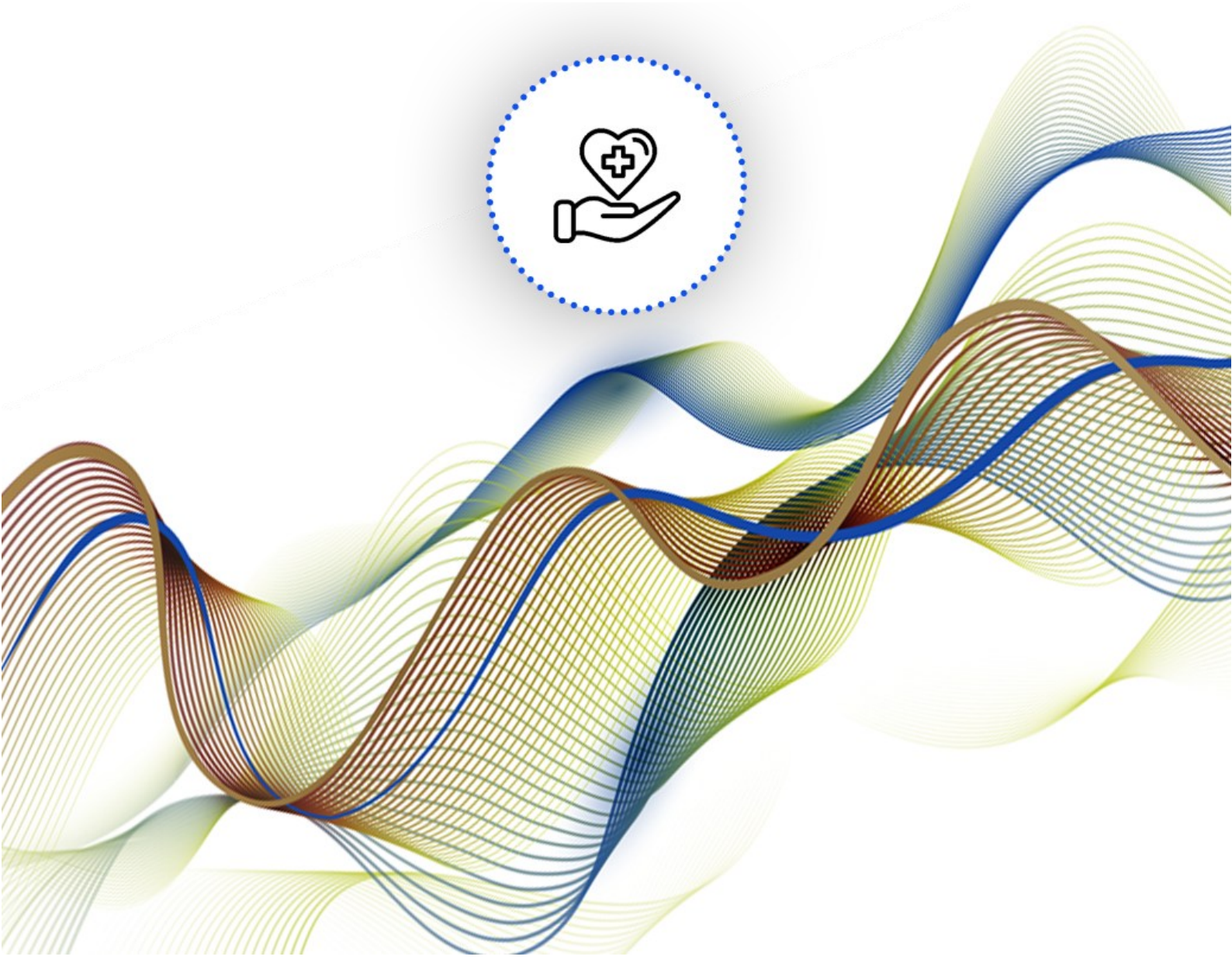
TCS Infrastructure as a Service (IaaS) Services

