rackspace technology.

Customer First.
Cloud First.

Rackspace Service Definition for G-Cloud 15 Cloud Support Services (Lot 3)

Date: 29th January 2026

Table of Contents

1. Introduction

1.1. Document Purpose

This service definition has been created to describe an overview of the Rackspace Sovereign Cloud Support Services suite of products.

1.2. Rackspace Company Overview

Rackspace is a pureplay private, public and hybrid cloud and AI solutions expert. We combine our expertise with the world's leading technologies – across AI, applications, data, security and cloud – to deliver end-to-end solutions. We have a proven record of advising our customers based on their organisational challenges, designing solutions that scale, building and managing those solutions and optimising returns into the future.

In the United Kingdom, we offer solutions that are specific to public sector organisations through our Rackspace Sovereign Services suite of products. We can help and support your organisation wherever you are on your journey to cloud adoption.

Rackspace has over two decades of experience supporting sovereign services within the UK. We have a wealth of expertise to support customers on both transitioning to a cloud-based solution for the first time or with migrating between cloud service providers. Globally, we provide cloud services and consulting to all verticals. Our head office is in San Antonio, Texas with multiple data centres and offices throughout the UK, EMEA and US.

To support our sovereign customers within the UK, Rackspace has dedicated teams and back-end support fabric that runs in isolation from each other and the global Rackspace tooling and support model. We have in place a fully UK sovereign support model utilising UK security cleared staff and a dedicated and secure operations building. Additionally, all public sector customer support operations are conducted via Rackspace's PSN-accredited, secure management environment that allows us to provide customers with high levels of assurance regarding the security of all our service offerings.

1.3. Privacy by Design

Rackspace complies with the data protection laws of the countries in which it operates. Rackspace's internal policies and processes consider the requirements of GDPR and adhere to the regulations as defined in the Data Protection Act 2018.

Rackspace does not determine the types of data that customers store on Rackspace's hosting environments and does not determine the classification of that data or how it is to be accessed, exchanged, or otherwise processed. Each customer retains full responsibility for protecting application access to any data that is stored on Rackspace's hosting environments.

However, Rackspace will work with each customer to design solutions that will meet an individual customer's requirements on data protection and will advise on suitable controls to implement. The responsibility for approving any additional security controls will always remain with the customer.

Please visit the Rackspace Privacy Centre for more information on our approach to data privacy: https://www.rackspace.com/information/legal/privacycenter

1.4. Rackspace Sovereign Cloud Support Services Certifications

Rackspace UK maintains a variety of certifications to provide high levels of assurance to our customers. These certifications include:

- ISO/IEC 27001:2013
- ISO/IEC 9001:2015
- ISO 27017
- ISO 27018
- Cyber Essentials+ (UK corporate network)
- PSN Service Provider (RSS Central – Secure Management Platform)

1.5. Rackspace Secure Management

Rackspace maintains a dedicated and air-gapped management environment, called Rackspace Sovereign Services Central (RSSC), to provide secure management of customer platforms, networks and workloads. RSSC is maintained to PSN Service Provider levels of assurance and is fully aligned to the highest level of NCSC guidance for secure third party support.

Access to RSSC is subject to approval by the Rackspace UK Sovereign Services team and is restricted to UK sovereign and security cleared engineers. The environment maintains its own domain, separate to the Rackspace corporate domain with strict role-based access control in place to minimise permissions for engineers while working within the environment. All activity is logged within a dedicated SIEM solution, which is monitored 24x7. All customer support activity is conducted via RSSC “edge node” servers, positioned in the customer network and subject to all relevant customer security policies.

All support tooling hosted within RSSC is fully tenanted, which allows Rackspace to maintain data separation between customers, as required by NCSC guidance. By using a tenanted approach to tooling, Rackspace can also support different customer configurations without causing impact across the customer tenants.

2. Cloud Support – Managed Private Cloud Services

Rackspace Managed Private Cloud Services has been designed to address the specific security, compliance and operational best practice needs of the UK public sector. A fully managed 24x7 service delivered remotely from our UK Sovereign Services centre of excellence and connected to our secure management fabric, so that it can support on-premises, at the edge as well as Rackspace-hosted UK sovereign private cloud solutions.

UK sovereign support includes the use of a suite of industry-standard ITSM tools that simplify operational management, while at the same time maximises security, systems availability and performance. All our systems are administered by UK vetted and security cleared staff.

Service Features

- 24x7 UK-based service from dedicated public sector centre of excellence
- Monitoring and alerting across IaaS and SaaS / PaaS elements
- End-to-end incident, problem and event management
- Regular patching, updates and configuration maintenance
- Managed DR and backup scheduling, execution and restore support
- Capacity and performance monitoring with proactive tuning
- SLA-driven UK-based service desk and operational support
- Change management, including planning and controlled implementation
- Service reporting, trend analysis and continuous improvement actions
- Health checks and full service lifecycle management

Service Benefits

- End to end UK digital sovereignty
- Reduced operational burden through fully managed IaaS and SaaS/PaaS
- Improved availability through proactive monitoring and optimisation
- Reduced risk with ITIL-aligned change, incident and problem processes
- Predictable outcomes through ongoing reporting and service governance
- Increased availability supported by continuous health and performance oversight
- Greater operational consistency through defined maintenance and patch cycles
- Enhanced resilience with managed DR, backup and restore services
- Improved long-term efficiency through continuous service improvement
- Confidence that critical services are performed by UK technical specialists

2.1. Managed Private IaaS

Rackspace Managed Private IaaS provides full operational management of a customer's dedicated infrastructure environment. Delivering end-to-end service oversight, including 24x7 monitoring, incident and problem management, capacity and performance management, patching, backup operations and ongoing platform optimisation. Our teams take responsibility for the health, stability and availability of the environment, coordinating change management, service reporting and continuous improvement activities.

By combining proactive operations with structured governance and clearly defined SLAs, the service ensures predictable performance, reduced operational risk and a consistently high-quality service experience.

2.2. Managed Private SaaS / PaaS

The Rackspace Managed Private SaaS / PaaS delivers a fully governed, secure and operationally managed application, database and platform environment tailored to UK public sector needs. We take end-to-end responsibility for security, performance, lifecycle management and continuous optimisation. This includes monitoring, patching, incident and problem management, capacity oversight, data protection and controlled change processes.

By combining hosting with managed platform services, we ensure predictable performance, improved security posture and reduced operational complexity. Customers gain a resilient, compliant and scalable environment that enables rapid application delivery while freeing internal teams to focus on innovation and business value.

3. Cloud Support – Managed Public Cloud Services

Rackspace Managed Public Cloud Services has been designed to address the specific security, compliance and operational best practice needs of the UK public sector. A fully managed 24x7 service delivered remotely from our UK Sovereign Services centre of excellence and connected to our secure management fabric, so that it can support Microsoft Azure, Amazon Web Services (AWS) and Google Compute Platform (GCP) cloud solutions.

UK sovereign support includes the use of an inclusive suite of industry standard ITSM tools that simplifies operational management, while at the same time maximises security, systems availability and performance.

Service Features

- 24x7 UK-based services across Azure, AWS and GCP
- Monitoring and alerting across IaaS, SaaS and PaaS
- End-to-end incident, problem and event management
- Scheduled patching, updates and configuration maintenance
- Managed DR and backup scheduling, execution and restore support
- Capacity and performance monitoring with proactive tuning
- SLA-driven UK-based service desk and operational support
- Change management, including planning and controlled implementation
- Service reporting, trend analysis and continuous improvement actions
- Platform health checks and lifecycle management

Service Benefits

- Single cloud service provider across Azure, AWS and GCP
- Reduced operational burden through fully managed IaaS, SaaS, PaaS
- Improved availability through proactive monitoring and optimisation
- Reduced risk with ITIL-aligned change, incident and problem processes
- Predictable outcomes through ongoing reporting and service governance
- Increased availability supported by continuous health and performance oversight
- Greater operational consistency through defined maintenance and patch cycles
- Enhanced resilience with managed DR, backup and restore services
- Improved long-term efficiency through continuous service improvement
- Confidence that critical infrastructure is overseen by UK-vetted cloud experts

3.1. Managed Public IaaS

Rackspace Managed Public IaaS provides full operational management of a customer's tenant and infrastructure environment. Delivering end-to-end service oversight, including 24x7 monitoring, incident and problem management, capacity and performance management, patching, backup operations and ongoing platform optimisation. Our teams take responsibility for the health, stability and availability of the environment, coordinating change management, service reporting and continuous improvement activities.

By combining proactive operations with structured governance and clearly defined SLAs, the service ensures predictable performance, reduced operational risk and a consistently high-quality service experience.

3.2. Managed Public SaaS / PaaS

The Rackspace Managed Public SaaS / PaaS delivers a fully governed, secure and operationally managed application, database and platform environment tailored to UK public sector needs. We take end-to-end responsibility for security, performance, lifecycle management and continuous optimisation. This includes monitoring, patching, incident and problem management, capacity oversight, data protection and controlled change processes.

By combining hosting with managed platform services, we ensure predictable performance, improved security posture and reduced operational complexity. Customers gain a resilient, compliant and scalable environment that enables rapid application delivery while freeing internal teams to focus on innovation and business value.

4. Cloud Support – Managed Hybrid Cloud Services

Rackspace Managed Hybrid Cloud Services has been designed to address the specific security, compliance and operational best practice needs of the UK public sector. A fully managed 24x7 service delivered remotely from our UK Sovereign Services centre of excellence and connected to our secure management fabric so that it can support multicloud and hybrid cloud environments. Environments that combine private clouds (on-premises, at the edge and Rackspace sovereign private cloud) and one or many public clouds (Microsoft Azure, Amazon Web Services and Google Compute Platform).

UK sovereign support includes the use of an inclusive suite of industry-standard ITSM tools that simplifies operational management, while at the same time maximises security, systems availability and performance.

Service Features

- Unified 24x7 UK-based services across private and public cloud infrastructure
- 24x7 hybrid IaaS, SaaS, PaaS monitoring and alerting
- Coordinated patching and full lifecycle maintenance
- Managed incident, event and problem response
- Hybrid DR, backup, restore and data protection services
- Performance optimisation across all workload locations
- Capacity monitoring and proactive resource planning
- Controlled change and configuration management
- Security controls and vulnerability management integration
- Monthly service reporting and continuous improvement activities

Service Benefits

- Simplified hybrid operations with unified service management
- Increased reliability through proactive monitoring and response
- Reduced risk via structured governance and controls
- Improved performance across distributed workloads
- Enhanced security with consistent protection everywhere
- Scalability using hybrid cloud resource flexibility
- Strengthened continuity with robust data protection
- Predictable service quality and outcomes
- Internal teams freed to focus on business innovation
- Confidence that service are delivered by UK public sector experts

4.1. Managed Hybrid IaaS

Rackspace Managed Hybrid IaaS delivers fully governed infrastructure operations across private and public cloud environments, providing consistent performance, security and availability wherever workloads reside. We manage all core operational activities, including monitoring, patching, incident response, capacity planning, backup operations and change control.

