing premium level support
Application Management	• Configuration Management • Release and Deployment Management • Change Management • Asset Management • Audit and Event Monitoring
Security Management	• Logical and physical firewall devices • Configuration settings within cloud platform • Management of Multi-factor user authentication services • Central monitoring and recording of logs, configuration and policies changes for all infrastructure and security devices • Security Service / Device management and support (including health and availability management, performance, and capacity management) • Perform firewall changes (access lists, remote access, VPN management) • Software and firmware updates • Patch management • Vendor and 3rd Party Escalation
Server Management	• Managing all elements required for delivery of a Virtual Server environment

Service	Description
	• System Monitoring of availability and server elements such as CPU / memory / disk and network subsystems • System Support services (workability / functionality support) • System Management (including health and availability management, performance, and capacity management) • Configuration changes (including performance enhancements, user account management) • Operating System Support • System Backups/Restores to agreed Service Levels • Patch management for operating system and application software • Vendor and 3rd Party Escalation • Anti-Virus software management including anti-Virus signature updates
Storage Management	• Monitoring of all storage sub-system elements such as availability, capacity, performance • Support of storage systems (physical / virtual – workability / functionality support) • Management of storage systems (health and availability, capacity, etc.) • Configuration changes (including performance enhancements, security configuration, tier changes) • Patch management • Management of storage to support backup / restorations within agreed Service Levels • Vendor and 3rd Party Escalation
Database Management	• Backup and Restore of Database and Transaction Logs • Critical and Security Database patch / updates • Monitoring of indexes health • Management of Database clusters • Monitoring of backup jobs • Monitoring Database availability / Performance / State / Locking / Blocking / expensive transactions • Database – Lock Requests per deadlock • Capacity planning - Database/Log file used size/percentage • Operating System Service status monitoring for database related services • Add, Move, Changes to security permissions of users / groups / roles • Data File, Storage Container, Tablespace and Object Management • Patch management • Ad-hoc Database auditing
Network Management (Within CMSaaS Platform)	• Device monitoring of availability and networking elements such as bandwidth utilisation, latency, packet loss, traffic flow, etc. • Device support for both remote and on-site • Device Management (including health and availability management, performance, and capacity management, etc.)

Service	Description
	• Configuration changes (e.g., routing, switch port configuration, VLAN configuration, performance changes and access account management) • System Backups/Restores • Device operating system Software Updates (if applicable) • Patch management • Vendor and 3rd Party Escalation
Disaster Recovery	• Monitoring and management of DR systems (i.e., file and database replication services and infrastructure) • Periodic DR/Fail-over testing • DR fail-over reporting • Implementation and compliance with agreed disaster recovery plan • Provide as requested information required to complete audit, compliance, or regulatory audit reporting · Work with independent companies at request to perform external firewall testing and vulnerability assessments

Citadel Key Contacts

Support Type	Times
Service Desk (Accessible 24 x 7)	Web portal: via MF Email: support@citadelgroup.com.au Phone: +61 1800 314 498 Location: Melbourne AU, Canberra AU & Brisbane AU
Service Desk Team Leader (First Level Support and contactable)	Name: Paul Mondin Email: TBApaul.mondin@citadelgroup.com.au Phone: +61 1800 314 498 Location: Melbourne AU
Customer Success Manager (Escalations, for General Support issues and matters – during business and support hours)	Name: TBA Email: TBA Phone: +61 1800 314 498 Location: Brisbane AU
Technical Operations Manager (Escalation, for Technical Infrastructure issues and matters)	Name: Jakub Zverina Email: Jakub.Zverina@citadelgroup.com.au Phone: +61 1800 314 498 Cell: +61 490 177 176 Location: Canberra AU