G-Cloud 15: Lot 1a

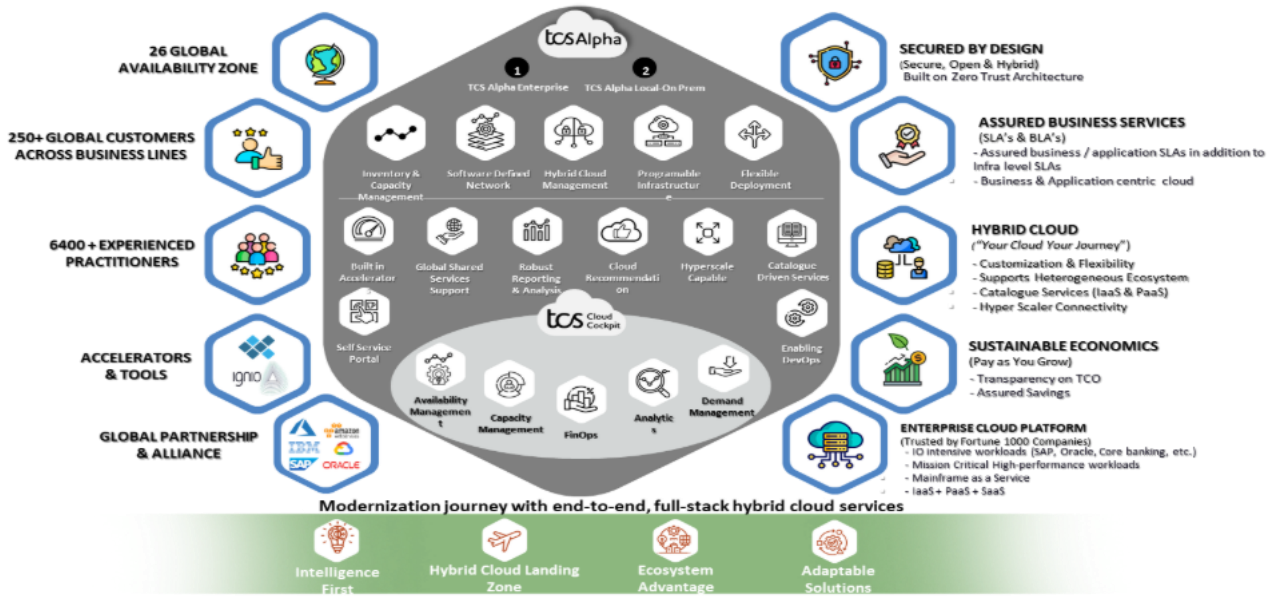
Service Definition



Contents

1. Service Description

TCS' state-of-the-art Enterprise Cloud Platform (ECP) or SovereignSecure Cloud Platform (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 ECP or SSC 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 –** TCS 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.

1.1 Bare Metal Services

Bare Metal Services provide dedicated, single-tenant compute, storage, and network infrastructure designed for workloads requiring deterministic performance, strict isolation, and full operational control. The service enables customers to run business-critical, regulated, and performance-sensitive applications without the overhead or variability of shared or virtualised platforms. Customers retain complete control over firmware, operating systems, security hardening, and runtime configuration, while benefiting from a fully managed operational model including monitoring, backup, patching, incident, and change management. The service is ideal for public sector, regulated industries, and core digital platforms where availability, integrity, confidentiality, and auditability are mandatory.

Key Features:

- **Dedicated Single-Tenant Infrastructure**: Provides exclusive physical servers with no shared resources, ensuring isolation, sovereignty, and predictable performance.
- **Standardised Bare Metal Profiles**: Offers a catalogue of pre-defined server, storage, and network configurations that can be combined into application landing zones.
- **Full Stack Control**: Enables control from firmware and BIOS through operating system and security hardening, with optional hypervisor support where required.
- **High-Performance Storage Options**: Supports multiple storage tiers ranging from high-IOPS block storage for transactional workloads to capacity-optimised storage for archives and backups.
- **Enterprise Network Architecture**: Includes segmented VLANs, spine-and-leaf architecture, firewall clusters, load balancers, DMZ and intranet zones, DNS, DHCP, and NTP services.
- **Managed Operations and Monitoring**: Provides 24x7 monitoring of server health, hardware sensors, resource utilisation, and core services using enterprise monitoring platforms.
- **Lifecycle and Vendor Management**: Covers firmware updates, driver management, OS patching, incident triage, root cause analysis, and vendor coordination.

Benefits:

- **Predictable and Deterministic Performance**: Eliminates noisy-neighbour effects, delivering consistent performance for latency-sensitive and high-throughput workloads.
- **Strong Isolation and Data Sovereignty:** Ensures strict tenant isolation and full control over data, infrastructure, and security configurations.
- **Compliance by Design**: Supports regulatory and public-sector compliance requirements through dedicated infrastructure and auditable controls.
- **Operational Simplicity with Full Control**: Combines the flexibility of owning the stack with the convenience of a managed service model.
- **Suitable for Mission-Critical Workloads**: Ideal for core platforms, regulated data repositories, archiving systems, and infrastructure applications requiring high availability and reliability.