By integrating private-cloud assurance with public-cloud scalability, the service enables flexible workload placement while reducing operational complexity. Customers benefit from proactive optimisation, unified governance and SLA-driven reliability. This hybrid approach ensures resilient, compliant and high-performing infrastructure that supports evolving business requirements, while allowing internal teams to focus on innovation rather than day-to-day operations.

4.2. Managed Hybrid SaaS / PaaS

Rackspace Managed Hybrid SaaS / PaaS provides fully governed, end-to-end management of applications, databases and platform services across both private and public cloud environments. We deliver unified operational control, including monitoring, incident and problem management, patching, release coordination, performance optimisation and data-protection services across hybrid estates.

By integrating private-cloud assurance with public-cloud scalability, we ensure consistent service quality, compliance and reliability regardless of where workloads reside. This hybrid approach reduces operational complexity, accelerates application delivery, strengthens security posture and provides customers with a flexible, resilient and optimised environment that supports evolving business and regulatory requirements.

5. Cloud Support – Security Services

Rackspace UK Sovereign Managed Security Service provides end-to-end protection, governance and assurance across the full security lifecycle. Delivered entirely within UK jurisdictions by accredited and vetted / security cleared personnel, the service covers strategy development, secure architecture design, incident management, continuous monitoring, threat response, audit readiness, quality assurance and testing. We provide comprehensive oversight of risks, controls, compliance and operational security, ensuring that organisations maintain resilient and defensible environments aligned to UK regulatory and sovereignty requirements.

Through integrated processes, validated tooling and rigorous assurance, the service enhances visibility, reduces risk, improves organisational readiness and enables customers to operate with confidence in a constantly evolving threat landscape.

Service Features

- Continuous monitoring aligned to NCSC security and CAF principles
- Threat detection using government-aligned security controls and tooling
- 24x7 incident response following HMG SPF requirements
- Vulnerability management aligned to NCSC best practice
- Security event analysis with intelligence-led recommendations
- Compliance reporting supporting UK GDPR and NIS obligations
- Governance dashboards mapped to CAF outcomes
- Managed security controls aligned to ISO 27001
- Regular risk assessments using UK public-sector methodologies
- Proactive improvement based on threat and control insights

Service Benefits

- Strengthens defence with continuous, standards-aligned protection
- Reduces risk through proactive threat and vulnerability management
- Ensures compliance with UK public-sector requirements
- Improves resilience with assured incident readiness
- Enhances visibility via dashboards and comprehensive governance reporting
- Supports secure operations across private, public and hybrid environments
- Lowers operational burden on internal teams
- Accelerates detection, response and remediation with expert guidance
- Improves decision-making through clear risk insights
- Maintains trust with consistent, audited security processes

5.1. Security Strategy

The Rackspace Sovereign Security Strategy delivers a clear, evidence-based approach for strengthening organisational security in line with UK government policies, regulatory requirements and national security expectations. The service continuously assesses current organisational risks, capabilities, governance structures and compliance with standards such as NCSC guidance and sector specific regulatory requirements. It defines a target security posture, prioritised roadmap and investment plan that balance operational needs with public-sector accountability.

Through expert advice, architecture recommendations, policy development and actionable improvement plans, the service enhances resilience, supports assurance activities and enables departments to protect sensitive data, services and UK citizens.

5.2. Security Risk Management

Rackspace Sovereign Security Risk Management provides structured, evidence-based oversight of security risks across departmental systems, data and operations. The service identifies, assesses and prioritises risks in line with NCSC guidance, HMG security classifications and applicable legislative requirements. It delivers clear risk treatment plans, governance models and assurance reporting to support accountable decision-making.

Through continuous monitoring, threat evaluation, control validation and expert advisory support, the service ensures risks are understood, managed and escalated appropriately. This enables departments to protect sensitive information, maintain service continuity, meet statutory obligations and strengthen overall resilience within the UK government security framework

5.3. Security Design

Rackspace Sovereign Security Design delivers zero trust architectures that are secure, resilient and scalable to protect sensitive government data and critical services. The service identifies the security requirements, design patterns, controls and assurance approaches needed to support departmental, multi-agency and citizen-facing services. It includes threat modelling, risk-based design decisions, integration of protective measures and validation of proposed architectures against organisational needs. The service ensures systems are designed to prevent, detect and withstand attacks while supporting operational availability and continuity.

By combining expert guidance with structured design governance, it enables departments to deliver secure digital services confidently and effectively across complex hybrid environments.

5.4. Security Incident Management

Rackspace Sovereign Security Incident Management delivers a fully managed capability for identifying, analysing, responding to and recovering from security incidents across the entire technology landscape. The service provides continuous monitoring, rapid triage, coordinated response, containment, eradication and structured recovery activities. It ensures incidents are managed efficiently from detection through to resolution, with clear communication, evidence capture and post incident reviews to drive improvements.

By combining expert analysis, proven processes and actionable reporting, the service reduces operational impact, improves resilience, strengthens organisational readiness and enables teams to quickly restore normal operations, while maintaining confidence in their overall security posture.

5.5. Security Audit Services

Rackspace Sovereign Security Audit Service uses expert security professionals to provide an independent, end-to-end audit of a public sector organisation security controls, processes and governance practices. Reviewing technical, procedural and operational processes, in order to identify gaps, validate compliance and assess overall level of control and security posture. It includes evidence-based testing, documentation reviews, stakeholder interviews, configuration analysis and evaluation of risk management practices. The service delivers clear findings, prioritised recommendations and actionable remediation plans that strengthen assurance and support informed decision-making.

By offering transparent insight into weaknesses and resilience levels, the service helps departments improve security posture and protect critical public services.

5.6. Security Quality Assurance (QA) and Testing

Rackspace Sovereign Security Quality Assurance and Testing ensures that security controls, systems and processes are designed, implemented and are operating effectively across critical public sector environments. The service provides independent validation through structured testing, including functional security testing, configuration assurance, vulnerability assessment and verification of control effectiveness. It evaluates whether solutions meet security requirements, behave as intended and maintain resilience under real-world conditions.

Through detailed reporting, defect analysis and remediation guidance, the service helps departments reduce risk, improve reliability and maintain confidence in service integrity. This ensures secure, high-quality delivery of public services across complex and evolving technology estates.

6. Cloud Support – Cloud Migration Planning

Rackspace Sovereign Managed Cloud Migration Planning Service forms part of our proven cloud migration methodology. Delivering a structured, secure and risk-controlled approach to preparing workloads for migration into a sovereign cloud environment. The service includes a full assessment of current estates, workload readiness analysis, risk identification, data-flow mapping, interdependency evaluation and compliance considerations specific to sovereignty and the UK public sector. It defines the migration strategy, wave plans, landing-zone alignment and target-state architecture required for a seamless, controlled transition.

Expert guidance, detailed planning and clear governance, the service reduces migration risk, accelerates timelines and ensures organisations move to private, public and hybrid cloud confidently, securely and with no unplanned disruption to operations.

Service Features

- Comprehensive discovery and workload assessment
- Migration strategy tailored to sovereign requirements
- Infrastructure, application and data dependency mapping
- Risk analysis with mitigation planning
- Target hybrid architecture and landing-zone alignment
- Security, compliance and sovereignty planning
- Sequenced migration wave planning
- Cost modelling and commercial optimisation options
- Operational readiness and support planning
- Project control, governance, reporting and stakeholder engagement

Service Benefits

- Reduces migration risk through structured planning
- Accelerates time-to-cloud adoption
- Ensures alignment with compliance and sovereign requirements
- Improves cost efficiency and predictability
- Minimises unplanned service disruption during migration
- Ensures operational readiness for cloud
- Provides confidence with expert guidance
- Improves visibility through transparent project control, communication and governance
- Supports long-term cloud strategy development
- Ensures secure, predictable and controlled workload transition

6.1. Capability Analysis

Rackspace Sovereign Capability Analysis service provides a detailed evaluation of an organisation's readiness to adopt cloud. Assessing technical, operational and service capabilities needed to support successful cloud migration. It assesses current skills, processes, tooling, integration maturity and operational readiness across infrastructure, applications, data, security and service management. The service identifies capability gaps, suggests detailed uplift requirements and recommends the structures, competencies and operating models needed for cloud adoption.

By delivering clear insights, evidence-based recommendations and a roadmap for capability development, the service ensures organisations are fully prepared to operate, secure and optimise workloads in a hybrid / cloud environment.

6.2. Enterprise Architecture

Rackspace Sovereign Enterprise Architecture service defines the entire IT landscape architecture required to support a secure, efficient and scalable transition into the cloud. It assesses current architectures, identifies technical debt, maps system interdependencies and establishes the target-state (and any mid-state) architecture needed to enable migration and long-term cloud operations. The service provides reference architectures, integration patterns, data-flow designs and alignment across business, application, data and technology domains.

By delivering architecturally sound, risk-aware and future-ready designs, the service ensures organisations can migrate confidently, maintain operational continuity and optimise their digital estate within a hybrid / cloud environment.

6.3. Cloud Gap Assessment

Rackspace Sovereign Cloud Gap Assessment delivers a detailed evaluation of the differences between a public sector organisation's current IT environment against the requirements of operating in a hybrid / cloud environment. It analyses infrastructure, applications, data / dataflows, security controls, operational readiness to identify gaps that may impact successful adoption. The service produces a clear, prioritised set of remediation actions, target-state recommendations and readiness indicators.

By defining what must change and why, the service reduces risk, accelerates adoption and ensures organisations are technically, operationally and strategically aligned for a smooth transition into the target hybrid / cloud.

6.4. Architecture Options Analysis

Rackspace Sovereign Architecture Options Analysis performs a detailed assessment of a public sector organisation existing IT architecture to determine its readiness for migration into a hybrid / cloud environment. It evaluates application design, integration patterns, infrastructure components, data / dataflows, security controls and operational dependencies to identify security, compliance and performance constraints and opportunities. The service defines the target architecture required to support secure scalable and efficient cloud operations.

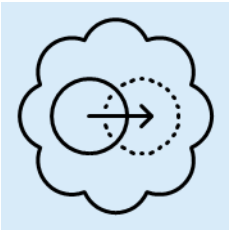
Through clear recommendations architectural patterns and technical guidance, the service reduces design risk and enhances alignment with cloud principles, ensuring organisations can transition into hybrid / cloud with confidence and minimal disruption.

6.5. Delivery Road-Mapping

Rackspace Sovereign Delivery Road-Mapping provides a clear set of expected outcomes and a structured plan that outlines how an organisation will move from preparation into execution. It defines the sequence of migration waves, key milestones resource needs, risk triggers and decision points required for a controlled transition into hybrid / cloud. The service aligns technical activities with business priorities and dependencies ensuring a realistic achievable and well-governed delivery timeline.

Through detailed planning transparent communication and cross-team coordination the Delivery Road-Mapping service reduces uncertainty improves readiness and enables organisations to manage migration activities with confidence predictability and minimal operational disruption.

7. Cloud Support – Setup and Migration



Rackspace Sovereign Managed Cloud Setup and Migration service provides a secure, compliant and expertly-delivered transition to UK sovereign cloud environments. Using UK based migration specialists and best practice methodologies such as PRINCE2 and Agile, the service manages assessment, design, build and migration with rigorous governance and risk control. It ensures data residency, operational resilience and adherence to industry and government standards.

