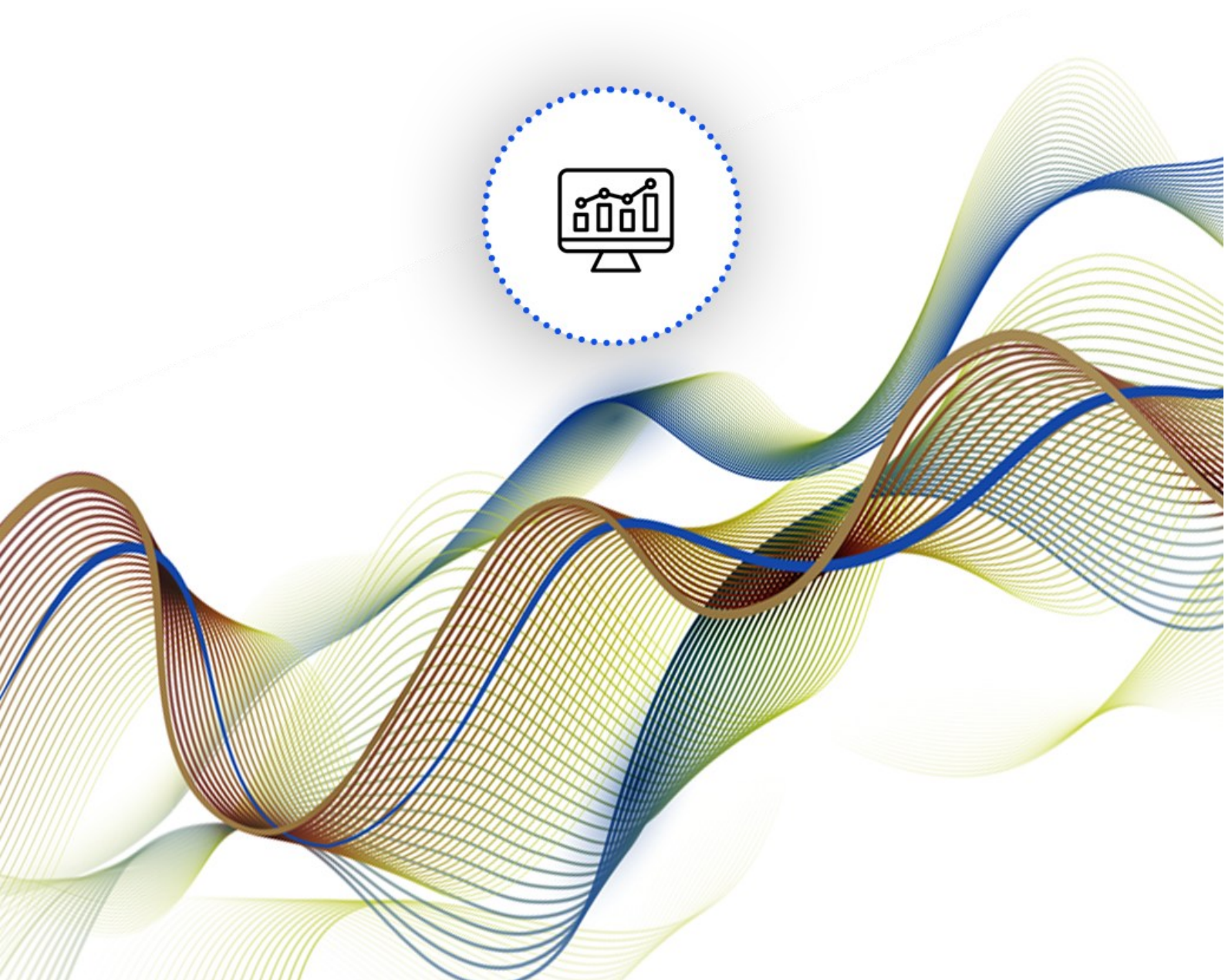


TCS Platform as a Service (PaaS) Services

G-Cloud 15: Lot 1a
Service Definition

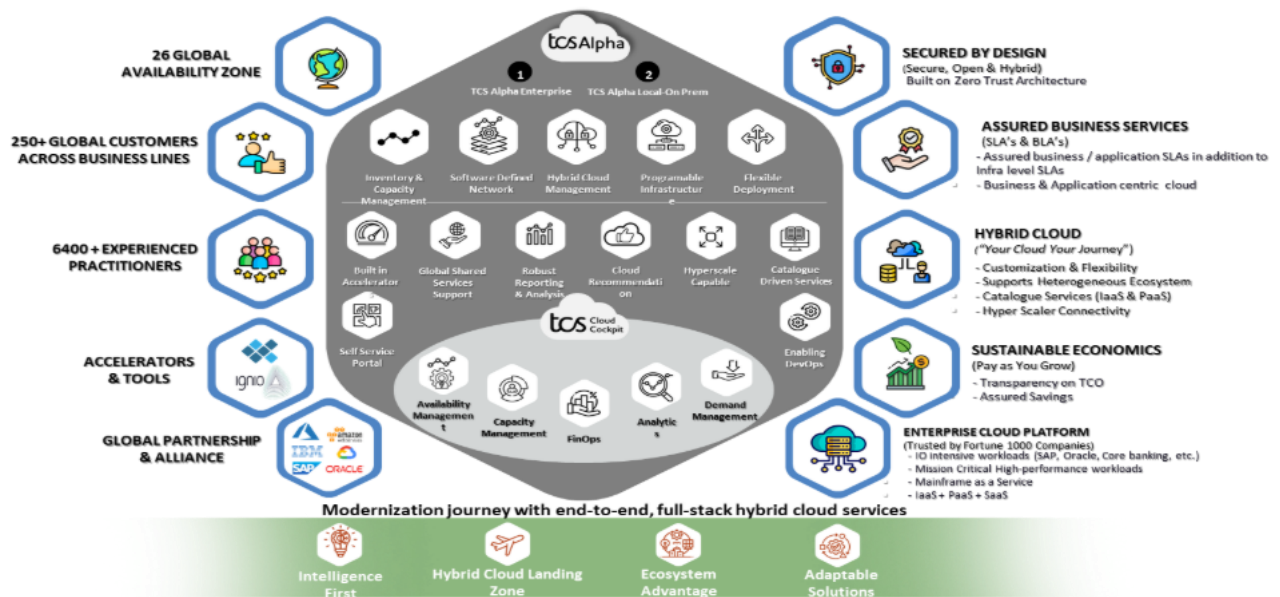


Contents

1. Service Description	3
1.1 Container as a Service (CaaS).....	4
1.2 Database-as-a-Service	5
1.3 Kafka as a Service.....	7
1.4 API As A Service.....	8
1.5 RabbitMQ Messaging Service.....	10
1.6 Workbench As a Service	12
2. Service Features	13
3. Service Benefits.....	14
4. Data Backup and Restoration Approach.....	14
5. Onboarding and Offboarding Support.....	16
6. Service Constraints.....	17
7. Roles and Responsibilities – R A C I	17
8. Service Levels	18
9. System Requirements.....	18
10. Outage and Maintenance Management.....	19
11. Hosting Options and Locations.....	20
12. Access to data (upon exit)	20
13. Security.....	21
14. Why TCS	22
15. Pricing.....	25
16. Terms and Conditions.....	25

1. Service Description

TCS' state-of-the-art Enterprise Cloud Platform (ECP) or SovereignSecure Cloud (SSC) are curated to support enterprise' cloud journey and the ongoing operations of hybrid cloud environments. TCS ECP or SSC is a reliable private cloud platform to run the mission-critical production environments, without compromising on High Performance with IO-intensive workloads. Our software-defined (SDx) capability enables automation, cloud service brokerage, and resilience at all levels. It is built on a zero-trust architecture using an open secure architecture-based backbone with extensive automation and tooling.



Our key value proposition is described below:

- **Hybrid cloud technology** is increasingly being recognised as a choice of cloud; this brings real value with the inherent flexibility. TCS ECP or SSC enables enterprises to run their production workload along with the legacy infrastructure in the private cloud and public cloud services through a hybrid platform thus, leveraging the best of both worlds.
- **Secure by design** built on Zero Trust Architecture with denial by default. TCS Enterprise or SovereignSecure Cloud strengthens enterprise resilience and innovation by helping drive synergy across IT, tapping into the power of ecosystems, and providing fit-for-purpose solutions.
- **Assured Business Services SLAs** enables the customer to concentrate on their core business and focus on innovation and offload IT management. Thereby reduce the overall Total Cost of Ownership (TCO) and maximise the Return on Investment (ROI).

- **Sustainable Business Economics** – ECP or SSC provides assured saving including the accountability and responsibility to transform and modernise to the next generation technologies. We custom curate flexible pricing models that provide transparency in costs over the deal term