<table>
<tr><td>Service unit</td><td colspan="6">Per server</td></tr>
<tr><td>Licenses used</td><td colspan="6">Not applicable</td></tr>
<tr><td>Service level options</td><td colspan="6"><table>
<tr><th>SLA level</th><th>Availability target</th><th>RPO/RTO</th><th>Capacity and performance</th><th>DR / Failover</th><th>Scope</th></tr>
<tr><td>Gold</td><td>99.9</td><td>RPO ≤ 4 hours / RTO ≤ 4 hours</td><td>IOPS/latency targets; CPU/RAM space ≥ 20%</td><td>Active-passive failover (≤ 2 hours)</td><td>Dedicated or reserved hosts for high-priority apps</td></tr>
<tr><td>Silver</td><td>99.5</td><td>RPO ≤ 8 hours / RTO ≤ 8 hours</td><td>Optimal performance monitoring</td><td>Documented recovery plan (≤ 1 BD)</td><td>Shared rack resources; non-critical workloads</td></tr>
<tr><td>Bronze</td><td>99</td><td>RPO ≤ 24 hours / RTO ≤ 2 BD</td><td>Basic capacity controls</td><td>Best effort recovery</td><td>Non-critical hosts; dev/test</td></tr>
</table></td></tr>
</table>

1.2 Virtual Servers

Virtual Server Services provide logically isolated compute, storage, and network resources delivered on a managed hypervisor platform, enabling predictable performance, strong isolation, and operational sovereignty at the operating system and application layers. The service preserves full customer control of the guest environment including OS configuration, security hardening, and runtime settings while leveraging platform controls such as resource

reservations, affinity policies, and QoS to mitigate noisy-neighbour effects. The service is integrated into a managed operational model encompassing golden images, monitoring, backup and recovery, patching, and incident and change management, making it suitable for business-critical and regulated workloads that require elasticity, rapid provisioning, and compliance by design

Key Features:

- Managed Hypervisor-Based Compute: Virtual machines run on a managed hypervisor with support for Windows and Linux guest images, golden templates, and policy baselines.
- Strong Logical Isolation and QoS Controls: Resource reservations, scheduler affinity, and QoS policies provide predictable performance and minimise noisy-neighbour impact.
- Composable VM, Storage, and Network Catalogue: Curated VM profiles, storage tiers, and network constructs can be assembled into application landing zones.
- Flexible Storage Tiers: Storage options range from high-IOPS block volumes for transactional workloads to capacity-optimised tiers for archives and backups, defined by IOPS, throughput, and latency.
- Enterprise Network Architecture: Spine-and-leaf fabric with segmented VLANs/VRFs, firewall clusters or virtual firewalls, load balancers across DMZ and intranet zones, and supporting DNS, DHCP, and NTP services.
- Full Guest OS Control: Customers retain control of guest OS configuration, security hardening, and application runtime settings.
- Managed Operations and Lifecycle: 24×7 monitoring of VM health, resource utilisation, and core services, with incident triage, root cause analysis, provider coordination, and lifecycle management for images, tools/drivers, hypervisor updates, and guest OS patching.

Benefits:

- Predictable Performance with Elasticity: Delivers consistent performance through reservations and QoS while enabling elastic scaling and rapid provisioning.
- Operational Efficiency: Reduces infrastructure management overhead through a fully managed platform and standardised building blocks.
- Strong Isolation without Dedicated Hardware: Achieves secure, logical isolation suitable for regulated workloads without the cost of bare metal.
- Compliance by Design: Supports public sector and regulated requirements for availability, integrity, confidentiality, and auditability.

- Faster Time to Value: Accelerates application deployment using golden images, standardised profiles, and automated operations.

Service unit	Per server					
Licenses used	Not applicable					
Service level options						
	SLA level	**Availability target**	**RPO/RTO**	**Capacity and performance**	**DR / Failover**	**Scope**
	Gold	99.9%	RPO ≤ 4 hours / RTO ≤ 4 hours	IOPS/latency targets; ≥ 20% CPU/RAM headroom	Active-passive (warm standby, storage/host replication) with VM restart ≤ 2 hours	Dedicated or reserved pools for high-priority applications
	Silver	99.5%	RPO ≤ 8 hours / RTO ≤ 8 hours	Continuous performance monitoring	Documented recovery plan (≤ 1 business day)	Shared clusters; non-critical VM workloads
	Bronze	99%	RPO ≤ 24 hours / RTO ≤ 2 business days	Basic capacity controls	Best-effort recovery	Non-critical VMs; dev/test environments

1.3 Storage Services

TCS Storage Services provide end-to-end technical ownership of enterprise storage platforms across on-premises, hybrid, and multi-cloud environments, covering strategy, architecture, engineering, migration, and 24x7 operations. TCS delivers comprehensive services for block, file, and object storage, including SAN (Fibre Channel, iSCSI), NAS (NFSv3/v4, SMB/CIFS), scale-out and parallel file systems, software-defined storage, hyper-converged infrastructure, and cloud-native storage platforms. The service includes storage discovery and baselining, capacity and performance modelling (IOPS, latency, throughput), workload characterisation, tiering strategies, thin provisioning, compression and deduplication, storage virtualisation, multipathing configuration, zoning, LUN masking, namespace design, and QoS enforcement to meet application SLAs. TCS executes non-disruptive data mobility, storage refresh and technology upgrades, controller and fabric integration, storage consolidation, and vendor-agnostic interoperability management, while ensuring encryption at rest, role-based access control, secure tenancy, audit logging, and compliance alignment. Ongoing operations include firmware and microcode lifecycle management, proactive health and performance monitoring, automation using APIs and

orchestration frameworks, predictive capacity forecasting, cost and utilisation optimisation, incident and change management, and continuous service improvement, enabling high-availability, scalable, secure, and performance-optimised storage environments aligned with enterprise application, database, virtualisation, and cloud adoption strategies