Rackspace delivers fully managed landing zones, secure connectivity, workload modernisation and a structured cutover, enabling organisations to accelerate cloud adoption while maintaining sovereignty, performance and continuity.

Service Features

- Public sector compliant design with strict data residency controls
- PRINCE2-aligned project governance and risk management
- Agile delivery cycles for accelerated migration progress
- UK-based certified project management with cloud and migration specialists
- NCSC aligned secure landing zone build and hardening
- Detailed application, data and infrastructure discovery
- Migration waves sequenced for minimal service disruption
- Modernisation options for apps and workloads
- Continuous compliance and security monitoring
- Fully managed post-migration operations

Service Benefits

- Ensures full UK public sector compliance
- Reduces migration risk through structured control and governance
- Accelerates cloud adoption with predictable delivery outcomes
- Improves security posture and operational resilience
- Minimises downtime during transition
- Lowers TCO via known best practice cloud architecture patterns
- Enhances performance across critical workloads
- Supports continuous regulatory compliance
- Simplifies and reduces cost of ongoing cloud environment
- Underpins immediate and scalable digital transformation

7.1. Data Auditing and Organising

Rackspace Sovereign Data Auditing and Organising service provides a structured approach to preparing public sector data for migration into a hybrid / cloud environment. UK-based specialists analyse the existing data estates to validate integrity, classify sensitivity levels and ensure alignment with any sovereignty and regulatory requirements. The service restructures and optimises datasets to support efficient, low-risk migration while eliminating duplication and addressing quality issues.

Through controlled preparation, clear data mapping and the application of sovereign best practices, organisations gain a clean, well-organised and compliant data foundation ready for seamless transition into their new hybrid / cloud environment.

7.2. Data / Information Structure Design

Rackspace Sovereign Data / Information Structured Design provides a disciplined approach to shaping how data is structured, governed and prepared for use in a hybrid / cloud environment. UK-based specialists define logical and physical data models, establish classification rules and designs secure dataflows aligned to sovereignty, regulatory and organisational requirements. The service creates a clear, consistent and optimised data architecture that supports efficient migration, improves data quality and ensures controlled access.

This structured design enables reliable and predictable workload behaviour in the hybrid / cloud and by doing so establishes a scalable foundation for future data-driven services.

7.3. Engagement and Communication Planning

Rackspace Sovereign Engagement and Communication Planning service ensures stakeholders remain informed, aligned and confident throughout the project. The service uses existing best-practice to define a tailored communication plan that supports governance, manages expectations and maintains momentum during setup and migration activities. UK-based Project Specialists create clear communication plans, stakeholder maps, decision pathways and governance boards to ensure decisions and messages are accurate, timely and relevant.

Through structured engagement, transparent reporting and coordinated communications, the service strengthens collaboration, reduces project uncertainty and enables smooth execution, ensuring all stakeholders understand progress, risks and upcoming actions throughout the project.

7.4. Project Management and Governance

Rackspace Sovereign Project Management and Governance provides structured leadership and control across all stages of setup and migration. Rackspace UK-based Project Managers apply their extensive experience and best practice methodologies, such as PRINCE2 and Agile, to maintain milestone timeline, manage risks and to drive predictable delivery.

The service establishes governance boards and forums, decision pathways, reporting cycles and quality controls that keep stakeholders aligned and ensure the programme remains aligned to the agreed budget, timeline and quality outcomes. Through clear planning, coordinated execution and consistent communication, the service enables a well governed,

transparent and efficient migration journey that delivers outcomes safely, on time and without unplanned disruption.

7.5. Service Optimisation / Right-Sizing

Rackspace Sovereign Service Optimisation / Right-Sizing ensures workloads are efficiently designed for performance, cost and compliance before entering the target hybrid / cloud environment. UK-based specialists analyse workload characteristics, utilisation patterns, future business needs and technical constraints to define optimal resource configurations that balance resilience with efficiency and cost. The service identifies opportunities to streamline architectures, most appropriate buying models (pay-as-you-go, spot, reserved instances etc.), reduce overprovisioning and ensure each workload is matched to the most appropriate hybrid / cloud platform.

By applying these optimisation practices during setup and migration, organisations gain a well-tuned, cost-efficient and scalable cloud foundation that delivers reliable performance and long-term operational value

8. Cloud Support – Ongoing Support

Rackspace Sovereign Ongoing Support provides continuous operational management of public sector organisations' hybrid / cloud environments. It is delivered remotely by skilled Rackspace hybrid / cloud engineers and service specialists from the UK Sovereign Services support centre. It offers a proactive 24x7 managed service that includes monitoring, incident response, patching, vulnerability management, optimisation and configuration management across the hybrid / cloud. Customers will have named UK account team and receive consistent real-time dashboards, self-service portals, service management reporting and access to expert guidance, to ensure their cloud platforms and services remains secure, compliant and well-optimised.

Through structured processes, automation and a dedicated UK public sector support team, the service simplifies day-to-day cloud / hybrid operations, reduces operational risk and ensures workloads run reliably, while supporting ongoing business and transformation needs.

Service Features

- 24x7 services managed by UK public sector specialists
- Proactive monitoring, alerting incident response and resolution
- ITIL-compliant service management
- Performance tuning for critical workloads
- Configuration and policy management
- Automated health and compliance checks
- Cost and resource optimisation reviews
- Service dashboard, monthly reporting with operational insights
- Access to expert hybrid / cloud engineering specialists
- Expert product specialists to support complex issues

Service Benefits

- Improves reliability through continuous expert operations management
- Reduces risk with proactive incident handling
- Enhances security via vendor-recommended review and updates
- Workload performance, security & availability improvements
- Lowers costs through ongoing optimisation
- Ensures compliance with sector-specific and operational standards
- Allows internal resources to focus on business outcomes not IT
- Enables predictable hybrid / cloud operations
- Prevents service disruption with early issue detection
- Supports ongoing transformation and growth

8.1. Product Support Capabilities

Rackspace Sovereign Product Support Capabilities delivers comprehensive operational assistance to ensure hybrid / cloud services run reliably, securely and efficiently. UK-based support specialists provide expert guidance on third party product functionality, configuration, optimisation opportunities and issue resolution across a wide range of cloud and traditional IT infrastructure estates.

The service offers 24x7 support channels, defined KPIs and SLAs, guidance and clear vendor escalation pathways. The service augments the capabilities of existing IT teams, remove unplanned outages and resolve problems quickly.

8.2. Logging and Management of Incidents

Rackspace Sovereign Logging and Management of Incidents provides auditable, compliant and responsive handling of operational incidents. UK-based support teams use ITIL-compliant process to log, triage and manage incidents using defined workflows, ensuring accurate categorisation, prioritisation and rapid response aligned to agreed customer SLAs.

The service delivers UK-based ITSM tools, dashboards, clear escalation paths, timely communication updates and full auditability. Best practice incident management practices minimise service disruption, restore service quickly and provide transparent reporting that enables organisations to maintain stable, secure and resilient hybrid / cloud operations.

8.3. Reporting and Proactive Results Analysis

Rackspace Sovereign Reporting and Proactive Results Analysis provides real-time and continuous visibility and insights into the health, security, performance and compliance of the hybrid / cloud environments. UK-based specialists build customer dashboards and produce structured operational reports, trend analyses and risk assessments that highlight emerging issues and optimisation opportunities. Proactively analysing operational data and identifying patterns before they become problems.

The service maximises availability, strengthens security posture and helps organisations make informed decisions that improve the reliability and efficiency of their hybrid / cloud operations.

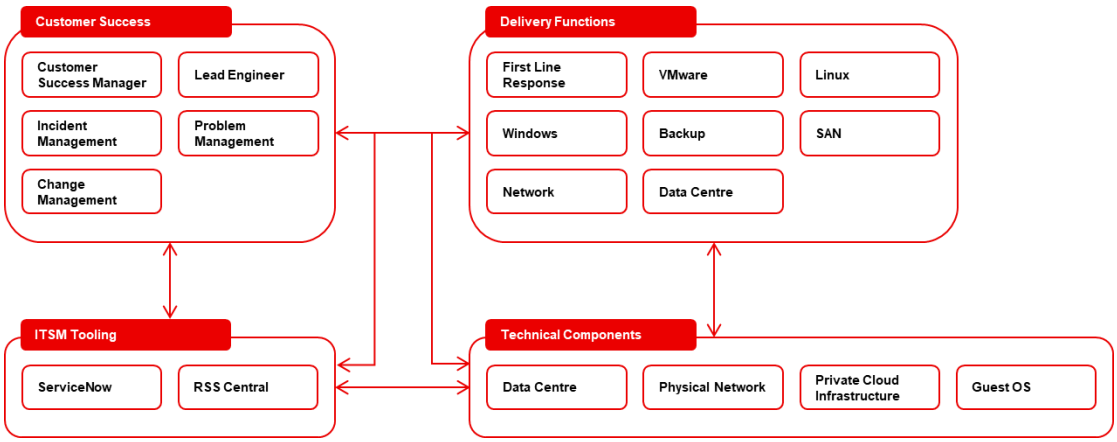
8.4. Dispatch of Service Technicians and/or Parts

Rackspace Sovereign Dispatch of Service Technicians and/or Parts provides controlled, rapid and coordinated response to hardware-related issues affecting hybrid / cloud environments. When requested by the customer, faults are detected or reports incidents require physical intervention, UK-based teams initiate pre-defined and agreed dispatch processes to deliver approved and accredited engineers with the necessary replacement parts to the required location. The service ensures swift restoration of service through controlled logistics, validated components and strict UK Government-aligned handling procedures.

The service minimises downtime, maintains operational resilience and ensures that critical infrastructure remains available and fully supported.

9. Rackspace Sovereign Service Overview

Rackspace Sovereign Cloud is a fully managed solution that aims to reduce the risk, time and costs required for design, deployment, and continued support of a secure private cloud environment. Rackspace Sovereign Cloud is a fully managed solution that aims to reduce the risk, time and costs required for design, deployment and continued support of a secure private cloud environment.



9.1. ITIL-Aligned Service Management

Rackspace Sovereign Cloud in whichever configuration or specific security domain, is delivered as a fully managed solution, designed to allow Rackspace to provide security and compliance assurances to public sector customers. As such, the service management functions are aligned with ITIL best practices and includes the following elements, all dedicated to Rackspace's UK public sector customers:

- UK Sovereign Change Management Team
- UK Sovereign Problem Management Team
- UK Sovereign Incident Management Team
- UK sovereign and secure instance of ServiceNow

The solution also allows for named account management resources to be assigned to oversee the service provision to each customer. This account management team will provide single points of contact for service provision and technical requirements or issues:

- Named Customer Success Manager
- Named Customer Lead Cloud Engineer

9.2. NCSC-compliant Stack

Rackspace Sovereign Cloud provides a templated deployment of a secure-by-design solution that exceeds NCSC guidance for supporting customers working at data classification of UK OFFICIAL, OFFICIAL-SENSITIVE and up to NHS Class V.

Rackspace assures the design of each deployment of Rackspace Sovereign Cloud and Rackspace will maintain every deployment to the security requirements laid out by NCSC. Each customer is separately responsible for conducting its own CHECK / CREST test on its environment, which Rackspace will support and then conduct any remediation work identified as part of the service provision.