- **Enterprise Grade Cloud** with business relevant and technology defined. Our Digital ready cloud platform enables hosting of mission critical workloads and is unlike Industry Cloud Providers who give mostly technology-centric offering but leave its consumption for the enterprises to determine their cloudification journeys.

TCS Enterprise Cloud or SovereignSecure Cloud Platform's Platform as a Service (PaaS) offering details multiple managed cloud services designed to support enterprise IT and DevOps needs, focusing on container management, databases, streaming platforms, APIs, data lakes, machine learning operations, workbenches, DevOps, visualisation, messaging, and serverless functions. Each service is described with its overview, key features, benefits, security aspects, service catalogue, scope of services, cluster configurations, and reasons to choose TCS.

1.1 Container as a Service (CaaS)

The Container as a Service (CaaS) Platform enables IT and DevOps professionals to more easily deploy, manage, and scale container-based applications and services, helping enterprises to reduce application delivery cycle times and improve their business agility. As part of the CaaS offering, TCS can provide end to end Container services starting from Consulting, Build, Migration and Managed services.



The CaaS offering is built on top of our TCS Enterprise Cloud or SovereignSecure Cloud Platform and provides flexibility to enterprises by supporting a multitude of Container distribution platforms as per the specific need of the customer. The key platforms that are supported include: Opensource Kubernetes and Docker, RedHat OpenShift.

Key Features:

- **Flexible Deployment Options** - Designed to support business-critical enterprise applications for increased agility and stability across Opensource or Enterprise Grade container orchestration platforms.

- **Optimised Clusters** - Choose from different distributions, instance types - memory-optimised, compute-optimised, or general-purpose, with clusters sized to meet enterprise needs
- **Fully Managed Cluster** - E2E Container platform (Master, Infrastructure, and Worker nodes) managed by TCS, backed by enterprise support
- **Integrated Container Registry** - Secure internal OpenShift registry integrated with each cluster and ready to use out-of-the-box
- **Logging, metrics, and monitoring** - Includes services for monitoring cluster events, tracking usage, and capacity planning.
- **DevOps Enabled** - Pre-built API/Web hooks for integration with DevOps tool chains
Easy provisioning and management with Automation

Benefits:

- **Enhanced Flexibility:** Make the most of enterprise investments in existing, on-premises software licenses while migrating to the cloud with our 'Bring Your Own License' (BYOL) solution.
- **Fully managed container platform:** A fully managed container platform to customers that accelerates speed and agility of their digital transformation and innovation initiatives with faster onboarding time
- **Improve developer productivity** with pre-built access to workspaces that include runtimes, plugins for languages, tools and integrate with CI/CD pipelines across multiple technologies
- **Modular applications:** Build applications that are easy to maintain and manage by leveraging the Auto scaling and Auto healing capabilities
- **Pre-built API/Web hooks** for integration with DevOps tool chains, and seamless management of the Kubernetes versions
- **Integrated security** with containers and built-in frameworks for authentication and authorisation
- Run applications with greater reliability, portability and predictability with the ability to seamlessly port applications across multiple different environments /systems and hardware platforms

1.2 Database-as-a-Service

TCS managed Database as a Service is a comprehensive solution that delivers a fully managed database platform, covering everything from hardware and software provision to continuous management and administration. The service includes database provisioning, setup in active-active or active-passive modes, user management, software updates, backup and restore, monitoring, and round-the-clock incident management. Additional features

include cluster expansion, infrastructure support, vendor coordination, usage reporting, resource chargeback, and compliance with service level agreements, enabling organisations to transition to a more agile, centralised, and business-sensitive database environment



Key Features:

- **Multi-Layered Reference Architecture:** The DBaaS reference architecture is structured into three primary layers: IaaS, Database, and DBaaS Services. The IaaS layer includes virtual machines, networking, storage, and essential hardware for hosting databases.
- **Comprehensive Database Support:** The database layer supports various types of databases, including RDBMS and NoSQL options such as MSSQL, MySQL, MongoDB, Cassandra, and PostgreSQL.
- **Automated DBaaS Services:** The DBaaS service layer provides accelerators for standard services like database instance provisioning, version upgrades, and backup configurations. It also enables on-demand services such as clustering and high availability, supported by the TCS DBaaS team through a cloud management portal for automated technical assistance.
- **Integrated Monitoring Capabilities:** Database monitoring is managed through a dedicated compute and monitoring layer, utilising specialised tools to ensure effective oversight.
- **Enhanced Security:** Security is enforced through a dedicated layer, leveraging security options offered by each database vendor to protect data and operations.
- **Enterprise Integration:** An enterprise gateway connects the DBaaS to other enterprise components, enabling activities such as role-based access via enterprise-specific Active Directory, LDAP, and similar solutions.

Benefits:

- **Platform Flexibility:** Choose from a wide range of database distribution platforms to suit your enterprise needs.
- **Deployment Versatility:** Select either single or multi-data centre (DC) deployment options based on your specific requirements.
- **Fast Provisioning:** Quickly provision and create new databases, reducing costs and accelerating your time-to-market.
- **Reduced Ownership Costs:** Benefit from integrated basic support services that help lower the total cost of ownership.
- **Tailored Database Solutions:** Receive customised database solutions designed to meet your unique business requirements.
- **Comprehensive Managed Services:** Take advantage of end-to-end database management for streamlined operations.
- **Integrated Monitoring:** Monitor your database environment seamlessly with built-in monitoring capabilities.
- **Customisable SLAs:** Benefit from business Service Level Agreements (SLAs) tailored to your organisational needs.

1.3 Kafka as a Service

TCS' Kafka as a Service delivers a fully managed, scalable, and secure real-time streaming platform that empowers IT teams to build high-performance data pipelines and applications. By integrating messaging, storage, and stream processing, the service facilitates seamless analysis of both historic and real-time data. Key features include end-to-end Kafka cluster deployment and configuration for distributed environments, expert Zookeeper management, implementation of the Kafdrop UI, robust monitoring and administration, effortless cluster expansion, comprehensive platform and infrastructure support, frequent software and security updates, and coordinated vendor support where required. With these capabilities, TCS enables organisations to innovate and extract insights from their data, while experienced professionals handle the complexity of managing the platform.

Key Features:

- **Fully Managed Kafka Platform:** End-to-end management of Kafka clusters including provisioning, configuration, scaling, patching, and version upgrades, ensuring stable and reliable streaming operations.
- **High Availability and Resilience:** Built-in fault tolerance through multi-broker deployment, data replication, and automated failover to maintain continuous availability of streaming services.

- **Elastic Scalability and Performance Optimisation:** Dynamic scaling of brokers, partitions, and throughput to handle varying event volumes while maintaining low latency and predictable performance.
- **Enterprise-Grade Security and Access Control:** Authentication, authorisation, encryption, and role-based access control to secure data streams and align with organisational security policies.
- **Centralised Monitoring and Operational Visibility:** Comprehensive observability with monitoring of broker health, consumer lag, throughput, and alerts, enabling proactive operations and SLA adherence.

Benefits:

- **Kafka Management:** Configuring the Kafka cluster environment to enable development activities for the IT team.
- **Message-Based Integration:** Leveraging Kafka's capabilities to integrate diverse applications through publish-subscribe, queuing, and streaming models.
- **API Integration:** Offering four standardised Kafka APIs—Producer API, Consumer API, Streams API, and Connector API—for seamless connectivity.
- **Scalability:** Kafka's partitioned log architecture enables efficient data distribution across multiple servers, providing scalability far beyond single-server limitations.
- **Performance:** By decoupling data streams, Kafka ensures exceptionally low latency and high throughput.
- **Data Durability:** Data partitions are distributed and replicated across several servers, with all information stored on disk, ensuring resilience and durability even in case of server failures.
- **Integrated Security:** Utilises Kafka's built-in authentication and authorisation feature to safeguard access and maintain compliance.
- **Cost Efficiency:** Kafka's open-source nature minimises licensing expenses.
- **No Vendor Lock-In:** Organisations maintain flexibility and independence from proprietary solutions.