The service supports multiple consumption models and integrates seamlessly with virtual servers, bare metal platforms, container platforms, and PaaS services. Storage resources are provisioned as composable building blocks and aligned to application landing zones, enabling organisations to select the right balance of performance, resilience, and cost while maintaining compliance by design

Key Features:

- **Multiple Storage Types and Tiers**: Supports block, file, and object storage with tiers optimised for performance, capacity, or archival needs.
- **Defined Performance Characteristics**: Each storage tier is clearly defined by IOPS, throughput, and latency to support predictable application performance.
- **Enterprise-Grade Data Protection**: Built-in support for snapshots, replication (where applicable), and integration with centralised backup and recovery services.
- **Secure Logical Segregation**: Storage volumes are logically segregated across tenants and workloads to ensure data isolation and security.
- **Scalable and Elastic Capacity**: Enables on-demand scaling of storage capacity without service disruption, supporting growth and changing workload demands.
- **Integrated Monitoring and Management**: 24×7 monitoring of storage health, capacity utilisation, and performance, with proactive alerting and incident management.
- **Lifecycle and Retention Management**: Supports data lifecycle policies for retention, archival, and secure deletion in line with compliance requirements.

Benefits:

- **Predictable Storage Performance**: Ensures consistent application behaviour through clearly defined and managed performance tiers.
- **Optimised Cost Efficiency**: Enables right-sizing by matching workload requirements to appropriate storage tiers.
- **High Availability and Reliability**: Designed to support enterprise availability requirements with resilient architecture and managed operations.
- **Strong Security and Compliance**: Protects data through isolation, encryption (where applicable), and auditable controls aligned to regulatory standards.
- **Operational Simplicity**: Reduces administrative overhead by delivering storage as a managed service integrated with compute and platform services.

Service unit	Per TB				
Service level options	**Storage Tier**	**Availability**	**Performance**	**Replication/Resilience**	**Support**
	Gold	99.9%	2000 IOPS/TB	Yes	24x7
	Silver	99.5%	1000 IOPS/TB	Yes	8x7
	Bronze	99%	500 IOPS/TB	No	8x5

1.4 Backup & Restore Services

TCS Backup Services deliver end-to-end design, implementation, and managed operations for enterprise data protection platforms across on-premises, hybrid, and multi-cloud environments. TCS provides comprehensive backup services covering application-consistent and crash-consistent backups for physical, virtual, database, container, and cloud workloads, using agent-based, agentless, snapshot-integrated, and API-driven backup mechanisms. The services include backup architecture and sizing, policy design (RTO/RPO aligned), scheduling, retention management, media management, catalogue and metadata management, encryption in transit and at rest, key integration, role-based access control, and immutable backup configurations to protect against data loss and cyber threats. TCS performs backup onboarding, job orchestration, performance tuning, backup window optimisation, failure remediation, restore validation, and regular recovery testing, along with platform upgrades, patching, and vendor interoperability management. Through 24x7 proactive monitoring, automation, capacity forecasting, reporting, and ITIL-aligned incident and change management, TCS ensures reliable, scalable, secure, and compliant backup operations that meet enterprise data protection, audit, and regulatory requirements while minimising operational risk.

Key Features:

- **Policy-Driven Backup Scheduling:** Supports automated, scheduled backups and ad-hoc backups on request, aligned to governance and compliance requirements.
- **Multi-Level Backup and Restore:** Enables file-level, application-level, and system-level restores based on workload and recovery needs.
- **Immutable and Tamper-Resistant Backups:** Supports immutable backup configurations to protect data during the defined retention period.
- **Defined RPO/RTO Alignment:** Backup execution and restore operations align with agreed recovery point and recovery time objectives.
- **Secure Backup Storage and Media Handling:** Utilises secure storage facilities with encryption, controlled access, and secure media or device disposal.

- **24×7 Monitoring and Reporting:** Backup jobs are continuously monitored with scheduled reporting and alerting for failures or anomalies.
- **Isolated Backup Operations:** Backup processes are isolated from production workloads to minimise performance impact.

Benefits:

- **Reduced Risk of Data Loss**: Ensures consistent and reliable protection of critical data and configurations.
- **Improved Recovery Confidence**: Enables predictable and auditable restore operations aligned to business recovery objectives.
- **Enhanced Protection Against Cyber Threats**: Immutable backups and encryption reduce the impact of ransomware and data tampering.
- **Operational Simplicity**: Centralised management and monitoring reduce administrative effort and operational complexity.
- **Compliance and Audit Readiness**: Supports retention management, audit trails, and secure disposal to meet regulatory requirements.