9.3. Proactive Operational Management

Rackspace Sovereign Cloud is a fully managed solution and includes several additional service components, when compared to other managed service offerings.

9.4. Network Firewall

9.4.1. Single-Tenant

The customers' dedicated Rackspace Sovereign Cloud is protected by Common Criteria 'PP Compliant' (EAL4+) firewall pairs to provide a hardened boundary within our secure DCs. The firewalls are fully managed by Rackspace to ensure network traffic always follows the pre-defined routing within the environment and that the firewall configuration is maintained to comply with NCSC guidance.

9.4.2. Multi-Tenant

Within the top level of the multi-tenant environments, firewalls that separate the customer domains and customers from each other are physical, multi-tenanted devices deployed to control access. Multiple fail-safes are in place to ensure there is no possibility of cross talk between tenants. The top level platforms are protected by Common Criteria 'PP Compliant' (EAL4+) firewall pairs to provide a hardened boundary within our secure DCs. The firewalls are fully managed by Rackspace to ensure network traffic always follows the pre-defined routing within the environment and that the firewall configuration is maintained to comply with NCSC guidance.

Within each of the customer tenants, a dedicated software firewall is provided as standard (upgradable to a physical device if required), fully managed and pre-templated with EAL4+ standards.

9.5. Security Event Logging (SIEM) / SOC

Rackspace Sovereign Cloud variations include comprehensive security event logging for all elements of the supported environment. Rackspace can provide these logs to the customer's own Security Incident and Event Monitoring (SIEM) solution to support security incident investigation and remediation activities. As part of the service, the SIEM logs are retained for a minimum of 12 months and are available for forensic analysis. As part of an additional costed option, a fully searchable SIEM and managed SOC service is available.

Rackspace can also provide detailed optional administration session recording if required, although this does use customer storage due to the security design of Rackspace Sovereign Cloud; this option will be offered during onboarding.

9.6. Guest OS Support

Rackspace Sovereign Cloud services include full OS management for the customer workloads, covering a wide range of Linux and Windows operating system versions. In some circumstances, Rackspace will provide reasonable endeavours support for OS versions that are no longer in mainstream support, but this will be dependent on the customer taking out extended support options where available.

9.7. Backup and Recovery

Rackspace Sovereign Cloud includes a fully managed backup solution. As standard, Rackspace offers a range of standard backup policies that can be selected as the 'default' policy for the customer workload, or a bespoke policy can be developed during onboarding, if operational constraints dictate. All requested VMs are enrolled for image-level backups as part of the commissioning process.

9.8. Disaster Recovery

Rackspace Sovereign Cloud includes a fully managed Disaster Recovery solution, the product is delivered as default in dual data centres and virtual machines nominated for Disaster Recovery are replicated to the second site. Rackspace Sovereign Cloud includes a fully managed disaster recovery solution; the product is delivered as default in dual data centres and virtual machines nominated for disaster recovery are replicated to the second site. A tiered service is offered based on RTO and RPO requirements, defined during customer onboarding.

9.9. Vulnerability Management

Rackspace Sovereign Cloud includes a comprehensive vulnerability management solution as standard. Rackspace will configure monthly scans, with reports provided as part of the monthly service review. The account Lead Engineer is responsible for managing scans and remediation work, as well as advising the customer on exposure and risk in response to GovCERT or CareCERT alerts, or zero-day vulnerability announcements.

9.10. Anti-Malware Protection

Rackspace uses an enterprise-level, anti-malware protection tool that is automatically deployed to all supported VMs. The tool will deploy an agent to each VM that checks for updates on an hourly basis and can work in isolation should circumstances require. Alerts generated by the service are monitored 24x7, with alerting configured to meet NCSC security monitoring standards. Rackspace will review all alerts and instigate recovery procedures as required, including triggering Rackspace's major incident management process if customer systems are at risk of compromise.

9.11. Workload Monitoring

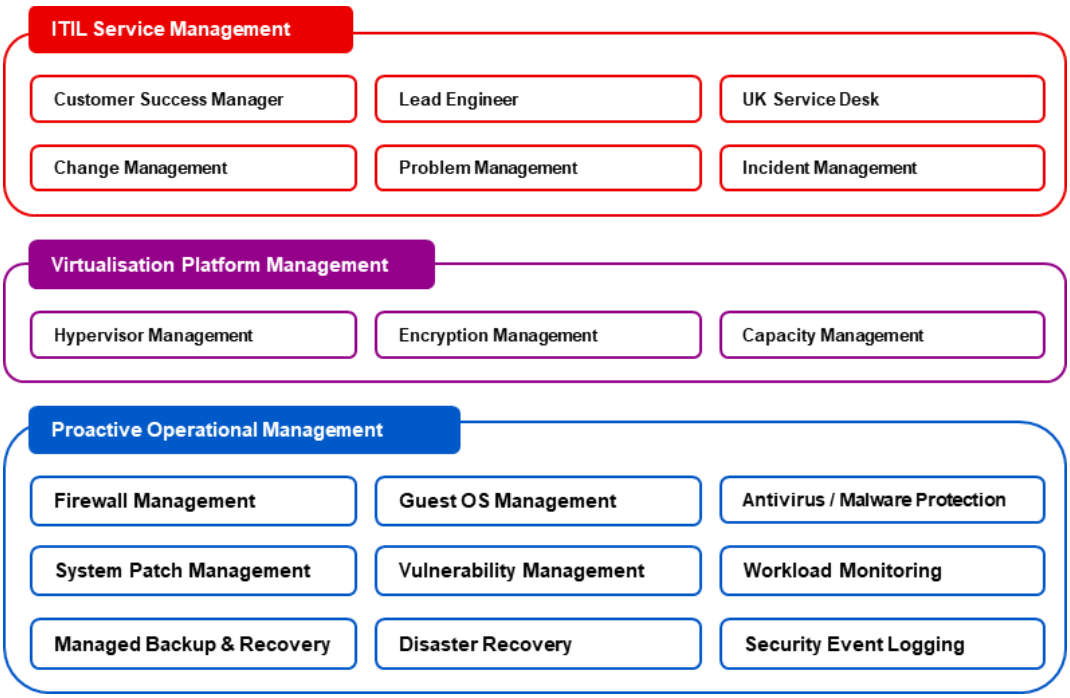
Rackspace Sovereign Cloud includes comprehensive performance and capacity monitoring for the customer workload VMs. Rackspace will deploy a standard monitoring configuration but can support customer-specific configurations if needed. Any change to standard monitoring may incur additional setup costs and on-going management charges.

9.12. System Patching

Rackspace is responsible for maintaining patch levels on all supported elements within the customer workload. Rackspace Sovereign Cloud includes a comprehensive patching solution that can be configured to meet individual customer operational restrictions. As part of on-boarding, Rackspace will work with the customer to design suitable maintenance schedule, making sure that patching does not interfere with critical operations. Rackspace will respond to any critical 'out-of-band' customer patch requests that are driven by NCSC, or vendor alerts, but this may require the waiver on relevant SLAs if deployment timelines mean that standard patch testing cannot take place.

10. Rackspace Sovereign Cloud Managed Services

The following section provides detailed information on the managed service elements provided as part of the Rackspace Sovereign Cloud standard support solution. The individual components of the service are outlined in the diagram below.



10.1. ITIL Service Management

The managed services included in Rackspace Sovereign Cloud are all designed to align with ITIL best practices. As such, there are several distinct components of the solution that will meet public sector customer expectations for an ITIL-aligned service.

10.1.1. Customer Success Manager

As part of the Rackspace Sovereign Cloud managed service, the customer will be provided with a named Customer Success Manager (CSM). This role will be accountable for all aspects of a customer's support during the term of the contract.

The governance model followed by the CSM is designed to achieve the following guiding principles:

- Promotion of trust through transparency and bilateral communication
- Maintaining the strength of the relationship between the customer and Rackspace as a critical success factor for both
- Alignment of both parties' business and IT objectives
- Development of a customer specific runbook to highlight specific operational requirements and details
- Itemising relevant customer service innovation or expansion priorities
- Establishment of a shared organisation and structure to streamline day-to-day management and administration of the outsourcing relationship
- Allowing customer and Rackspace management teams to focus on strategic issues

- Optimising customer and Rackspace expertise to provide the most effective IT Services to Service recipients
- Ensuring overall monitoring of contract performance on service levels, financials, deliverables and customer satisfaction
- Ensuring that potential issues are investigated, resolved and/or, if necessary, escalated

10.1.2. Overall Partnership Governance Structure

The purpose of service delivery governance is to establish effective means for managing the delivery of Rackspace services and innovation as determined by the customer's business objectives. This is a joint framework managed equally by Rackspace and the customer.

The three-tier governance model (Operational, Programme and Strategic) is used to account for priorities, planning, oversight, recommendations and approvals, as well as risk, action, issue and dependency management:

Governance effectiveness is measured throughout the process with a joint scorecard that considers the parties' business objectives narrowed down in terms of IT priorities. The categories and variables are jointly defined by Rackspace and the customer. The joint scorecard is broken into three sections:

- Operational performance as viewed by the services consumer (e.g. line of business / department)
- Innovation and transformation as viewed by the services consumer
- Realisation of innovation and transformation objectives as viewed by the customer Executive Steering Committee

10.1.3. Account Reviews

To provide oversight of the governance of services, the assigned Rackspace CSM will provide regular reviews to analyse the performance of the customer's environment and provide recommendations for service improvements and cost optimisations. This includes recommendations for the use of reserved instances, root causes of alerts and investigation for performance improvements coupled with reporting data from Rackspace system monitoring tooling.

The review may include the following:

- Support tickets
- Monitoring alerts
- Upcoming maintenance events
- Product roadmap updates
- Potential cost optimisation
- Rackspace best practice recommendations
- Recent environment changes
- Upcoming customer events requiring Rackspace support
- Product announcements
- DR test planning

10.1.4. Service Reporting

The account CSM will provide a monthly service summary report, normally within 5 business days of the close of the month. The report pack will include detailed information on the following service areas:

- KPIs, SLAs and response performance
- Analysis of tickets raised in the previous month
- Analysis of open / closed / new problem records
- Backup performance
- Capacity management review and recommendations
- Security incident review
- Security services performance and status
- Platform roadmap
- Service risk register updates
- Service improvement plan updates
- Active project updates

The content and format of the monthly reporting may be altered to suit individual customer requirements, but the standard report package is aligned to ITIL best practices for service reporting.

10.1.5. Lead Cloud Engineer (LE)

The customer account team includes a named Lead Cloud Engineer (LE), a technical expert who will be responsible for managing the Rackspace technical solution and ensuring customer systems are maintained to the required levels. The LE will be familiar with the customer's technical solution and requirements, allowing them to advise on service improvements and to coordinate support responses to customer queries of system issues.

The LE is responsible for oversight and reporting on all aspects of Rackspace's technical solution, including:

- Capacity Management – advising the customer on potential capacity issues and providing effective solutions
- Performance Management – monitoring the performance of the customer's environment, ensuring resources are applied effectively and advising the customer on resolving potential resource issues
- Patch compliance – coordinating patch deployment with the relevant support teams, liaising with the customer on patch deployment plans and reporting on patch compliance for the supported environment
- Vulnerability Management – managing the monthly scans of the supported environment, advising on suitable mitigation or updates to address identified vulnerabilities and providing monthly reports on vulnerability risk across the supported environment
- Change Management – oversight and review of all Rackspace driven changes and for customer changes where they impact Rackspace supported services

10.1.6. Service Desk

Rackspace Sovereign Cloud is supported by a 24x7x365 service desk based in the secure operations building in Cardiff.