Support Type	Times
Security Operations Manager (Escalation, for Information Security issues and matters)	Name: Sean Lengyel Email: SOC@citadelgroup.com.au Phone: +61 1800 314 498 Cell: +61 411 115 342 Location: Canberra AU
General Manager Enterprise Solutions (Service Owner) (Escalation, for Overall Service or Contact issues)	Name: Ryan Harris Email: Ryan.Harris@citadelgroup.com.au.au Phone: During agreed service hours: +61 1800 314 498 Location: Brisbane AU
Technical Account and Partner Manager (Partner Success)	Name: Kurt Wieprecht Email: kurt.weiprecht@citadelgroup.com.au Phone: +61 1800 314 498 Cell: +61 434532667 Location: Brisbane AU

Citadel General Team Contact Information

Requests for support can be logged with the CMSaaS Service Desk in the following ways:

Team	Contact Methods
CMSaaS Platform Operation Team	Phone: +61 1800 314 498
CMSaaS Security Operations Team	Phone: +61 1800 314 498
Enterprise Solutions Management Team	Phone: +61 1800 314 498

Citadel Standard Support Services

Support Hours	Service Window
Global	24 x 7, 365 days a year

Citadel Management Escalation Contacts

Team	Contact Methods
CMSaaS Platform Operation Team	Phone: +61 1800 260 333
CMSaaS Security Operations Team	Phone: +61 1800 260 333
Enterprise Solutions Management Team	Phone: +61 1800 260 333

Support Request Prioritization

Support request prioritization is based on Impact and Urgency. The following tables describes the priority matrix:

Business Impact	Urgency		
	Low	**Medium**	**High**
High	Priority 3	Priority 2	Priority 1
Medium	Priority 4	Priority 3	Priority 2
Low	Priority 5	Priority 4	Priority 3

Support Requests are classified by determining the Business Impact and Urgency**.** **Business Urgency** is the time that the Customer / user feel is reasonable to be without normal operation:

Business Urgency	Definition
High	• The damage caused by the Incident increases rapidly • Work that cannot be completed by user is highly time sensitive • A minor Incident can be prevented from becoming a major Incident by acting immediately - Several users with VIP status are affected
Medium	• The damage caused by the Incident increases considerably over time - A single user with VIP status is affected
Low	• The damage caused by the Incident only marginally increases over time - Work that cannot be completed by staff is not time sensitive

Business Impact is the effect that the incident has on the Normal Operation of the Business.

Business Impact	Definition
High	• Greater than 75% of total user bases is affected and/or not able to do their job • 75% of total users are affected and/or acutely disadvantaged in some way • The financial impact of the Incident is likely to exceed $10,000 • The damage to the reputation of the business is likely to be high • Someone has been injured
Medium	• Greater than 25% of total users are affected and/or not able to do their job properly • A moderate number of customers are affected and/or inconvenienced in some way • The financial impact of the Incident is likely to exceed $1,000 but will not be more than $10,000 • The damage to the reputation of the business is likely to be moderate
Low	• Less than 25% of total users are affected and/or able to deliver an acceptable service, but this requires extra effort • Less than 25% of total users are affected and/or inconvenienced but not in a significant way • The financial impact of the Incident is likely to be less than $1,000. • The damage to the reputation of the business is likely to be minimal

Stated Service Level Objectives

The following SLOs from part of the standard offering for CMSaaS.

Stated Service Level Objectives (SLO)	
SLO Type	• SLO
Provisioning	• Instance provisioned within 10 Business Days from receiving approved SOW
Support	• As per Micro Focus Business & Premium Support Packages
Availability	• 99.9%
Data Recovery	• Production Instance (Gold Edition): RPO < 15 minutes. • Production Instance (Platinum Edition): RTO <4 hours | RPO < 15 minute • Production Instance (Titanium Edition): RTO < 15 minutes | RPO < 1 minute

Internal Service Level Objectives

The following Service Level Objectives are Citadel's commitment to delivering services to Micro Focus in support of the CMSaaS offering.