Service unit	Per GB					
Service level options	**Backup Tier**	**RPO**	**RTO**	**Backup policy (baseline)**	**Encryption (at rest / in transit)**	**Offsite handling (if tape in scope)**
	Bronze	≤ 24 hours	≤ 2 business days	Policy-driven; on-demand supported	Mandatory	Optional; scheduled offsite
	Silver	≤ 24 hours	≤ 24 hours	Policy-driven; daily/weekly cadence	Mandatory	Scheduled offsite handling
	Gold	≤ 4 hours	≤ 4 hours	Policy-driven; daily incremental / weekly full	Mandatory	Scheduled offsite handling

1.5 Firewall Services

Managed Network Firewall Services provide centrally governed, secure perimeter and internal network protection across on-premises, data centre, and cloud environments. Service covers the complete firewall lifecycle including design, deployment, policy management, secure connectivity, monitoring, and compliance. The offering supports both physical and virtual firewalls, deployed in high-availability architectures, and integrated with

enterprise security operations to ensure continuous protection, operational resilience, and audit readiness.

The service is designed to secure municipal, public sector, and enterprise environments by enforcing least-privilege access, preventing threats, and ensuring secure network segmentation. Firewall operations are embedded into a managed service model with 24×7 monitoring, SIEM integration, change and incident management, configuration version control, and regular testing to meet regulatory and compliance obligations.

Key Features:

- **Physical and Virtual Firewall Platforms**: Supports hardened physical appliances and virtual firewalls deployed on-premises, in data centres, or cloud environments.
- **High Availability and Resilience**: Firewalls are deployed in HA pairs or clusters with failover to ensure continuous network protection.
- **Advanced Threat Protection**: Includes stateful inspection, application and URL filtering, IPS/IDS, DoS/DDoS protection, and policy-based TLS decryption.
- **Secure Connectivity Services**: Supports site-to-site and remote connectivity using IPSec/IKEv2 VPNs, NAT, and routing services.
- **Strong Access Control and Administration**: Administrative access is secured using RBAC with MFA, PAM/bastion access, and controlled management networks.
- **Centralised Monitoring and SIEM Integration**: Firewall telemetry (syslog, SNMP, NetFlow) is integrated with SIEM for correlation, alerting, and security visibility.
- **Policy and Configuration Lifecycle Management**: Firewall rules and configurations are version controlled, backed up, patched, and regularly tested, including DR validation.
- **Compliance and Audit Alignment**: Controls are aligned to ISO 27001, BIO, NEN7510, NIS2, and GDPR requirements.

Benefits:

- **Improved Network Security Posture**: Protects environments from external and internal threats through layered, policy-driven controls.
- **High Availability and Business Continuity**: HA deployments and tested failover reduce the risk of network outages.
- **Operational Consistency and Control**: Centralised management ensures consistent policy enforcement and reduces configuration drift.
- **Regulatory and Audit Readiness**: Built-in logging, monitoring, and compliance mapping simplify audits and regulatory reporting.
- **Reduced Operational Overhead**: Offloads firewall operations, monitoring, patching, and incident handling to a managed service model.

Service unit	Per firewall instance (Physical/Virtual)			
Licenses used	IPS license, VPN Client to Site License			
Service level options	SLA	Gold	Silver	Bronze
	Availability	99.9%	99.50%	99%
	Support	24×7	9x7	9x5

1.6 Load Balancer Services

Load Balancer as a Service (LBaaS) offers a centrally managed solution for dependable traffic distribution across various backend application targets, such as virtual machines, containers, and platform services. This service significantly enhances application availability, performance, and security by intelligently directing client traffic through policy-driven controls and continuous health monitoring. LBaaS uses both physical and virtual Application Delivery Controllers and supports Layer 4 and Layer 7 load balancing, ensuring robust application delivery across data centres and cloud environments. The service is provided within a fully managed operational model, encompassing design, deployment, monitoring, patching, configuration governance, backup, and capacity planning. Moreover, LBaaS integrates security, observability, and compliance controls to guarantee audit-ready operations, predictable performance, and high availability for both business-critical and public-facing applications.

Key Features:

- **Layer 4 and Layer 7 Traffic Management**: Supports TCP/UDP and application-aware HTTP/HTTPS traffic distribution.
- **Advanced Routing and Load-Balancing Policies**: Includes round-robin, least-connections, weighted routing, and session persistence (sticky sessions).
- **High Availability and Auto-Failover**: Deployed in HA pairs or clusters with active health probes and automatic failover.
- **TLS Offload and Re-Encryption**: Supports TLS termination, re-encryption, SNI, HTTP/2, gRPC, and certificate lifecycle management.
- **Security Integration**: Supports RBAC with MFA, optional WAF integration, DDoS protection, mutual TLS, and PKI-based certificates.
- **Continuous Monitoring and Observability**: Metrics, logs, and telemetry integrated with SIEM for alerting, correlation, and drift detection.
- **Managed Operations and Lifecycle**: Includes patching, encrypted configuration backups, capacity planning, and performance tuning.