The desk provides the following support:

- Monitoring of systems performance and responding to alerts
- Monitoring of A/V solution and responding to alerts
- Telephone support for customer incident logging
- Triage of incidents and creation/assignment of support tickets
- First line support for customer issues
- Coordination of second- and third-line support activities
- Maintenance of customer runbooks and service-specific operation guides

The Sovereign Government Cloud service desk also manages the Sovereign Services ITSM tool, a UK-hosted instance of ServiceNow which is dedicated to Rackspace's UK sovereign & public sector customers. Access to the ticketing tool is controlled by the government operations team and is subject to staff being UK based and having obtained the relevant security clearances.

10.1.7. Change Management

Rackspace Sovereign Cloud standard service includes a dedicated and UK sovereign and security cleared change management team, responsible for all Rackspace generated changes that affect the customer's supported environment.

Rackspace's change management team will provide the following:

- Management of all Rackspace logical and physical changes to the supported customer environment
- Provide 24x7x365 change management support
- Defined standard and emergency change processes, including escalation / approval paths for out-of-band or emergency changes
- Participation in the customer's change advisory board (CAB) to present Rackspace changes as required
- Full support for customer driven changes, where they impact Rackspace support operations
- Cooperate with any third parties to deliver externally driven changes on the supported environment platform
- Agreed maintenance windows and change freeze periods to minimise impact to customer operations

While agreed maintenance windows are preferred, all Rackspace driven changes will be subject to customer approval and will be scheduled in conjunction with the customer to minimise impact wherever possible.

Rackspace's Change Management team will provide regular reporting on change implementation success and failure, as well as managing a forward schedule of change to meet the customer's operational requirements.

The customer is expected to fully participate in the Rackspace change management process to ensure changes are dealt with efficiently. The Rackspace Change Management team will liaise fully with the relevant customer change team but will expect the customer to:

- Provide advance notice to Rackspace of:
  - Proposed change freezes, which are times when no changes can be made to the customer environment
  - High-priority, business-driven events
  - Any other of the customer's operational factors that impact the scheduling of change implementation
- Agree exceptions to change freezes, high priority business driven events and any other than the customer's operational factors that impact on the scheduling of change implementation
- Participate in change advisory board (CAB) and emergency change advisory board (ECAB)
- Participate in post implementation reviews for all large-scale or high-risk changes

10.1.8. Problem Management

The Rackspace Sovereign Cloud managed service includes a problem management process, with dedicated problem managers assigned to identify the root cause of incidents. Where applicable, the problem manager raises change requests or known errors, as required and manages them through to a permanent resolution of the identified issue.

Rackspace problem management for Rackspace Sovereign Cloud will:

- Implement ITIL best practice approach to problem management
- Assign a member of the account team to act as a problem manager
- Chair monthly (or more frequent as agreed by both parties) joint problem management forums with the customer incident and problem management team
- Document actions as tickets on the UK sovereign ServiceNow ITSM tool
- Proactively analyse problem records, identify trends and recommend and/or implement service improvements
- Work with the LE to conduct proactive technical reviews and provide recommendations for potential service improvement at the regular service review meetings
- Create a known error database to support the problem management function
- Monitor and report updates to the known error database
- Add known errors to the customer runbook

The customer is required to engage with the Rackspace Problem Manager to:

- Provide resource to assist in the coordination of a problem management investigation and co-ordinate actions with its third party suppliers Provide resource to assist in the coordination of a problem management investigation and coordinate actions with its third party suppliers
- Provide points of escalation for the Rackspace Problem Manager

10.1.9. Incident Management

Rackspace provides incident management across all aspects of the Rackspace Sovereign Cloud solution. Minor incident management is a separate responsibility of the service desk team leader. A dedicated Incident Manager will be assigned in the event of a major incident, or on the request of the customer if an incident is seen as critical to the maintaining business operations.

The Rackspace fully managed service for Rackspace Sovereign Cloud will:

- Provide incident management 24x7x365
- Provide 24x7x365 technical support available via telephone
- Log incidents raised by telephone
- Establish incident management escalation paths to either the customer or any nominated third parties
- Investigate the incident following Rackspace incident management processes
- Prioritise incidents based on a pre-agreed customer priority and impact matrix
- Review incidents to identify trends and areas of continuous service improvements
- If applicable, monitor, maintain and report on incident backlogs
- Manage and track incidents through to resolution
- Review instructions on the customer account (documented via the account runbook and account management guidelines)
- Collaborate with the customer and any nominated third parties
- Communicate regularly with the customer throughout the incident, detailing findings and actions taken
- Escalate the incident at any time until resolution is achieved
    - This escalation may be hierarchical (to a more-senior engineer or the Customer Success Manager) or functional (involving specialised technical expertise from other functional groups or partner cloud teams)

Where an incident causes a significant business impact, it is classed as a major incident. The following is a non-exhaustive list of occurrences Rackspace classifies as major incidents:

- Total loss of service, such as the failure of a major site or data centre application, at critical times
- Significant degradation of the delivered service or a major element thereof
    - For example, loss of a critical application or a major degradation to system functionality, such as a slow network or system response
- Incident severely affecting the business
- Risk to the customer or Rackspace (such as a suspected or actual loss of data, security)

For major incident management, Rackspace will:

- Provide major incident management 24x7x365
- Deliver ITIL best practice approach to major incident management
- Assign a Major Incident Manager in the event of an incident
- Escalate to nominated customer personnel or third parties in the event of an incident
- Escalate to relevant technology or service vendors in the event of an incident
- Implement a three-tier major incident management communications strategy
- Resolve incidents or provide the customer with acceptable workarounds as soon as feasible

- Advise of any commercial implications prior to implementation of any workarounds to resolve incidents
- Provide root cause analysis (RCA) reports within 10 business days of major incident resolution

The customer is expected to play an integral part of incident management. Rackspace will work with the customer on all aspects of incident resolution but does require the customer to be proactive in raising a major incident.

In the event of a major incident, the customer should:

- Notify Rackspace via telephone as soon as an incident is identified
- Invoke the major incident process based on incident criteria agreed during the onboarding process

Management of incidents is handled with the restoration of affected services as the primary objective. Rackspace endeavours to restore normal service as quickly as possible when a problem or incident occurs. To assist this aim, the customer must not unreasonably disagree with changes that are proposed to resolve the incident.

Rackspace will apply the following consistent approach to all incidents:

- All incidents will be logged in tickets accessible via the dedicated UK sovereign public sector ServiceNow portal
- Rackspace support teams will investigate the incident in accordance with the severity level once logged
- Support suitable escalation of response priorities should a customer encounter a performance-impacting incident
    - Incidents logged with a specific priority are not changed to another priority without the agreement of all parties involved
- Review instructions on the customer's account as a 'first step' investigation of the incident
- Collaborate with the customer, as well as with any third parties the customer nominates as technical contacts to resolve the incident
- Ensure relevant support teams communicate regularly with the customer throughout the incident, detailing their findings and any actions taken
- If a Support Engineer is unable resolve an incident, he or she may escalate the incident at any time until resolution is achieved
    - This escalation may be hierarchical (to a more senior engineer) or functional (involving specialist technical expertise from other functional groups or from the vendor)

The action required to resolve an incident may vary depending on investigative findings. In some cases, a proposed solution may be complex or cause additional disruptive impact to the customer's environment. In these cases, the incident is handled as a change through the Rackspace change management process and the customer is consulted to determine the time window during which the solution or change may be implemented. Alternately, the customer may be required to take action to resolve the incident, which is communicated should such need occur.

An incident will be deemed closed only when the customer confirms that it is resolved. This is normally achieved through the incident ticket being set to "Solved" status. At this point the customer may agree to close the ticket or respond with feedback if further work is required.

10.2. Platform Management

10.2.1. Hypervisor Management

Rackspace Sovereign Cloud deploys either a fully dedicated or shared multi-tenant infrastructure and environment for each customer. The deployment is built to meet NCSC and vendor guidance for securing data at UK OFFICIAL.

The hypervisors and consoles are fully managed by Rackspace, with no customer access. Monitoring is in place and support is provided by a dedicated UK sovereign 24x7x365 service desk initially, escalating to virtualisation teams as required.

10.2.2. Encryption Management

Tooling, services and agents within the customer estate are configured as default to perform data encryption in transit.

All data is stored on the dedicated customer SAN. Data encryption at rest is enforced using encrypted disks that are encrypted as default and managed by the SAN controller modules. Data at rest encryption is validated and certified to FIP140-2 standards and meets, or exceeds, NCSC and NHS Digital guidance on protecting data at rest.

10.2.3. Capacity Management

Capacity management of the customer's Rackspace Sovereign Cloud physical stack will be reviewed by the Lead Engineer on a case-by-case basis, as reporting and monthly service reviews require. The Lead Engineer will advise the customer on options to maximise performance and cost benefits throughout the contract by conducting regular analysis of the system monitoring and monthly report data.

10.3. Proactive Operational Management

As Rackspace Sovereign Cloud is a fully managed solution and includes a wide range of support functions that would be additional cost options by other service providers. The reason Rackspace includes these additional functions is twofold:

- To meet the higher expectations of public sector customers without complicated and costly service add-ons
- To allow Rackspace to provide comprehensive assurance statements on compliance to the NCSC 14 Cloud Security Principles

10.3.1. Firewall Management

Rackspace Sovereign Cloud deploys a fully managed firewall pair on both the primary and secondary site.

The customer may request changes to the firewall, as part of application development, but all changes will be implemented by and subject to security review by Rackspace.

10.3.2. Guest OS Support

As part of the fully managed service, Rackspace will provide full guest Operating System support that includes the following areas:

- Provisioning of new VMs
- Hardening of VM builds to approved standards
- Encryption (provided via SAN encryption)
- Patching of all supported OSs
- Administration of VMs including routine preventative maintenance, troubleshooting and incident investigation

10.3.3. Provisioning

Rackspace Sovereign Cloud includes an automatic VM tooling provisioning function that ensure all VMs are created and tooling applied before being presented for use. Firstly, a VM is created, the patch tooling is applied and the VM enrolled into the relevant customer tenant.

Once registered, the patching tool will automatically deploy all relevant patches for the running OS and scan to ensure all patches are applied correctly; this may require several restarts of the VM, which is carried out automatically. When all relevant patches are applied, the patch tool will deploy monitoring and anti-virus agents to the VM. The agents automatically register the VM with the relevant central servers, apply customer-specific configurations (if required) and then download any updates that are available.

The VM is not made available for use until all security and monitoring agents are installed and working correctly. As soon as the VM is made available it becomes visible to the central vulnerability scanning tool and is automatically registered in the customer tenant on the service and is made available on the scanning console.

10.3.4. Encryption

Tooling, services and agents within the customer estate are configured as default to perform data encryption in transit.