The Internal SLOs have been set intentionally higher than Micro Focus's standard SaaS and Business / Premium Support offerings to ensure back-to-back SLO's can be achieved between the organizations while preserving the SLO to the Customer.

Service Incident SLO

The following table describes the applicable Response service objectives for Service Incidents:

Service Incident Acknowledgement and Response Service Level Objectives					
Priority	**Acknowledge Target (Automatic)**	**Initial Response**	**Initial Response After Hours**	**Update Frequency**	**Measurement Hours**
Priority 1	Within 5 Minutes	Within 15 minutes	Within 15 minutes	30 Minutes	24 X 7
Priority 2	Within 5 Minutes	Within 30 Minutes	Within 30 minutes	60 Minutes	24 X 7
Priority 3	Within 5 Minutes	Within 8 Business Hours	N/A	1 Business Day	Business Hours
Priority 4	Within 5 Minutes	Within 16 Business Hours	N/A	1 Business Day	Business Hours

The following table describes the applicable Resolution services objectives for Service Incidents:

Service Incident Resolution Service Objectives			
Priority	**Resolution Target**	**Update Frequency**	**Measurement Hours**
Priority 1	Restore within 2 Hour	30 Minutes	24 X 7
Priority 2	Restore within 8 hours	60 Minutes	24 x 7
Priority 3	Restore within 24 Hours	8 Hours	Business Hours
Priority 4	Resolution within 40 hours	N/A	Business Hours

For all Major Incidents (Priority 1 or 2), a full incident report will be provided to Micro Focus within 5 business days covering all of the details of the event, steps taken to resolve and post incident review.

Security Incident SLO

The CMSaaS Platform is certified ISO/IEC 27001:2013 – Information Security Management compliant. The following table provide the service objectives with regards to Security Incidents:

Security Incident Classification			
Classification	**Type of Incident**	**Definition**	**Example**
Major (Red)	Security violation	A deliberate, negligent, or reckless action that leads to the loss, damage, corruption, or disclosure of official information	1. Actual or suspected malicious activity such as unauthorised access to official or classified information 2. Significant breach of ICT system 3. Data leak
Minor (Yellow)	Security breach / infringement	An accidental or unintentional failure to observe Service Providers or Customer's ICT security policies and procedures, failure to adhere to security awareness training.	1. Clicking on a malicious link 2. Opening a malicious attachment 3. Data spill

The following table describes the applicable Response services objectives for Security Incidents:

Security Incident Acknowledgement and Response Service objectives					
Priority	**Acknowledge Target (Automatic)**	**Initial Response**	**Initial Response After Hours**	**Update Frequency**	**Measurement Hours**
Major (Red)	Within 5 Minutes	Within 15 minutes	Within 15 minutes	30 Minutes	24 X 7
Minor (Yellow)	Within 5 Minutes	Within 8 Business Hours	N/A	1 Business Day	Business Hours

The following table describes the applicable Resolution services levels for Security Incidents:

Service Incident Resolution Service Levels			
Priority	**Resolution Target**	**Update Frequency**	**Measurement Hours**
Major (Red)	Restore within 2 Hour	30 Minutes	24 X 7
Minor (Yellow)	Restore within 24 Hours	8 Hours	Business Hours

For all Major (Red) Incidents, a full incident report will be provided to the customer with 5 business days covering all of the details of the event, steps taken to resolve and post incident review.

Request Fulfilment SLO

The following table describes the applicable Response services levels for Service Requests:

Request Fulfilment Acknowledgement and Response Service Levels				
Priority	**Acknowledge Target (Automatic)**	**Initial Response**	**Update Frequency**	**Measurement Hours**
Priority 1	Within 5 Minutes	Within 2 Business Hours	Not Applicable	Business Hours
Priority 2	Within 5 Minutes	Within 4 Business Hours	Not Applicable	Business Hours
Priority 3	Within 5 Minutes	Within 8 Business Hours	Not Applicable	Business Hours