1.4 API As A Service

The TCS Managed API as a Service Platform delivers a comprehensive and integrated solution for managing the full lifecycle of APIs, leveraging the reliability of the open-source KONG gateway and the scalability of the TCS Enterprise Cloud or SovereignSecure Cloud Platform. The platform provides robust capabilities including user and role management, policy definition, and API governance, which collectively ensure that only authorised users can access and modify API resources. Essential configuration options such as rate limiting and advanced threat protection help safeguard applications against common vulnerabilities, including DDoS attacks and SQL injection, while also mitigating risks from API abuse. A

diverse range of authentication and authorisation mechanisms such as OAuth, JWT, API Keys, and SAML enable flexible access control tailored to organisational requirements. The solution further supports continuous monitoring to ensure ongoing performance and security, and provides streamlined processes for software, patch, and security updates to maintain system integrity. When needed, vendor coordination is available to facilitate seamless integration and support across third-party solutions. With these features, the platform empowers organisations to manage APIs securely, efficiently, and at scale within dynamic operating environments.

Key Features:

- **Controlled API Lifecycle Management:** APIs are established, changed, versioned, and retired using defined and documented procedures to ensure consistency, traceability, and controlled operation throughout the service lifecycle.
- **Centralised Interface and Traffic Control:** API access is mediated through a centralised gateway enforcing routing, throttling, rate limits, and availability controls to protect services and maintain agreed service levels.
- **Identity-Based Access and Security Enforcement:** Authentication, authorisation, encryption, and token management are applied to APIs based on least-privilege principles and organisational information security requirements.
- **Scalable and Resilient Service Architecture:** API services are deployed using resilient and scalable architectures designed to maintain availability and performance under varying demand and failure conditions.
- **Monitoring, Logging, and Governance Oversight:** API usage, performance, and security events are logged, monitored, and reviewed to support incident management, compliance reporting, and continual service improvement.
- **API User and Roles Management:** TCS enables secure and efficient management of user identities and roles across multiple platforms, ensuring streamlined onboarding, modification, and deprovisioning processes.
- **Software Security updates, patch management:** TCS ensures timely identification and resolution of security vulnerabilities through continuous assessment, risk-based patching, and compliance-driven updates. Our patch management process includes rigorous testing, packaging, and phased deployment to minimise business disruption while maintaining system integrity.

Benefits:

- **API Gateway Management:** Establishes the API Gateway platform, enabling the IT team to configure and orchestrate APIs effectively.
- **Security & Compliance:** Leverages the inherent security and compliance features of the API Gateway, ensuring data privacy, robust authentication and authorisation, and comprehensive threat protection.
- **Centralised API Management:** Focuses on enhanced traffic management through load balancing policies, policy enforcement for API governance, rate limiting, caching, and quota management across both internal and external APIs.
- **Scalability and Performance Optimisation:** Utilises the API Gateway's capabilities for elastic scaling, reduced latency, efficient caching, and data compression to improve overall system performance.
- **Observability and Monitoring:** Delivers centralised logging and analytics, with seamless integration to cloud monitoring tools such as Prometheus and Grafana

1.5 RabbitMQ Messaging Service

RabbitMQ as a Service (PaaS) provides a fully managed messaging platform that enables reliable, scalable, and decoupled communication between applications and systems. TCS delivers end-to-end ownership of the RabbitMQ platform, allowing IT teams to simplify application integration and event-driven communication without managing the underlying infrastructure or middleware components.

The service is built around a standard RabbitMQ messaging architecture, supporting producers, RabbitMQ core components, and consumers (workers). Producer applications publish messages to RabbitMQ exchanges, where routing logic directs messages to appropriate queues based on defined rules. Queues persist in messages reliably until they are consumed by worker applications, ensuring asynchronous processing, load levelling, and fault tolerance. TCS provisions and operates the RabbitMQ platform on secure cloud or private infrastructure, managing broker configuration, exchanges, queues, routing policies, and message persistence settings. The service supports flexible messaging patterns, reliable queues, and seamless scalability to handle varying message volumes and application workloads.

High availability and resilience are achieved through clustered RabbitMQ deployments, ensuring continuity of messaging services during node or infrastructure failures. The platform is continuously monitored for health, performance, queue depth, and throughput, with alerts and operational controls to maintain service stability. Security is embedded into the offering through controlled access to brokers, users, and virtual hosts, ensuring that only authorised producers and consumers can publish or consume messages. TCS also

manages platform lifecycle activities including upgrades, configuration changes, capacity planning, and integration with enterprise monitoring and ITSM processes.

Key Features:

- **Fully Managed RabbitMQ Platform :** End-to-end provisioning, configuration, upgrades, patching, and operational management of RabbitMQ brokers, removing infrastructure and platform management overhead from application teams.
- **Flexible Messaging and Routing Patterns:** Supports point-to-point, publish/subscribe, topic-based, and request-reply patterns using exchanges, queues, and bindings, enabling reliable and loosely coupled application integration.
- **High Availability and Scalability:** Clustered RabbitMQ deployments with queue mirroring and load balancing ensure resilience, fault tolerance, and scalable message processing as workload demand grows.
- **Enterprise Security and Access Control:** Implements authentication, role-based authorisation, secure communication, and tenant isolation to protect messaging infrastructure and data flows.
- **Monitoring, Alerting, and Operational Visibility:** Provides real-time monitoring of queue depth, throughput, consumer lag, and broker health with alerts and logs to support proactive operations and SLA compliance

Benefits:

- **Simplified Application Integration:** Enables seamless and reliable communication between distributed systems without tight coupling, improving system interoperability and flexibility.
- **Improved Reliability and Resilience:** Durable messaging, acknowledgements, retries, and fault-tolerant architecture ensure message delivery even during component or infrastructure failures.
- **Faster Time-to-Market:** Pre-built, managed messaging capabilities allow development teams to focus on application logic instead of messaging platform setup and maintenance.
- **Reduced Operational and Platform Risk:** Managed operations, standardised configurations, and proactive monitoring reduce the risk of outages, misconfigurations, and performance issues.
- **Scalable and Cost-Efficient Messaging:** Elastic scaling and shared platform services enable efficient handling of varying message volumes while optimising infrastructure and operational costs

1.6 Workbench As a Service

Workbench as a Service (PaaS) provides a secure, scalable, and fully managed JupyterLab-based development environment designed for data scientists and AI/ML developers. Delivered by TCS, the service enables users to develop, test, and visualise data models in a collaborative workspace hosted on cloud or on-premises infrastructure. It supports standardised environment provisioning, package and dependency management, notebook sharing, and seamless connectivity to enterprise data sources, enabling efficient end-to-end experimentation and model development workflows.