All data is stored on the dedicated customer SAN. Data encryption at rest is enforced using encrypted disks that are encrypted as default and managed by the SAN controller modules. Data at rest encryption is validated and certified to FIP140-2 standards.

10.3.5. Patching

Regular and out-of-band patching is a standard offering for all supported OS versions.

10.3.6. Administration

Rackspace Sovereign Cloud includes comprehensive guest operating system support, a continuous service that includes all aspects of OS maintenance and troubleshooting. Rackspace engineers will constantly review server statuses and proactively investigate any issues before they cause an impact or outage.

The customer Lead Engineer may also direct engineers to conduct preventative maintenance under standard changes to ensure efficient running of the customer's workload.

The customer will retain management responsibilities for user access account requests. Rackspace will comply with customer account request processes to comply with the customer ISMS requirements. Rackspace will not be held accountable for any service impacts caused by delays in approving access account requests.

10.3.7. Anti-Malware Protection

As part of onboarding, Rackspace will deploy a fully tenanted, enterprise-grade endpoint protection service to protect all customer VMs under Rackspace management.

Rackspace will provide a fully managed anti-malware service that is monitored 24x7, including:

- Ensuring anti-malware protection is configured to vendor recommendations, including standard exceptions as recommended by vendors for individual OS versions
- Agents are deployed automatically during VM provisioning:
  - Realtime scanning enabled for read / write activity
  - Full system scans scheduled on a weekly basis
- Monitor and alert on malware detections as per NCSC Security Monitoring guidance:
  - 3 instances of the same malware within 5 mins across all managed devices
- Remedial work to address malware detections that are unable to be cleaned or quarantined
- Monitor installed agents for availability and recovery
- Automatic update of endpoint agent software and anti-virus patterns – checked on 4-hourly basis
- Monthly reporting of endpoint protection performance

Rackspace will work with the customer to implement recommended scan exceptions required as part of customer application onboarding.

10.3.8. System Patch Management

During the customer onboarding process, Rackspace will discuss suitable patching schedules and maintenance windows to minimise impact to the customer's business.

Once a patching schedule is agreed, Rackspace will:

- Configure the central patching service to provide patching support for supported guest operating systems following agreed schedules
- Provide ongoing support in the form of:
  - Scheduling changes
  - Responding to failed patch / update runs
  - Optional patching reviews

- Provide support for out-of-band patches as defined by software vendors, NCSC GovCERT alerts or NHS Digital CareCert alerts, applied in agreement with the customer security team
- Provide monthly patch compliance reports (included in monthly service report pack)

Patch jobs are created automatically each month but are locked until reviewed by Rackspace engineers. Once a patch run is cleared for deployment, the support team will log a change for approval via the change management process. The actual patch job is only released once the monthly patch change is approved.

The customer can request a delay to patching if there are critical business operations that cannot be stopped or re-scheduled. In these cases, the customer security authority must formally approve the change in patch deployment and agree a new date for the affected systems to be patched.

Rackspace will not patch middleware or customer applications due to the potential of harming the customer's environment when not thoroughly tested in its specific environment. Rackspace will support customer requests to apply specific hot fixes or service packs to customer-supported software, but the customer must accept all associated risk.

10.3.9. Vulnerability Management

Rackspace Sovereign Cloud includes a fully tenanted, enterprise-grade vulnerability management service to protect all customer VMs under Rackspace management. The service will be used primarily by the customer Lead Engineer to ensure all supported VMs are maintained correctly and that any vulnerabilities are addressed as quickly as possible, or suitable mitigation controls are implemented while updates are coordinated with the customer.

Rackspace will provide a fully managed vulnerability management service including:

- Monthly scans of Rackspace supported VM workload
- Monthly scan reports included in service review pack
- Remediation plans for OS vulnerabilities detected on Rackspace supported VMs
    - Rackspace will provide advice on suitable risk mitigation plans if updates are not possible due to operational constraints
- Notification of software vulnerabilities detected in customer supported middleware and applications running on Rackspace supported VMs
- Risk assessment of zero-day vulnerabilities with full reporting showing exposed systems

Rackspace can offer extended scans on non-supported elements of a customer's network, but this service will be subject to agreement and additional service charges.

10.3.10. Backup and Recovery

Rackspace Sovereign Cloud offers multiple standard backups, varying retention, off-site and immutability options. These image-based backups are non-intrusive and provide customers with the ability to restore an entire virtual machine or individual files from the backup image. Where file level backups are required, agent-based backup is also available.

Should a backup job fail to complete, the issue will be escalated to the Rackspace support teams to investigate as required. If a customer requires data restored from an image-level backup, the customer must raise a restore ticket with the Rackspace service desk.

Restore requests must provide detailed information regarding the VM instance and to what VM that snapshot should be attached. Rackspace will only restore an image-based backup to a new server and the customer will be responsible for validating any restored data and moving it into relevant applications. Rackspace recommends that customers regularly test restoration as part of normal business continuity planning.

The monthly account service review reports include sections showing backup activity, the details included fully meet the recommended monitoring levels as laid out by the NCSC Security Monitoring guidance. Additional reports can be produced if required but may incur additional costs to set up; details can be discussed with the customer at point of engagement.

10.3.11. Disaster Recovery

The Rackspace Sovereign Cloud solution includes a disaster recovery solution that replicates VMs to the secondary site. During customer onboarding, agreement will be needed on the tiered RPO & RTO requirements for the customer's operational needs, as well as which VMs require DR replication.

Replicated VMs are added to DR if specified at build time. DR also includes a pre-set up secondary site with all routing, security elements already in place along with a redundant firewall pair provided as part of the Rackspace solution.

Rackspace will support an annual DR test, as part of the standard service wrap and will coordinate activity with the customer to ensure testing meets customer requirements and compliance. The account Customer Success Manager (CSM) will discuss timetables for testing with the customer service management team and will be responsible for raising all necessary change control tickets.

Joint communications will be agreed during the monthly service review meetings; the customer service management team is responsible for obtaining all relevant business permissions for testing to take place.

After the annual DR test, Rackspace will support a 'lessons learnt' review with the customer and update the customer runbook to reflect the outcome of this analysis.

10.3.12. Security Event Logging

Rackspace Sovereign Cloud solution design allows for all relevant system and application logs to be pushed to a customer's existing SIEM solution, although this will require individual service configuration changes and may be subject to additional charges.

11. Roles and Responsibilities

The customer retains responsibility for the annual accreditation CHECK testing of its environment and workload. Rackspace will provide support for the customer's annual accreditation testing as part of the standard service.

It is anticipated that there are two parties involved in supporting the Rackspace Sovereign Cloud environment, specifically:

- Rackspace UK Sovereign Support team*
- Customer (including any in-house IT resources)

* Rackspace may include additional resources from the wider company if required, subject to approval from the customer.

The RACI model includes the following roles and relationships:

- **Responsible (R)** means, for the purposes of the RACI matrices, the person who carries out the process or task assignment and is responsible to get the job done
- **Accountable (A)** means, for the purposes of the RACI matrices, the person who is accountable for the process or task being completed appropriately
- **Consulted (C)** means, for the purposes of the RACI matrices, people who are not directly involved with carrying out the task, but who are consulted and may be a stakeholder or subject matter expert
- **Informed (I)** means, for the purposes of the RACI matrices, those who receive output from the process or task, or who have a need to stay informed

The following table outlines the service relationships (roles and responsibilities):

Service Component	Rackspace	Customer
Account Service Management		
Provide named Customer Success resource	R, A	C, I
Provide named technical Lead Engineer resource	R, A	C, I
Agree standard service reporting content and format	R, A	C, I
Agree standard account reporting on service tools	R, A	C, I
Monthly service review meetings	R, A	C, I
Identify opportunities for cost and performance optimisation	R, A	C, I
Provide opinions and best practices around account architecture, security and resiliency	R, A	C, I
Customer runbook development	R, A	C, I
Service Desk		
24x7x365 service desk availability for customer incidents	R, A	C, I
Monitoring of alerts from management tooling	R, A	C, I
Initial response, escalation and troubleshooting of alerts on customer applications	C, I	R, A
Incident escalation management	R, A	C, I
Customer runbook maintenance	R, A	C, I
Change Management		
Review of Rackspace changes to supported environment	R, A	C, I
Review of customer changes to supported environment	C, I	R, A
Change ticket management	R, A	C, I
Change approval board management	R, A	C, I
Forward schedule of change management	R, A	C, I
Change ticket reporting	R, A	C, I
Failed change review and analysis	R, A	C, I
Problem Management		
Incident investigation	R, A	C, I
RCA analysis	R, A	C, I
Known error management	R, A	C, I
Issue workaround management	R, A	C, I

Process / service change management	R, A	C, I
Problem record management and reporting	R, A	C, I
Incident Management		
Initial incident notification – customer driven	C, I	R, A
Initial incident notification – service alerting	R, A	C, I
Incident ticket logging and management	R, A	C, I
Incident review and assessment	R, A	C, I
Incident recovery management	R, A	C, I
Emergency change management	R, A	C, I
Hypervisor Management		
Build and deployment of environment	R, A	C, I
Configuration and management of hypervisor security	R, A	C, I
Annual testing of environment and customer workload	C, I	R, A
Encryption Management		
Implementation of NCSC encryption protocols for SAN	R, A	C, I
Management of encryption keys	R, A	C, I
Annual testing of encryption protocols	C, I	R, A
Capacity Management		
Deployment of monitoring agents and initial configuration	R, A	C, I
Modification of standard capacity alerting to customer requirement	R	A, C, I
Monitoring of capacity alerts	R, A	C, I
Responding to performance / capacity alerts	R, A	C, I
Monthly capacity reporting	R, A	C, I
Review of capacity and performance data	R, A	C, I
Recommendations on performance / capacity changes	R, A	C, I
Firewall Maintenance		
Rule change request – customer driven	C, I	R, A
Customer change review and approval	R, A	C, I
Rackspace rule change request review by security architect	R, A	C, I
Implementation of approved rule changes	R, A	C, I
Firewall OS update management	R, A	C, I
Quarterly rule review and remediation	R, A	C, I
Guest OS Management		
Secure build image management	R, A	C, I
New VM request	C, I	R, A
VM provisioning management	R, A	C, I
UAT on new VMs	C, I	R, A
Guest OS patch management (see below)	R, A	C, I
Monthly vulnerability scan remediation work	R, A	C, I
Anti-malware Protection		
Initial creation of customer tenant	R, A	C, I
Deployment of NCSC approved protection and alerting configuration	R, A	C, I
Request application exceptions	C, I	R, A
Request modified malware alerting levels (may incur charges)	C, I	R, A
Review of configuration changes	R, A	C, I
Implementation of configuration changes	R, A	C, I
Alert response and remediation	R, A	C, I
Monthly anti-malware status reporting	R, A	C, I
System Patch Management		
Initial creation of customer tenant	R, A	C, I
Deployment of patching agents	R, A	C, I
Implementation of virtual patching function (if selected)	R, A	C, I
Agreement on customer-specific patching schedule	C, I	R, A
Implementation of patching schedule	R, A	C, I
Review of released patches	R, A	C, I
Creation of monthly patch jobs	R, A	C, I
Patching change submission	R, A	C, I
Patch run initiation	R, A	C, I
Monthly patch compliance reporting	R, A	C, I
Vulnerability Management		
Initial creation of customer tenant	R, A	C, I
Deployment of agents and creation of scan database	R, A	C, I
Scheduling of monthly scans	R, A	C, I
Creation of customer-specific scans (additional costed option)	R, A	C, I
Monthly scan reviews	R, A	C, I
Scan remediation planning and management	R, A	C, I
Vulnerability risk assessment and mitigation design	R, A	C, I
Monthly vulnerability compliance reporting	R, A	C, I