Benefits:

- **Improved Application Availability:** Ensures continuous service delivery through health checks, redundancy, and automated failover.
- **Enhanced Application Performance**: Optimises traffic distribution and reduces latency through intelligent routing and TLS offload.
- **Built-In Security for Application Traffic**: Protects applications with integrated security controls and optional WAF and DDoS defences.
- **Operational Consistency and Governance**: Centralised management, version-controlled configurations, and audited change processes.
- **Scalable and Resilient Application Delivery**: Supports growth and varying traffic patterns without application redesign.

Service unit	Per Load balancer instance (Physical/Virtual)			
Licenses used	WAF			
Service level options	SLA	Gold	Silver	Bronze
	Availability	99.9%	99.50%	99%
	Support	24×7	9x7	9x5

1.7 GPU As A Service

GPU as a Service provides on-demand access to high-performance Graphics Processing Units (GPUs) required for compute-intensive workloads such as artificial intelligence and machine learning (AI/ML), deep learning, high-performance computing (HPC), rendering, and advanced analytics. Delivered by TCS the service enables enterprises to consume GPU capabilities without investing in specialised hardware, while ensuring scalability, security, and operational efficiency.

The service abstracts the underlying GPU infrastructure and delivers it as a managed platform hosted on cloud, private cloud, or on-premises environments. It supports parallel processing workloads by providing optimised GPU resources that can be dynamically allocated based on workload demand, enabling faster model training, simulation, and data processing.

Typical Use Cases

- Deep Learning and AI Model Training
- High-Performance Computing (HPC) workloads
- Video Rendering and 3D Graphics Processing
- Big Data Analytics and Advanced Analytics (e.g., sentiment analysis, customer segmentation)
- MLOps pipelines and model experimentation

- Image Processing and Computer Vision
- Text and Natural Language Processing (NLP)
- Audio and Video Processing
- Legacy Code Modernisation and Acceleration

Key Features:

- **GPU Hardware Layer**: Provides access to high-end GPUs from multiple OEMs, optimised for parallel processing and compute-intensive workloads such as AI/ML training, HPC, and rendering.
- **Virtualisation Layer**: Enables secure sharing of GPU resources across multiple tenants using GPU virtualisation and container-based isolation, ensuring efficient utilisation and workload separation.
- **Service Orchestration and Scheduling**: Manages GPU resource allocation, scheduling, scaling, and workload prioritisation based on demand, enabling elastic consumption and optimised performance.
- **Security and Isolation**: Ensures tenant isolation and workload protection through virtualisation controls, container security, and controlled access mechanisms.
- **Monitoring and Resource Management**: Provides visibility into GPU utilisation, performance, and consumption to support capacity planning, optimisation, and governance.

Benefits:

- **Accelerated Compute-Intensive Workloads**: Significantly reduces processing time for AI/ML, HPC, and analytics workloads.
- **Cost-Efficient GPU Consumption:** Eliminates upfront hardware investment through shared, on-demand GPU usage.
- **Elastic Scalability:** Scales GPU capacity up or down based on workload requirements.
- **Reduced Operational Complexity:** Offloads GPU infrastructure management, scheduling, and maintenance.
- **Secure and Governed Platform Usage:** Ensures controlled access, tenant isolation, and compliance with enterprise policies.

Service unit	Per GPU Virtual Machine			
Licenses used	Not Applicable as this service provides only the GPU infrastructure and no additional software is provided			
Service level options	**Parameter**	**Gold**	**Silver**	**Bronze**
	License Type	Not Applicable	Not Applicable	Not Applicable
	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

2. Service Features

- **Hybrid and Multi-Cloud Infrastructure Enablement:** Seamless infrastructure across on-premises, private and public cloud platforms.
- **Direct Hyperscaler Support Enablement**: Integrated licensing and hyperscaler support through standard and enhanced options.
- **Elastic Compute and Storage Provisioning**: On-demand scalable compute and storage aligned to workload requirements
- **Standardised Operations and Automation**: Automated, standardised infrastructure operations with centralised visibility and control.
- **Multi-Cloud Brokering and FinOps Console:** Centralised multi-cloud brokering with unified billing and financial visibility.