TCS manages the complete platform lifecycle including JupyterLab deployment and configuration, user and role management, authentication and authorisation, environment provisioning using containerised and Python package frameworks, and ongoing platform maintenance. The service also includes usage monitoring, resource management, access logging, software patching, and vendor coordination, ensuring a compliant, reliable, and governed AI development platform while allowing teams to focus on analytics and model innovation rather than infrastructure operations.

Key Features:

- **Managed JupyterLab Environment:** Fully managed JupyterLab deployment with configuration, upgrades, and platform maintenance handled centrally.
- **Standardised Environment Provisioning:** On-demand creation of isolated development environments using Docker and Python package management.
- **User, Role, and Access Management :** Role-based access control with authentication and authorisation aligned to enterprise security policies.
- **Notebook Collaboration and Sharing:** Secure notebook sharing with access logging to support collaborative development and traceability.
- **Integration with Enterprise Data Sources:** Seamless connectivity to data lakes, databases, and other data platforms for model development.
- **Usage Monitoring and Resource Management:** Monitoring of compute and resource consumption to ensure controlled usage and cost governance.

Platform Patching and Maintenance: Regular software updates, patching, and operational maintenance to keep the platform secure and stable

Benefits:

- **Ready-to-Use Development Environment:** Provides an instantly available JupyterLab workspace with no local installation required, enabling developers and data scientists to start coding and experimenting from any location.

- **Improved Collaboration and Productivity:** Enables shared notebooks and consistent environments across teams, reducing setup inconsistencies and improving collaboration between data science and engineering teams.
- **Optimised Resource Utilisation:** Supports controlled compute usage with monitoring and start/stop capabilities, helping optimise infrastructure consumption and reduce unnecessary costs.
- **Secure and Compliant Platform:** Delivers enterprise-grade security with authentication, role-based access control, network isolation, and audit trails to meet organisational and regulatory requirements.
- **Faster Model Development Lifecycle:** Streamlines experimentation, data exploration, and model development by integrating development tools, environments, and data access into a single managed platform.

2. Service Features

1. Managed Application Runtime Environment

Provides a fully managed platform to host, run, and operate applications without requiring buyers to manage servers, operating systems, or middleware components.

2. Standardised Development Frameworks

Supports commonly used programming languages, frameworks, and runtime versions to ensure consistency across development, testing, and production environments.

3. Integrated CI/CD Tooling

Enables automated build, test, and deployment pipelines using integrated tools to support repeatable and controlled application releases.

4. Elastic Scaling Capabilities

Allows applications and platform components to scale automatically or based on defined policies in response to workload demand.

5. Built-in Security Controls

Includes identity and access management, encryption at rest and in transit, secure configuration baselines, and audit logging.

6. Monitoring and Logging Services

Provides platform-level monitoring, log aggregation, and alerting to support service health, performance tracking, and incident response.

7. High Availability and Resilience

Supports deployment across multiple availability zones or regions to improve service continuity and reduce single points of failure.

8. Service Integration and APIs

Enables integration with other cloud services and third-party systems using standard APIs and messaging mechanisms.

3. Service Benefits

1. **Reduced Infrastructure Management Effort**
Eliminates the need for buyers to manage underlying infrastructure, allowing teams to focus on application functionality and outcomes.
2. **Faster Time to Market**
Accelerates application delivery by providing pre-configured environments and automated deployment processes.
3. **Improved Scalability and Performance**
Supports dynamic scaling to meet changing demand, helping maintain application performance during peak usage.
4. **Consistent Security and Compliance**
Applies standard security controls across environments, supporting compliance with organisational and regulatory requirements.
5. **Operational Stability and Reliability**
Improves service reliability through built-in resilience, monitoring, and managed platform operations.
6. **Cost Efficiency**
Reduces capital and operational costs by using shared platform services and consumption-based pricing models.
7. **Simplified Operations and Support**
Centralised monitoring, logging, and management reduce operational complexity and support overhead.
8. **Improved Integration and Interoperability**
Supports easier integration with cloud-native and external services, enabling modern, service-oriented architectures.

4. Data Backup and Restoration Approach

Data Backup and Restoration Approach TCS ECP or SSC provides a robust, multi-tiered backup and restoration framework designed to ensure business continuity and disaster recovery across enterprise workloads.

TCS Enterprise Cloud or SovereignSecure Cloud provides an enterprise-grade backup, restore, and disaster recovery framework designed to ensure data protection, service availability, and business continuity. The approach aligns with TCS governance, security, and compliance standards and is tailored to customer-defined business requirements.

Backup & Recovery Availability: Backup and recovery services are enabled by default on the TCS Enterprise Cloud or SovereignSecure Cloud platform and are managed through

standardised operational processes. Backup schedules, retention, and recovery options are aligned to customer business needs and agreed RPO/RTO objectives.