Workload Monitoring		
Initial creation of customer tenant	R, A	C, I
Configuration of account-specific alerting	R, A	C, I
Deployment and management of monitoring tool and agents	R, A	C, I
Configuration of any customer application alerts (chargeable)	R, A	C, I
Backups and Recovery		
Customer onboarding and configuration of backup services	R, A	C, I
Management of standard VM backup policies and schedules	R, A	C, I
Development of customer-specific backup schedules	R, A	C, I
Monitoring and remediation of backup failures	R, A	C, I
Verification of validity of backup data and methodologies	C, I	R, A
Backup restoration testing	C, I	R, A
Backup restoration request	A	R, C, I
Disaster Recovery		
Design of DR / BCP strategy and creation of a disaster recovery plan	C, I	R, A
Design of DR replication architecture	R, A	C, I
Configuration of replication services	R, A	C, I
Configuration of replication virtual appliances	R, A	C, I
Emergency failover using pre-configured recovery plan	R	A, C, I
Perform ad-hoc DR “test failover” service	R, A	C, I
Application failover testing following DR test failover	C, I	R, A
24x7x365 incident response for DR replication issues	R, A	C, I
Security Event Logging (On Request)		
Implementation of customer-specific logging requests	R, A	C, I
Provision of logs to customer SIEM	R, A	C, I
Configuration of session recording (if selected)	R, A	C, I

12. Appendices

12.1.1. Appendix A: Service Elements

Standard Sovereign Support delivers a fully managed and inclusive service for secure and compliant public sector workloads.

The following table details the various support elements that are included in the standard support model for Rackspace Healthcare Government Cloud. The table also includes details of additional services available at an additional charge.

Service Element	Standard Support	Chargeable Options
ITIL-Aligned Service Management		
Named Customer Success Manager A named Customer Success Manager to serve as the primary point of contact for any service-related issues or requirements; works with your service management team to review service performance in regular reviews.	✓	
Named Lead Engineer A named technical resource manager with detailed understanding of your environment to assist in resolving technical issues and provide advice on system improvements; also participates in your change advisory boards and service reviews.	✓	
Service Desk 24x7x365 service desk with direct access to Rackspace support engineers to support escalations for incidents, using customer-specific support runbooks.	✓	
Change Management ITIL aligned change management processes with 24x7x365 access to Rackspace support engineers to manage configuration changes for your environment.	✓	
Problem Management ITIL aligned problem management of recurring incidents to remediate underlying issue.	✓	
Incident Management 24x7x365 service desk with direct access to Rackspace support engineers to manage the identification and remediation of issues from monitoring alerts.	✓	
24x7x365 Infrastructure Management Rackspace engineers available 24x7x365 for configuration, monitoring and ongoing management of your infrastructure.	✓	
Environment Management		
Deployment of New Environment NCSC-assured environment deployed by UK sovereign and security cleared build engineers using CIS and configurations.	✓	
Encryption Management Implementation and ongoing management of storage encryption to NCSC recommended encryption standards.	✓	
Capacity Management Regular review of environment capacity performance with reporting and recommendations on improvements provided via the account LE.	✓	
Proactive Operational Management		
Firewall Build and Deployment Deployment and implementation of a PP Compliant (EAL4+) firewall pair, using CIS build standards and incorporating all standard rulesets required for supporting the base environment.	✓	
Firewall Management Fully managed support for the deployed firewalls, including regular rule reviews	✓	

and OS patching as recommended by the vendor.		
Guest OS Management		
Hardened VM Images All supported OSs hardened to NCSC-compliant levels and maintained to ensure continued compliance (for 'greenfield' VMs only).	✓	
Automatic VM Tooling Enrolment VM creation and ensuring all new servers are deployed with all tooling before release for use.	✓	
Red Hat Enterprise Linux Support Instance creation, deletion and management of Red Hat Enterprise Linux OS.	✓	
CentOS Support Instance creation, deletion and management of CentOS OS.	✓	
Debian Support Instance creation, deletion and management of Debian OS.	✓	
Ubuntu Support Instance creation, deletion and management of Ubuntu OS.		✓
Windows Server Support Instance creation, deletion and management of Windows Server OS.	✓	
Anti-Malware Protection		
Fully Managed Endpoint Protection Automatic deployment of comprehensive endpoint protection agents on all managed VMs.	✓	
Host-based Intrusion Prevention Service (HIPS) Additional protection to prevent suspicious activity within the host VM OS, sometimes called 'virtual patching'. Requires additional configuration and management so is subject to an additional support charge.		✓
Anti-Virus Reporting Comprehensive alerting and reporting on the performance of the endpoint protection service, based on NCSC security monitoring guidance.	✓	
System Patch Management		
Fully Managed Update Management Automatic enrolment in OS-level patching for all VMs.	✓	
Patching Errors Troubleshoot patching errors.	✓	
Modifying Patch Schedules Modify patch schedules to meet customer operational requirements.	✓	
Modifying Maintenance Windows Modify maintenance windows as requested.	✓	
Patch Compliance Reporting On-demand report of patch compliance detail.	✓	
Patch Compliance Issues Remediation of patch compliance issues.	✓	
Custom Pre- or Post-Scripts Create custom pre- or post-scripts to apply before and after patching.		✓
Vulnerability Management		
Vulnerability Scanning Regular scans of the customer environment to identify vulnerabilities and assign remedial work to relevant support teams.	✓	
Vulnerability Remediation The account LE will coordinate any remediation work resulting from monthly scans and report on progress during the service review meetings.	✓	

Vulnerability Assessment The account LE will review applicable vendor notifications and provide an assessment on risk and recommendations for relevant mitigation where fixes are not available.	✓	
Workload Monitoring		
Workload Monitoring Automatic deployment of monitoring agents to all workload VMs with customisable alerting for performance levels and capacity management.	✓	
Monitoring Configuration Initial configuration of Rackspace standard monitors for incident ticket creation.	✓	
Backup and Recovery		
Backup Schedules & Retention 14 day retention as standard unless agreed otherwise with option to design specific schedules to meet customer demands.	✓	
Backup Service Enrolment New VMs requiring backup will be added to customer backup schedule before release for use.	✓	
Backup Recovery Fully managed recovery of failed backups with alerting and reporting.	✓	
Disaster Recovery		
Automatic Replication Dual environments with full replication to ensure availability of services.	✓	
Fully Managed Failover Dual-redundant platform design with managed failover of services in the event of issues with primary environment.	✓	
Security Event Logging		
NCSC-compliant logging All services deployed with logging and alerting configured to meet NCSC guidance on Security Monitoring.	✓	
Flexible Log Management Logs can be provided in multiple formats and re-directed to customer SIEM solutions as part of onboardings. (Rackspace does not offer managed SIEM service for customers.)		✓
Session Recording Rackspace engineer support sessions can be recorded and stored for analysis in the event of an incident. Utilises customer storage so will incur additional storage overhead, plus charges to cover the initial configuration and ongoing management.		✓
SOC Service Fully UK Sovereign 24x7 SOC service, available in Bronze, Silver & Gold versions.		✓

12.2. Appendix B: Public Sector Connectivity

If required, Rackspace is able to support customer connectivity to major UK public sector networks.

12.2.1. Health and Social Care Network

Rackspace has partnered with BT, an NHS Digital approved, HSCN consumer network service provider (CN-SP), to implement a 10Gbps connection to the HSCN with the ability to provide secure access from Rackspace's UK data centres.

BT will contract directly with customers to provide an accredited connection, Rackspace will provide a fully managed support wrap that will include liaising with BT on the customer's behalf, managing all changes to HSCN service routing and maintenance of connectivity across the Rackspace core network.

12.2.2. Public Services Network

Rackspace has over 10 years' experience in supporting customers requiring PSN access. Rackspace's secure management environment, RSS Central, is maintained to PSN Service Provider standards, which allows us to support any customer that wishes to offer services over the legacy PSN network.

While the PSN is now deprecated in the most part, Rackspace can still provide accredited PSN links into our main UK data centres, in conjunction with our global communications partner.

13. Social Value

13.1.1. Kickstart Economic Growth

At the core of every Racker is a drive to leave the world better than we found it. Our commitment to kickstarting economic growth takes many forms:

Community Donations and Support

- Donated over 1,500 computer monitors, 2,000 chairs and hundreds of desks to local charities and schools during our headquarters relocation
- Provided 168 refurbished laptops to community and educational partners
- Donated more than 1,200 devices to the Turing Trust, helping educate 10,000 people in Africa and bridging the digital divide
- Fed 500+ San Antonio families through our Thanksgiving Food Drive
- Rackers donated $18,000 to global food banks in 2024
- Raised $5,800 for flood relief in Kerr County, Texas and provided 275 pounds of food and over 100 pounds of cleaning supplies for relief efforts

Rackspace Foundation

Since its founding in 2009, the Rackspace Foundation has raised over $8 million and supported more than 10,000 students in underserved schools near our global headquarters in San Antonio. The Foundation takes a 'place-based' approach to community investment, providing holistic support including academic programs, enrichment activities and family engagement in our adopted schools.

We also support global STEM education through partnerships with Code.org, FIRST Robotics and the 1,000 Dreams Fund.

Delivery of our services also contributes to kickstarting economic growth through productivity improvements, supporting innovation and strengthening supply chains. Rackspace enables customers to adopt digitally optimised, consumption-based solutions. This helps improve business efficiency and reduces operational overhead. We encourage new technology adoption and such as AI and have a responsible, transparent supply chain governance.

13.2. Make Britain a Clean Energy Superpower

At Rackspace Technology, sustainability is a long-term priority that shapes how we think, build and support our customers. Our environmental strategy is straightforward: we aspire to give more than we take from our planet and support innovative technologies that drive positive change in the energy industry. We achieve this through renewable energy initiatives, conservation efforts and advocacy, as outlined in our Environmental Policy.

Progress on Our Journey

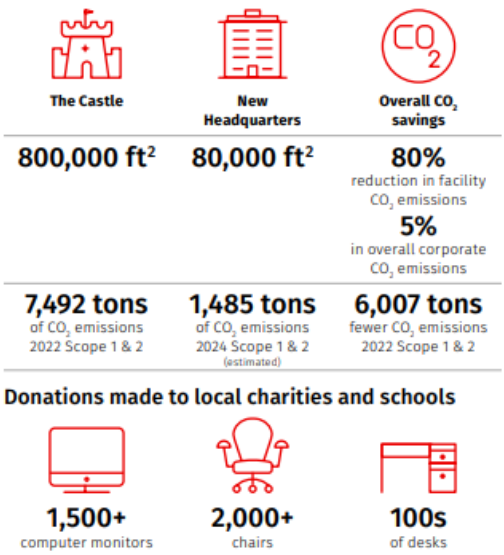
Since 2008, we have taken progressive action to reduce our carbon footprint, enhance energy efficiency and promote sustainability. In 2024-25, we strengthened our emissions data infrastructure, completed both a double materiality assessment and a climate risk assessment and expanded our work in Responsible AI—each representing a critical building block toward a more sustainable future. Following our 2020 IPO, Rackspace Technology committed to achieving net zero carbon emissions by 2045. In 2025, the Science Based Targets initiative

(SBTi) validated our greenhouse gas emissions reduction targets, confirming our commitment to limiting global warming to 1.5°C.