Priority 4	Within 5 Minutes	Within 16 Business Hours	Not Applicable	Business Hours
Priority 5	Within 5 Minutes	Within 5 Business Days	Not Applicable	Business Hours

The following table describes the applicable Resolution services levels for Service Requests:

Request Fulfilment Resolution Service Levels			
Priority	**Resolution**	**Update Frequency**	**Measurement Hours**
Priority 1	Within 4 Business Hours	Not Applicable	Business Hours
Priority 2	Within 8 Business Hours	Not Applicable	Business Hours
Priority 3	Within 16 Business Hours	Not Applicable	Business Hours
Priority 4	Within 32 Business Hours	Not Applicable	Business Hours
Priority 5	Within 10 Business Days	Not Applicable	Business Hours

Service Target Definitions and KPIs

The following Service Level Definitions and Reporting Frequencies apply to the Content Manager Select as a Service:

Service Objective	**KPI**	**Calculation**	**Reporting Frequency**
Service Incident – Acknowledgement and Response	Priority 1 - 99% of Incidents serviced according to the Service Targets Priority 2 - 98% of Incidents serviced according to the Service Targets Priority 3 - 98% of Incidents serviced	• Incident Response Rate = (1 - (A + B) / (2 * C)) * 100 • Where: • A is the number of Acknowledgements that occurred after 5 minutes or not at all during the Period. • B is the number of Initial Responses that occurred after the target time during the period. • C is the number of Incidents over the period. • Acknowledgement is the time the communication of the Incident was acknowledged by the Service Provider from the time the	Monthly

Service Objective	KPI	Calculation	Reporting Frequency
	according to the Service Targets Priority 4 - 95% of Incidents serviced according to the Service Targets	Customer communicates the Incident, or the service provider identified the Incident. • The Initial Response is the time at which the Service Provider has assigned a technician and has advised the intended remedial action to the Customer, measured from the time of Acknowledgement.	
Service Incident – Resolution	100% of Service Incidents serviced according to the Service Targets	• Incident Resolution Rate = (1 - (A - C) / (B - C)) * 100 • Where: • A is the number of incidents that were not resolved within the target time during the Period • B is the number of Incidents over the period • C is Excusable Incidents. Excusable Incidents is the number of Incidents attributable to Vendor Services or Network Services etc., not under Citadel management • The resolution time is measured from the time of incident Acknowledgement (or the time incident Acknowledgement should have occurred) to the time the incident is resolved.	Monthly
Security Incident – Acknowledgement Response	Red Severity - 100% of Service Incidents serviced according to the Service Targets Yellow Severity - 100% of Service Incidents serviced according to the Service Targets	• Security Incident Response Rate = (1 - (A + B)/(2 * C)) * 100 • Where: • A is the number of Acknowledgements that occurred after 5 minutes or not at all during the Period. • B is the number of Initial Responses that occurred after the target time during the period. • C is the number of Service Incidents over the period. • Acknowledgement is the time the communication of the Security Incident was acknowledged (perhaps automatically) by the	Monthly

Service Objective	KPI	Calculation	Reporting Frequency
		service provider from the time the Customer communicates the service Incident, or the Service Provider identified the Service Incident. • The Initial Response is the time at which the Service Provider has assigned a technician and has advised the intended remedial action to the Customer, measured from the time of Acknowledgement.	
Service Request Fulfilment – Response	100% of Service Requests serviced according to the Service Target	• Service Request Response Rate = (1 - A / B) * 100 • Where: • A is the number of Initial Responses that occurred after 4 hours or not at all during the Period. • B is the number of Service Requests during the Period. • The Initial Response is the time at which the Services Provider has acknowledged the Service Request and has advised the intended course of action and estimated completion timeframe to the Customer, measured from the time the Customer communicated the Service Request.	Monthly