Backup Coverage: The platform supports multiple backup methods to address different workload types and recovery scenarios:

- Databases (logical and snapshot backups)
- Container platforms (persistent volumes and platform metadata)
- Messaging platforms (Kafka, RabbitMQ – topic/queue data and configuration)
- API platforms (policies, configurations, metadata)
- AI/ML platforms (notebooks, models, metadata, persistent datasets)

Backup coverage includes data, configuration, and metadata where supported by the platform. Sensitive data is protected using encryption and access controls

Backup Methodology:

- Platform-native backup mechanisms
- Application-aware backups where supported
- Metadata and configuration and versioning

Backup & Restore Levels:

- Full Back up: Complete copy of data at defined intervals for baseline recovery.
- Incremental Backup: Captures changes since the last backup to reduce storage and network overhead.
- Snapshot-Based Backup: Point-in-time recovery for rapid restore of IaaS disks and PaaS services.
- Application-Consistent Backup: Ensures transactional integrity for databases and stateful PaaS workloads

Restore Levels :

- File-level restore for selective recovery
- Database restore with point-in-time recovery
- VM / system restore using full image backups
- Site-level restore through disaster recovery invocation

Restore activities are executed by authorised TCS Enterprise Cloud or SovereignSecure Cloud support teams and are fully auditable.

Datacentre & Disaster Recovery: TCS Enterprise Cloud or SovereignSecure Cloud operates from multiple datacentres with built-in disaster recovery capabilities. Primary and secondary sites are geographically separated to ensure resilience against site-level failures. Backup data is securely stored and replicated in line with enterprise standards.

Business Continuity & DR: Business continuity and disaster recovery plans are defined based on service criticality and business impact. DR solutions are designed to meet agreed

RPO and RTO targets, supported by documented runbooks, controlled failover procedures, and periodic DR testing.

Governance & Controls:

- Role-based access to backup and restore operations
- Secure backup storage and retention policies
- Centralised monitoring and reporting
- Periodic validation through restore and DR drills

Roles & Responsibilities:

Customers define business requirements and recovery objectives, while TCS Enterprise Cloud or SovereignSecure Cloud manages backup execution, monitoring, restore support, and DR operations through standardised support processes.

Business Value:

- Reduced risk of data loss and downtime
- Predictable and auditable recovery outcomes
- Compliance with enterprise and regulatory requirements
- Enhanced resilience and operational stability.

5. Onboarding and Offboarding Support

TCS provides structured onboarding and offboarding support to ensure a controlled, secure, and transparent engagement lifecycle for buyers consuming the service. Onboarding activities are designed to enable a smooth service initiation with minimal disruption; while offboarding processes ensure data protection, contractual compliance, and service continuity during exit.

Onboarding Support

During onboarding, TCS supports buyers through service initiation activities including service orientation, access enablement, and operational readiness. This includes the provision of service documentation, operating procedures, and architectural guidance in standard formats such as HTML, PDF, and ODF. Knowledge transfer sessions and walkthroughs are provided remotely, with optional onsite or virtual training where agreed. Onboarding activities are executed in alignment with the buyer's governance, security, and compliance requirements to ensure effective adoption of the service.

Offboarding and End-of-Contract Support

At the end of the contract, or upon termination, TCS supports an orderly offboarding process. Buyers retain full ownership and control of their data and may extract data using standard tools and APIs. TCS does not delete customer data for a defined retention period

(typically up to 30 days post-termination), allowing sufficient time for data retrieval, subject to settlement of applicable charges. Upon completion of data extraction and confirmation from the buyer, service access is securely decommissioned in accordance with agreed exit procedures and information security policies.

6. Service Constraints

- PaaS services are subject to pre-defined maintenance windows for platform upgrades, security patching, and infrastructure updates. Maintenance activities are communicated in advance, except in emergency situations.
- Customisation is limited to configuration-level changes (e.g., parameters, policies, resource sizing) within supported service boundaries. Platform core components, architecture, and underlying infrastructure are not customisable.
- Only approved runtimes, versions, and frameworks supported by the platform are permitted. Unsupported or custom platform components may not be deployed.
- Changes impacting shared PaaS components are governed through centralised change management and may require scheduling within standard maintenance windows.
- Administrative access to underlying platform infrastructure is restricted to TCS. Buyer access is limited to service-level interfaces and consoles.
- PaaS services operate in a shared, multi-tenant environment. Certain resource limits, quotas, and isolation controls apply to ensure platform stability.
- Backup frequency, retention, and restore options are defined by standard service policies and may not be customised beyond approved options.
- Emergency maintenance may be required to address critical security vulnerabilities or stability risks.
- Customisation requests outside standard service boundaries are subject to feasibility assessment and additional commercials.
- Service availability and support are governed by defined SLAs and support models.

7. Roles and Responsibilities – R A C I

Activities	TCS	Customer
Architecture Ownership and principles	C	A, R
Sizing as per Business Requirements	C	A, R
Provisioning of platform Service	A, R	C, I
Administration of Platform Service - Start/Stop Node / Cluster - Producer/Consumer Access Management - Platform Administration	A, R	C, I
Identity and access integration (IAM/PAM)	R, A	C, I

Activities	TCS	Customer
Monitoring and alerts - Monitoring of API clusters and metrics	R, A	C, I
Backup and recovery strategy (images/snapshots)	R, A	C, I
DR/Failover design and architecture (If applicable as per design)	R, A	C, I
DR/Failover testing (If applicable as per design)	R, A	C, I
Security hardening and zero-trust enforcement - Security patches, Releases & Patch Updates	R, A	C, I
Compliance and audit evidence (BIO/BIV)	R, A	C, I
Incident Management (P1–P3 triage/RCA)	R, A	C, I
Life cycle and EOL management (renewal/decommissioning)	R, A	C, I

8. Service Levels

Parameter	Gold	Silver	Bronze
License Type	Opensource	Opensource	Opensource
Availability	99.9%	99.5%	99%
Pricing RU	Per Node	Per Node	Per Node
Deployment	Dual DC / DR	Single DC / Dual DC	Single DC
Business Support Coverage	24x7	8x7	8x5

9. System Requirements

To enable delivery of TCS Enterprise Cloud Platform (ECP) or SovereignSecure Cloud(SSC) PaaS services, the Customer must ensure the following general and service-specific system and technical requirements are met.