3. Service Benefits

- **Simplified Partner Engagement Model:** Single partner managing hyperscalers, services, licensing, billing, and support.
- **Pay-As-You-Go Consumption Model:** Consumption-based pricing aligned to actual infrastructure usage and scalability
- **Financial Transparency:** Provides consumption-based pricing with visibility into resource utilisation and capacity planning
- **Foundation for Cloud-Native and PaaS services:** Acts as a stable and secure base layer for platform services, containers, data platforms, and application modernisation
- **Reduced Operational Overhead:** Offloads infrastructure management and lifecycle to a managed service model.

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 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 platform or SovereignSecure Cloud 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:

- Virtual machine images
- OS and data disks
- File system and attached storage
- Infrastructure configuration and metadata

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

Backup Methodology:

- Image-level and disk level backups
- Snapshot-based backups
- Incremental backups to optimise storage and network usage

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
- Disk level restore
- VM / system restore using full image backups
- Site-level restore through disaster recovery invocation

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

Datacentre & Disaster Recovery: TCS Enterprise 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 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

- Infrastructure maintenance such as hypervisor patching, firmware upgrades, and capacity enhancements is performed during approved maintenance windows, with prior notification wherever possible.
- IaaS allows greater customisation at the operating system and application layers. Customisation of underlying virtualisation, physical infrastructure, and network core components is restricted.
- Only supported OS images and versions are permitted. Unsupported or end-of-life operating systems may require exceptional approval.
- Certain maintenance activities may require VM reboots or live migrations. Buyers must ensure application readiness and support during such events.
- Security controls at the infrastructure layer are standardised. Buyer-specific security configurations must be compatible with platform standards.
- Resource allocation is subject to capacity availability and quota limits defined by the platform.
- Backup and restore capabilities are limited to defined service levels and may not support custom tooling outside approved solutions.
- 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

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

To enable delivery of TCS Enterprise Cloud Platform (ECP) or SovereignSecure Cloud (SSC) Infrastructure-as-a-Service (IaaS) offerings, the buyer is required to ensure the following general and service-specific system and technical prerequisites are fulfilled.

- **Network Connectivity**: Secure connectivity between buyer environments and TCS ECP or SSC IaaS infrastructure using VPN, private connectivity, or approved internet access, including required firewall rules and routing.
- **Identity and Access Management**: Integration with buyer identity services (Active Directory / LDAP / SAML) to enable authentication, authorisation, and role-based access to infrastructure resources.
- **Client Access and Administration Tools**: Supported web browsers and secure endpoints for accessing IaaS portals, consoles, and management interfaces, compliant with organisational security standards.

- **Operating System Licensing**: Buyer-owned licenses for operating systems (where BYOL is applicable) unless included as part of the IaaS service offering.
- **Security Tooling Integration**: Buyer-mandated security agents (anti-virus, EDR, vulnerability scanners) compatible with the IaaS platform and operating systems.
- **ITSM and Operational Interfaces**: Access to buyer ITSM systems, escalation paths, and approval workflows for incident, change, and service request management.
- **Compliance and Data Classification**: Buyer-provided data classification, regulatory obligations, and retention requirements to ensure appropriate security and backup controls.

9. Service Levels

Parameter	Gold	Silver	Bronze
Availability	99.9%	99.5%	99%
Deployment	Dual DC / DR	Single DC / Dual DC	Single DC
Business Support Coverage	24x7	8x7	8x5

10.Outage and Maintenance Management

Outage Management

- IaaS infrastructure components are monitored 24x7 for availability, performance, and faults.
- Infrastructure incidents are categorised by severity and managed through ITSM processes.
- TCS addresses outages related to compute, storage, network, and virtualisation layers within the IaaS scope.
- Buyers are notified of incidents impacting infrastructure availability or performance.
- Root cause analysis is provided for major infrastructure outages, along with corrective actions.

Maintenance Management

- Planned maintenance includes hypervisor updates, firmware upgrades, infrastructure patching, and capacity enhancements.
- Maintenance is scheduled during approved maintenance windows and communicated in advance.
- TCS coordinates maintenance activities to minimise service disruption, including live migration where supported.