Service Availability	99.95% Uptime	• Service Availability% = (1 - (B - C) / A) * 100
		• Where:
		• A is the Measurement hours over the period
		• B is the total of the periods (s) during which the Content Manager Select as a Service is not available
		• C is Excusable Downtime. Excusable Downtime is the totals of all periods(s) that the Content Manager Select as a Service is not available due to:
		  ○ Scheduled Downtime
		  ○ Downtime due to a failure of the Customer
			Monthly

Service Objective	KPI	Calculation	Reporting Frequency
		environment or component out of the Service Provider's control	

Instance Specifications

Instance Specifications			
SKU	**Vendor Product Code**	**Description**	**Product Specification**
TBC	CIX-SCM-C1	Content Manager Select Software as a Service Non-Production Instance	• Non-Production Instance Subscription - Content Manager • Up to 50GB Database + 50GB Document Store + 50GB Network Traffic • Optional DR and / or High Availability (additional charges apply) • Additional Storage Available (additional charges apply, refer Object Volume Packs)
TBC	CIX-SCM-C3	Content Manager Select Software as a Service - Gold Edition - Base User Pack (1000) + 300GB Database Pack Production Instance	• Support Services • Technical Account Manager (TAM) • 24 x 7 Platform Support, Maintenance and Monitoring • Disaster Recovery • Disaster Recovery and Geo-Replicated Data Protection Configuration • Recovery Point Objective (RPO) < 15 minutes • Recovery Time Objective (RTO) < 24 hours • Availability • High Availability • 99.9% Availability SLA • Max 1500 users per Tenancy • Security • IP Whitelisting • Single Sign-On and Federated Authentication Support • Active Cyber Security Management & Monitoring • ISO/IEC 27001:2013 Certified • Included Non-Production Instance • Non-Production Instance Subscription - Content Manager • Up to 50GB Database + 50GB Document Store + 50GB Network Traffic

Instance Specifications			
SKU	**Vendor Product Code**	**Description**	**Product Specification**
			• Optional DR and / or High Availability (additional charges apply). • Additional Storage Available (additional charges apply)
TBC	CIX-SCM-C5	Content Manager Select Software as a Service - Platinum Edition - Base User Pack (3000) + 300GB Database Pack Production Instance	• Support Services • Technical Account Manager (TAM) • 24 x 7 Platform Support, Maintenance & Monitoring • Disaster Recovery • Disaster Recovery & Geo-Replicated Data Protection Configuration • Recovery Point Objective (RPO) < 15 minutes • Recovery Time Objective (RTO) < 4 hours • Availability • High Availability • 99.95% Availability SLA • Security • IP Whitelisting • Single Sign-On and Federated Authentication Support • Active Cyber Security Management and Monitoring • ISO/SEC 27001:2013 Certified • Included Non-Production Instance • Non-Production Instance Subscription - Content Manager • Up to 50GB Database + 50GB Document Store + 50GB Network Traffic • Optional DR and / or High Availability (additional charges apply) • Additional Storage Available (additional charges apply)
TBC	CIX-SCM-C7	Content Manager Select Software as a Service - Titanium Edition - Base User Pack (3000) + 300GB Database Pack **Production Instance**	**Support Services** Technical Account Manager (TAM) 24 x 7 Platform Support, Maintenance & Monitoring **Disaster Recovery** Disaster Recovery and Geo-Replicated Data Protection Configuration Recovery Point Objective (RPO) < 1 minute Recovery Time Objective (RTO) < 15 minutes **Availability** High Availability 99.95% Availability SLA **Security** IP Whitelisting Single Sign-On and Federated Authentication Support Active Cyber Security Management & Monitoring

Instance Specifications			
SKU	**Vendor Product Code**	**Description**	**Product Specification**
			ISO/SEC 27001:2013 Certified **Included Non-Production Instance** Non-Production Instance Subscription - Content Manager Up to 50GB Database + 50GB Document Store + 50GB Network Traffic Optional DR and / or High Availability (additional charges apply) Additional Storage Available (additional charges apply)