- **Network Connectivity:** Secure network connectivity (VPN / private link / approved internet access) between buyer environments and TCS ECP or SSC, including required firewall openings and routing.
- **Identity and Access Management:** Availability of enterprise identity services (LDAP / Active Directory / SAML / OAuth) to support authentication, authorisation, and role-based access control.
- **Client Access and Tooling:** Supported browsers, secure endpoints, and user devices compliant with organisational security standards for accessing PaaS consoles and portals.
- **Licensing Responsibilities:** Buyer -owned licenses for application-level or third-party software unless explicitly included in the PaaS service scope.
- **ITSM and Operational Integration:** Access to buyer ITSM systems, escalation contacts, and approval workflows for incident, change, and service request management.

- **Compliance and Data Classification:** Buyer-provided data classification, regulatory requirements, and retention policies to ensure appropriate security and backup controls are applied.

10.Outage and Maintenance Management

Outage Management

- PaaS services are monitored 24x7 to detect service disruptions, performance degradation, and platform anomalies.
- Outages are classified based on severity levels aligned to business impact and service criticality.
- Incidents are logged, tracked, and managed through ITSM-integrated workflows, including escalation and communication.
- TCS performs platform-level troubleshooting and remediation, covering service components, platform configurations, and managed dependencies.
- Regular status updates are provided to stakeholders until service restoration and closure.
- Post-incident reviews are conducted for major outages to identify root cause and preventive actions.

Maintenance Management

- Planned maintenance activities include platform upgrades, patching, configuration changes, and security updates.
- Maintenance is performed during pre-approved maintenance windows with advance notification to the buyer.
- Changes follow controlled change management processes, including impact assessment and rollback planning.
- TCS ensures backward compatibility and service stability during platform upgrades wherever feasible.
- Emergency maintenance may be executed to address critical security or stability risks, with immediate notification.

Buyer Responsibilities

- Review and approve maintenance schedules and change notifications.
- Coordinate application-level testing post-maintenance where required.
- Report application-level issues not caused by the PaaS platform.

and comprehensive audit logging to maintain data confidentiality, integrity, and traceability throughout the process.

Once the customer confirms successful retrieval and verification of all required data, TCS initiates the secure decommissioning phase. Customer data residing in TCS-managed infrastructure is permanently deleted in accordance with contractual retention policies, regulatory obligations, and industry-recognised sanitisation standards. Evidence of deletion (such as data wipe certificates or audit logs) can be provided upon request.

All exit-related access, tooling, and data transfer channels are safeguarded through enterprise-grade security controls, including least-privilege role-based access control (RBAC), encryption in transit, multi-factor authentication (where applicable), continuous monitoring, and detailed audit logging. The entire exit process adheres to applicable data protection, privacy, and compliance requirements relevant to the customer's regulatory jurisdiction.

13.Security

Security Governance

- A named board-level executive is responsible for service security governance.
- Security governance is certified and audited against recognised standards.
- The service aligns with CSA CCM v3.0 and ISO/IEC 27001.
- Additional governance standards include ISO 27017, ISO 27018, Cyber Essentials Plus, and SOC 1/2/3.
- Information security policies and processes are based on public cloud provider standards, augmented by TCS industry and regulatory compliance expertise.

Operational Security

- User authentication supports:
 - Multi-factor authentication (2FA)
 - Public key authentication (including TLS client certificates)
 - Identity federation with enterprise identity providers
 - Restricted network access (e.g., PSN)
 - Dedicated connectivity (VPN)
 - Username/password where applicable
- Management access is protected using:
 - MFA and key-based authentication
 - Federated identity controls
 - Restricted management networks
 - Bastion host-based access

- Access restrictions to management interfaces and support channels follow cloud-provider controls with customer-specific compliance enhancements.
- Access restriction testing is performed at least every 6 months.

Data Protection

- Backup Recovery:
Users can recover backups themselves through secure web-based interfaces, subject to role permissions.
- Data in Transit:
 - TLS 1.2 or higher
 - IPsec or TLS VPN gateways
 - Secure private or public-sector networks
- Internal Network Protection:
 - Logical tenant segregation
 - Encrypted API calls
 - Encrypted console access using TLS

Physical Security

- Tier III certified data centres
- Multi-layer physical security controls
- Continuous surveillance, access logging, and biometric enforcement

Platform Security

- DDoS-protected multi-ISP internet connectivity
- Logical perimeter firewalls and IPS
- Secure load balancers with SSL offloading
- OS and middleware hardening managed by TCS
- Privileged Identity Management (PIM) for platform operations
- Centralised SIEM and SOC monitoring
- Encryption of data in flight and at rest.

14. Why TCS

The widespread adoption of technology by businesses has led people to expect similar experiences from the public sector. Governments across the world are harnessing digital innovation to respond to people's needs and empower them.

The vision is clear and compelling: a forward-thinking government that embraces innovation and is always a step ahead, ready to meet the future.

We ensure that technology and strategy work together to help governments meet people's needs, embrace innovation, and address complex issues – from climate change and public health to education and national security.

We work in partnership with our customers, co-developing solutions to assist in digital transformation and re-imagination. TCS helps organisations handle the competing pressures that the shift to digital can bring; providing the skills and scale needed to react quickly to short-term concerns, while always ensuring that the focus remains on what is right for the client in the long-term.