In 2024, our progress was recognised with an improved Carbon Disclosure Project (CDP) score—advancing from a C to a B-. This reflects our increased transparency, stronger climate governance and enhanced emissions management. We invested in a core carbon accounting platform for auditable performance tracking, engaged third party auditors to validate our emissions baseline and integrated sustainability into enterprise risk management and long-term planning.

We have begun the process of automating our large facilities with smart, energy-saving features. We have assembled a cross-functional team to define our ESG-related goals more clearly so we can better measure our impact in the future.

We have also invested in and are deploying smart building automation systems in several locations globally and three data centres, including London. These systems will drive reduced energy consumption in each of these locations, through building control systems that provide the ability to efficiently manage light, heat and cooling zones based on operational demand.



Last year (2024), the highest impact initiative is the move to a new corporate headquarters, which is estimated to reduce our HQ facility footprint and carbon emissions by around 80%. Details of this can also be found in our ESG report. This new location was also chosen with our employees, or ‘Rackers’, in mind, offering a shorter commute for most. Additionally, we continue to work with our partners to drive the use of renewable energy in our data centres and facilities worldwide. We estimate that 80% of energy usage is supplied by renewable sources.

We take a proactive approach to supporting environmental sustainability, operating with ethics and integrity and helping to ensure that our suppliers do the same. To recognise our commitment to sustainability, we created a new leadership role and have appointment Ben Blanquera, Vice President of Sustainability and AI. Working alongside our key functional leaders, with board oversight, Ben Blanquera drives our initiatives, merging innovation with sustainability in a vision that is both progressive and responsible.

13.2.1. Wider Climate Related Initiatives

Company-wide, our additional energy efficiency, environmental and sustainability initiatives include:

- Our efforts are already producing measurable results: 10% reduction in total emissions from 2023 to 2024, 20% reduction in Scope 1 & 2 emissions and 8% reduction in Scope 3 emissions
- Today, approximately 80% of our global data centres are powered by renewable energy and we are advancing toward 100% through new partnerships and ongoing efficiency initiatives.
- We have begun the process of automating our large facilities with smart, energy-saving features. We have assembled a cross-functional team to define our ESG-related goals more clearly so we can better measure our impact in the future.
- We take part in Climate Change Agreement (CCA), which is a UK voluntary scheme for energy-intensive industries.
- We seek to maximise waste through responsibly disposing of data centre assets to provide sustainable materials within our workspaces (for example, we refurbish retired IT equipment for aftermarket use and collect HVAC condensate to maintain landscaping and operate cooling towers).
- We have continued to purchase 100% REGO (Renewable Energy Guarantees Origin) backed energy to cover our consumption in our Slough data centre and our London HQ.
- Energy-saving initiatives include open air fee cooling and the ability to manage light, heat and cooling zones based on operational demand.

We further support carbon reduction through:

- Carbon Accounting Data Platform and Analytics offering, which can help unify data to support an organisation’s sustainability strategy. An optional service, implemented on request, it helps track carbon usage, by ingesting and integrating data from various data stores, for decisioning and external reporting.
- Inclusion of sustainability as a non-functional requirement (NFR) in our hybrid and multicloud solution designs, depending on the customer’s appetite and requirements. We utilise a business and domain-driven architecture framework, using 15+ criteria to guide towards a sustainable distributed cloud architecture, where applicable for the workload.

13.3. Break Down Barriers to Opportunity

Having a diverse workforce, made up of team members who bring a wide variety of skills, abilities, experiences and perspectives, is essential to Rackspace Technology's success. We are committed to the principles of equal employment opportunity, inclusion and respect.

Our Diversity, Inclusion & Belonging Statement

Rackspace Technology is committed to advancing diversity and inclusion at every level in our company. We deliver the future for our customers by creating a culture in which Rackers feel a sense of belonging and can thrive by being their authentic whole selves at work.

Supporting Diverse Communities

We provide equal employment opportunity to everyone who is legally authorised to work in the applicable country and provide reasonable accommodations to individuals with disabilities. Our nine Racker Resource Groups (RRGs) provide professional development, networking, support and belonging for diverse communities, including:

- EAST (Elevating Asian Strengths and Talents)
- POWER (Professional Organisation for Women's Empowerment)
- Together with Pride (LGBTQIA+ support)
- RISE (Black and African Cultures)
- Viva (Hispanic and Latinx culture)
- RackFam (working parents and caregivers)
- RackVET (military veterans)
- NextGen (emerging leaders)
- Rackspace Lavender (mental wellness and physical abilities)

Recognition and Awards: Our commitment to equal opportunities has been recognised by multiple third party organisations:

2025 Recognition

- America's Best Large Employers
- America's Greatest Workplaces for Women
- America's Greatest Workplaces for Diversity
- America's Greatest Workplaces for LGBTQ+
- Human Rights Campaign Leader in LGBTQ+ Workplace Inclusion
- Newsweek Greatest Workplaces in Tech

2024 Recognition

- America's Best Employers for Tech Workers
- America's Greatest Workplaces for Parents and Families
- Great Place to Work certification in Mexico

13.4. Build an NHS Fit for the Future

Rackspace contributes to the NHS’s long-term sustainability, efficiency and resilience by strengthening the digital foundations upon which modern healthcare depends. Although our role is primarily technological, the wider social value delivered – through improved patient care, reduced operational burden, workforce empowerment and enhanced digital inclusion – extends far beyond infrastructure. We draw on real outcomes from our work with NHS organisations apply this across our service delivery.

14. Our Experience

Rackspace has built up demonstrable experience and a strong history of delivering cloud, hosting and professional services to customers within the public sector, healthcare, finance and banking and retail and ecommerce industries, comprising a variety of technologies, for many well-known brands. Through our focus in combining integrated multicloud and support capabilities, we have a proven pedigree in providing private and public cloud and professional consultancy services.

14.1. CNWLCase Studies

CNWL NHS Foundation Trust meets cost-reduction mandates while innovating in multicloud

Central and North West London NHS Foundation Trust (CNWL) was facing enormous pressure to meet a growing demand for its healthcare services and security for its mounting volume of patient data. It needed modern technological capabilities and greater data security.

Our Customer

CNWL provides integrated healthcare in London, Milton Keynes, Surrey and elsewhere, employing over 8,500 staff to provide more than 300 different health services across 150 locations.

How we Helped

With Rackspace Private Cloud already providing the flexibility, speed and resilience it needed to bring innovation to its services, CNWL also deployed a public cloud on Microsoft Azure to deliver some of its services. To help ensure optimised security for its vast stores of sensitive patient data, Rackspace recommended Rackspace Government Cloud, a fully managed security platform-as-a-service.

CNWL chose Rackspace Government Cloud Solutions because of cost savings and low capex, as well as high level of security, offering built-in security at a government-mandated level.

To support a variety of optimisation projects along its journey, CNWL relied heavily on the expert resources available through Rackspace Elastic Engineering, a model which was very effective in building multidisciplinary teams to deliver the Trust's projects. Rackspace also helped to streamline the Trust's IT Operations with our Service Management and ServiceNow solutions, which improved the end-to-end user journey.

The Obstacles Faced

Just prior to the pandemic, CNWL partnered with Rackspace to implement a long-term digital transformation project. When COVID-19 hit, transformation plans were put on hold and CNWL pivoted to focusing on supporting remote work and new models of patient care.

Following the pandemic, CNWL was ready to resume its digital transformation journey. In particular, it needed modern systems that could support the ever-growing demand for its healthcare services and to overcome problems and constraints with capacity, storage, design and being able to expand and change infrastructure quickly. At the same time, the Trust also needed to be cautious about cloud deployments due to the enormous amount of sensitive patient healthcare data it processes.

What we Achieved Together

Cloud services are increasingly crucial to how the NHS delivers its services throughout England. Since expanding and optimising its multicloud infrastructure, CNWL has gained the agility and speed it needs to innovate. Among its innovations is a digital auditing application that allows clinicians to collect data on their phones or computers instead of using paper and pen. Another innovation is the use of QR codes on high-risk medications, which allows patients to watch videos instead of reading instructions.

Modernising on multicloud helped CNWL reduce costs by 15% to 18%. Rackspace Government Cloud makes it easier, faster and more cost effective for the Trust to be innovative. CNWL found that multicloud provides an IT environment that is an order of magnitude better than its former on-premises environment.

For further information, please see:
https://www.rackspace.com/en-gb/case-studies/cnwl

For additional Rackspace case studies, please visit:
https://www.rackspace.com/en-gb/case-studies

"For the past three years, we've reduced our footprint, servers and workloads by about 20%. And we've reduced costs between 15% and 18% just through optimisation."

Nigel Tazzyman, Deputy Director of ICT
Central and North West London NHS Foundation Trust (CNWL)

14.2. Customers

Some of our customers include:

NHS Central and North West London NHS Foundation Trust
TRANSPORT FOR LONDON EVERY JOURNEY MATTERS
BT
British Heart Foundation
NHS Royal Berkshire NHS Foundation Trust
Royal Mail
UK Civil Aviation Authority
OXFAM
NHS Buckinghamshire Healthcare NHS Trust
Great British ENERGY
TARMAC A CRH COMPANY

14.2.1. Contact Details

UK Sovereign Services Sales
Telephone: +44 (0)208 734 8107
Email: SovereignServices@rackspace.co.uk

15. Document History

DOCUMENT DATE	STATUS
29th January 2026	Initial document issue for G-Cloud 15

Table 1 – Document history

This service definition is intended only as a description of Rackspace capabilities with regard to the specified Services. This service definition is not a contract and nothing in this service definition is or may be construed as a legal obligation on the part of Rackspace or its Representatives. This service definition may change from time to time, at the sole discretion of Rackspace.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS A GENERAL INTRODUCTION TO RACKSPACE TECHNOLOGY SERVICES AND DOES NOT INCLUDE ANY LEGAL COMMITMENT ON THE PART OF RACKSPACE.

You should not rely solely on this document to decide whether to purchase the service. Rackspace detailed services descriptions and legal commitments are stated in its services agreements. Rackspace services' features and benefits depend on system configuration and may require enabled hardware, software or additional service activation.

Except as set forth in the agreement you sign with Rackspace, Rackspace assumes no liability whatsoever and disclaims any express or implied warranty, relating to its services including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose and noninfringement.

Although part of the document explains how Rackspace services may work with third party products, the information contained in the document is not designed to work with all scenarios. Any use or changes to third party products and/or configurations should be made at the discretion of your administrators and subject to the applicable terms and conditions of such third party. Rackspace does not provide technical support for third party products, other than specified in your agreement you have with Rackspace and Rackspace accepts no responsibility for third party products.

Rackspace cannot guarantee the accuracy of any information presented after the date of publication.