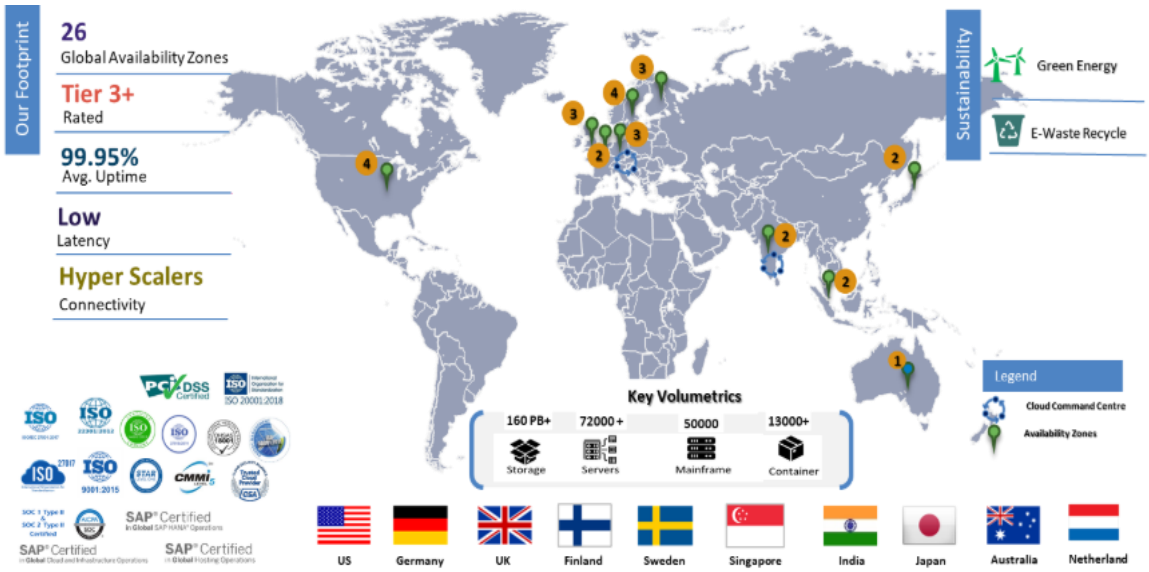
- Emergency maintenance may be required to address critical vulnerabilities or infrastructure risks, with prompt communication.

Buyer Responsibilities

- Manage application-level maintenance, patching, and testing within guest operating systems.
- Ensure application readiness for infrastructure maintenance activities.
- Approve and support planned maintenance windows and recovery testing.

11.Hosting Options and Locations

TCS currently operates 26 global availability zones that are fully functional to on-board global customers on their private or hybrid cloud journeys. These global locations are strategically chosen typically Tier-III, ISO Security standards compliant facilities and are serviced by Tier-1 Carriers, ISPs (Internet Service Providers) and Internet Exchanges (select locations) which offer low latency, high bandwidth Network Service. This also enables rapid interconnection with Enterprise Networks, the Internet and Tier-1 Cloud Providers like AWS and Azure.



12.Access to data (upon exit)

Customers always maintain full and exclusive ownership of their data throughout the service lifecycle. Upon service termination or contract expiration, TCS enables customers to retrieve all customer-owned data assets in a secure and controlled manner. This includes,

but is not limited to, application data, system and platform configurations, metadata, audit and operational logs, virtual machine images and disks, storage volumes, database backups, and any other platform artifacts relevant to the subscribed service model (IaaS, PaaS)

During the agreed exit period, customers are granted authorised access through secure, auditable mechanisms. Data is made available in industry-standard, non-proprietary formats wherever technically feasible, ensuring portability and seamless migration to alternate environments or service providers. Platform-specific configuration data, infrastructure definitions, deployment metadata, and operational runbooks are exported or documented to assist in re-establishing equivalent functionality in the target environment.

TCS provides structured, time-bound exit assistance subject to contractual terms to support data extraction, integrity validation, transfer activities, and formal handover. All exit operations follow established change management processes, information security controls, 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 effective 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 TCS, we are trusted transformation partners to leading enterprises worldwide, delivering secure, resilient, and future-ready cloud infrastructure solutions. Our Enterprise Cloud Platform (ECP) or SovereignSecure Cloud (SSC) is designed to empower organisations on their hybrid and multi-cloud journeys, combining deep technical expertise with a robust, business-centric approach.

Business Value Beyond Infrastructure

TCS doesn't just solve infrastructure challenges—we enable business transformation. Our hybrid cloud platform lets you seamlessly integrate legacy environments with modern cloud services, unlocking agility, scalability, and innovation. We help you accelerate time to value, reduce operational overhead, and maximise return on investment through assured business SLAs and transparent, consumption-based pricing.

Governance, Service Management, and Architecture Excellence

- **Governance:** TCS ECP or SSC is built on zero-trust principles, with security and compliance embedded by design. Our managed services model ensures strict data sovereignty, regulatory alignment, and auditable controls, giving you confidence in every decision and deployment.
- **Service Management:** We deliver end-to-end operational ownership, from onboarding to offboarding, with 24x7 monitoring, proactive incident management, and structured support. Our service desk, automation, and FinOps console provide 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. Whether you need bare metal, virtual servers, GPU-as-a-Service, or integrated storage and backup, our composable building blocks and standardised profiles ensure predictable performance, strong isolation, and operational simplicity.

Tailored Solutions for Every Customer

Our approach is flexible and adaptable. We work 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 hybrid cloud offering, TCS enables you to run mission-critical workloads with confidence—wherever and however you need.

Innovation and Sustainability

TCS is committed to continuous improvement and innovation. Our platform supports emerging technologies such as AI/ML, advanced analytics, and containerisation, while embedding sustainability and cost optimisation into every engagement. We help you modernise, transform, and scale—securely and responsibly.

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**