The TCS Advantage:

- **Modernisation Expertise** - TCS works closely with several Public Sector agencies across the globe to help leverage digitisation to modernise services
- **Public Sector domain experience** - Extensive experience in solutions for governments, local agencies, municipal corporations, public-sector entities, and security establishments
- **Dedicated Centres of Excellence (CoE)** - Mature assets and accelerators
- **Leveraging strategic partnerships with product vendors** – strategic alliances with industry leading and niche partners. We also effectively leverage the TCS Co-Innovation Network (COIN™) that brings start-ups, academia, customers, research institutions together to create innovative solutions to business problems.
- **Large pool of skilled resources** - Right blend of management, industry, and technology expertise.

TCS Enterprise Cloud Advantage:

At Tata Consultancy Services (TCS), we are committed to accelerating your digital transformation with a secure, resilient, and future-ready Platform as a Service (PaaS) offering. Our state-of-the-art Enterprise Cloud Platform (ECP) or SovereignSecure Cloud (SSC) is designed to empower organisations to innovate rapidly, modernise applications, and scale with confidence—while maintaining the highest standards of security, compliance, and operational excellence.

Business Value Beyond Platform

TCS PaaS provides more than just a managed platform—it is a catalyst for business agility and innovation. We enable you to focus on delivering business outcomes by eliminating the complexity of infrastructure and middleware management. Our platform service model supports a wide range of managed services, including containers, databases, streaming, APIs, DevOps, messaging, and AI/ML workbenches, all delivered with enterprise-grade reliability and security.

Governance, Service Management, and Architecture Excellence

- **Governance:** Built on zero-trust principles and certified against global standards (CSA CCM, ISO/IEC 27001, ISO 27017/18, Cyber Essentials Plus, SOC 1/2/3), TCS PaaS embeds security and compliance by design. Our managed services model ensures strict data sovereignty, regulatory alignment, and auditable controls, giving you confidence in every deployment.
- **Service Management:** We provide end-to-end operational ownership, from onboarding to offboarding, with 24x7 monitoring, proactive incident management, and structured support. Our service desk, automation, and integrated monitoring deliver unified visibility and control, enabling you to adapt quickly to new business initiatives and technical change.
- **Architecture:** TCS applies proven architecture frameworks and design principles to de-risk and future-proof your environment. Our composable building blocks—spanning containers, databases, messaging, APIs, and AI/ML—ensure predictable performance, strong isolation, and operational simplicity.

Developer Enablement and Innovation

- **Accelerated Application Delivery:** TCS PaaS provides pre-configured environments, integrated CI/CD tooling, and automated deployment pipelines, enabling faster time-to-market for your digital services.
- **Modern Application Architectures:** Support for microservices, containers, serverless, and API-driven development empowers your teams to build scalable, resilient, and cloud-native applications.
- **Integrated DevOps and Data Services:** Managed DevOps toolchains, database-as-a-service, streaming, and messaging platforms allow your teams to focus on innovation, not platform maintenance.
- **AI/ML and Data Science Ready:** Workbench as a Service delivers secure, collaborative JupyterLab environments for data scientists and AI/ML developers, accelerating experimentation and model development.

Security, Compliance, and Resilience

- **Enterprise-Grade Security:** Multi-factor authentication, encryption at rest and in transit, role-based access control, and continuous monitoring are standard across all services.

- **Operational Resilience:** High availability, disaster recovery, and automated backup/restore ensure business continuity and data protection.
- **Compliance by Design:** Our platform supports your regulatory requirements with built-in controls, audit trails, and data sovereignty.

Tailored Solutions and Global Reach

TCS works closely with you to understand your business requirements, compliance needs, and technology strategy, curating solutions that fit your unique context. With 26 global availability zones, enterprise-grade security, and a full-stack PaaS offering, TCS enables you to run mission-critical workloads with confidence—wherever and however you need.

Partner with TCS for Your Cloud Journey

Choose TCS for a cloud partnership that goes beyond technology. We deliver measurable business outcomes, operational excellence, and a foundation for ongoing innovation. With TCS, you gain a trusted partner dedicated to your success, every step of the way.

15.Pricing

Please refer to the TCS Pricing Document for this service.

16.Terms and Conditions

Please refer to the TCS Terms and Conditions for this service

About Tata Consultancy Services

Tata Consultancy Services (TCS) (BSE: 532540, NSE: TCS) is a digital transformation and technology partner of choice for industry-leading organisations worldwide. Since its inception in 1968, TCS has upheld the highest standards of innovation, engineering excellence and customer service.

Rooted in the heritage of the Tata Group, TCS is focused on creating long term value for its clients, its investors, its employees, and the community at large. With a highly skilled workforce spread across 55 countries and 202 service delivery centres across the world, the company has been recognised as a top employer in six continents. With the ability to rapidly apply and scale new technologies, the company has built long term partnerships with its clients – helping them emerge as perpetually adaptive enterprises. Many of these relationships have endured into decades and navigated every technology cycle, from mainframes in the 1970s to Artificial Intelligence today.

TCS sponsors 14 of the world's most prestigious marathons and endurance events, including the TCS New York City Marathon, TCS London Marathon and TCS Sydney Marathon with a focus on promoting health, sustainability, and community empowerment. TCS generated consolidated revenues of over US \$30 billion in the fiscal year ended March 31, 2025.

Visit www.tcs.com

All content / information present here is the exclusive property of Tata Consultancy Services Limited (TCS). The content / information contained here is correct at the time of publishing. No material from here may be copied, modified, reproduced, republished, uploaded, transmitted, posted, or distributed in any form without prior written permission from TCS. Unauthorised use of the content / information appearing here may violate copyright, trademark, and other applicable laws, and could result in criminal or civil penalties.

Copyright © 2026 Tata Consultancy Services Limited